ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО «ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ПЕДЧЕНКО ЄВГЕНІЙ МАКСИМОВИЧ

УДК 004.056.5

ДИСЕРТАЦІЯ
МЕТОДИ ТА МОДЕЛІ ОЦІНЮВАННЯ СТАНУ КІБЕРЗАХИСТУ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

125 – Кібербезпека
12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії в галузі Кібербезпеки

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Є.М. Педченко

Науковий керівник: **Іванченко Ігор Сергійович**
кандидат технічних наук, доцент

Київ – 2025

АНОТАЦІЯ

Педченко Є.М. Методи та моделі оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (12 – Інформаційні технології). – Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», м. Київ, 2024.

Розроблена дисертаційна робота присвячена оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури для раціонального впровадження заходів кібербезпеки хмарних сервісів, а саме – методу та моделі оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

Об’єктом дослідження дисертаційної роботи є процес оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури. Предметом дослідження дисертаційної роботи є методи та моделі оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

В дисертаційній роботі проведено аналіз існуючих реальних статистичних даних від компаній замовників, що описували різні підходи щодо проведення оцінювання та перевірки відповідності інфраструктурі хмарного сервісу.

В основі проведеного аналізу було використано існуючі системи опитування хмарних сервісів від компаній України, типи існуючих хмарних сервісів, функціональні взаємодії на різних моделях OSI, на основі яких, розроблено власний уніфіковані параметри для комплексного оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

Потреба в розробці параметрів оцінювання полягала в тому, що на сьогоднішній день, жодний стандарт чи регламент не забезпечує повноцінною перевіркою всіх модулів роботи рішення, що тим чи іншим чином обробляє дані бізнесу. Окрім цього, потрібно враховувати, що хмарні сервіси, повинні

забезпечувати кіберзахист даних бізнесу через постійні кібер-атаки, що виникають на просторах кіберпростору.

Розроблено узагальнену математичну модель та метод оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури на основі підготовлених параметрів оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, які детально описують послідовність виконання та опрацювання всіх критеріїв оцінювання, а також відповідей та рекомендацій, що видаються за результатами оцінювання хмарного сервісу. Кожний хмарний сервіс після проведення оцінювання отримує певну кількість балів, на основі яких видається результат-рекомендація, щодо подальшого використання хмарного сервісу для роботи та розгортання бізнес-додатків.

Розроблено структурну модель системи оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури на базі розроблених моделі та методу стану кіберзахисту хмарних сервісів, що включає в себе детальну послідовність виконання мережевого застосунку, що доступний аудитору для проведення оцінювання у зручному та сучасному форматі і з можливістю вибору світлої або темної теми. Окрім цього, представлено деталізовані блок-схеми кожного із параметрів оцінювання хмарних сервісів, і поетапним їх виконанням.

Розроблений мережевий застосунок оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури базується на основі розроблених моделі, методу та структурної моделі, презентуючи аудитору інтуїтивний інтерфейс із можливість проведення аудиту в будь-якій точці світу. За результатами проведеного оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, аудитор має змогу сформувати звіт за результатами оцінювання, отримати рекомендацію щодо подальшого використання хмарного сервісу, а також рекомендації, щодо підвищення кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури у разі його використання бізнесом.

Запропонований захищений мережевий застосунок може бути використаний аудиторами та власниками бізнесу задля оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури перед розміщенням власних бізнес процесів на вибраному хмарному сервісу.

Ключові слова: інформаційна безпека, кібербезпека, інформаційний вплив, критерії оцінювання хмарних сервісів, нечіткі множини та нечітка логіка, оцінювання та управління ризиками, кіберпростір, віртуальні середовища, рівень критичності, кіберзахищеність хмарних сервісів, кіберзагрози, управління інформаційною безпекою, вразливості хмарних сервісів, математична модель параметрів оцінювання, оцінювання нелінійних параметрів кіберзахисту.

ABSTRACT

Pedchenko Y. Methods and models of assessing the state of cybersecurity of cloud services of information infrastructure objects. – Qualification Scientific Work in the Form of a Manuscript.

Dissertation for the Degree of Doctor of Philosophy in the Specialty 125 "Cybersecurity" (12 – Information technologies). – State non-commercial enterprise "State University "Kyiv Aviation Institute", Kyiv, 2024.

The completed dissertation is devoted to assessing the state of cyber protection of cloud services of information infrastructure objects for the rational implementation of cyber security measures of cloud services, namely, the method and model of assessing the state of cyber protection of cloud services of information infrastructure objects.

The object of the dissertation is the process of assessing the state of cyber protection of cloud services of information infrastructure objects. The subject of the dissertation is methods and models of assessing the state of cyber protection of cloud services of information infrastructure objects.

In the dissertation, an analysis of existing real statistical data from customer companies was carried out, which described different approaches to the evaluation and verification of compliance with the infrastructure of the cloud service.

The basis of the analysis was the use of existing survey systems of cloud services from Ukrainian companies, types of existing cloud services, functional interactions based on various OSI models, based on which, our own unified parameters were developed for a comprehensive assessing the state of cyber protection of cloud services of information infrastructure objects.

The need for the development of evaluation parameters was the fact that today, no standard or regulation provides full verification of all work modules of the solution that in one way or another processes business data. In addition, cloud services must provide cyber protection of business data due to constant cyber-attacks that occur in cyberspace.

A generalized mathematical model and method has been developed based on the prepared parameters for assessing the state of cyber protection of cloud services of information infrastructure objects, which describe in detail the sequence of execution and processing of all evaluation criteria, as well as answers and recommendations issued based on the results of cloud service assessment. After the assessment, each cloud service receives a calculated number of points, based on which a recommendation result is issued regarding the further use of the cloud service for working with business applications.

A structural model of the assessing the state of cyber protection of cloud services of information infrastructure objects was developed based on the developed model and state method, which includes a detailed sequence of execution of the web application, which is available to the auditor for assessment in a convenient modern format and with the option of choosing a light or dark theme. In addition, detailed flowcharts of each of the assessment parameters of cloud services and their step-by-step implementation are presented.

The developed web application for assessing the state of cyber protection of cloud services of information infrastructure objects is based on the developed model, method and structural model, presenting the auditor with an intuitive interface with the possibility of conducting an audit anywhere in the world. According to the results of the assessment of the state of cyber protection of cloud services of information infrastructure objects, the auditor can create a report based on the results of the assessment, receive a recommendation on the further use of the cloud service, as well as recommendations on improving the cyber protection of cloud services of information infrastructure objects in the case of its use by business.

This proposed protected network application can be used by auditors and business owners to assess the state of cyber protection of cloud services of information infrastructure objects before placing their own business processes on the selected cloud service.

Keywords: cyber security, information security, information impact, criteria's assessment of cloud services, fuzzy sets (standards) and fuzzy logic, risk assessment

& management, cyberspace, virtual environments, criticality level, cloud services cyberprotection, cyber threats, information security management, cloud services vulnerabilities, mathematical model of assessment parameters, Assessment of nonlinear cybersecurity parameters.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Розділ у колективній монографії:

1. Pedchenko Y., Shulha V., Korchenko O., Ivanchenko Y., Vyshnevska N., Petrovska M. Mathematical model of security cloud services assessment. *Problems of scientific, technical and legal support for cybersecurity in the modern world* : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 13-21. DOI : 10.24917/9788668020861 .

Особистий внесок автора: розробка математичної моделі оцінювання хмарних сервісів об'єктів інформаційної інфраструктури на основі використання попередньо сформованих параметрів оцінки.

2. Pedchenko Y., Karpinski M., Lozova I., Kotyk O., Petrovska M. Damage assessment from the personal data loss. *Problems of scientific, technical and legal support for cybersecurity in the modern world* : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 34-46. DOI : 10.24917/9788668020861 .

Особистий внесок автора: проведення оцінювання потенційного рівня збитку компанії у разі витоку персональних даних співробітників та клієнтів.

Статті у фахових наукових виданнях:

1. Педченко Є.М., Корченко О.Г., Дрейс Ю.О., Лозова І.Л. Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*. 2020. Том. 22, № 2. С. 120-141. URL: https://doi.org/10.18372/2410-7840.22.14871

Особистий внесок автора: формулювання ключових параметрів оцінювання захищеності компанії від витоку персональних даних.

2. Педченко Є.М., Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Захист інформації*. 2023. Том 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232

Особистий внесок автора: опис параметрів оцінювання захищеності компанії від витоку персональних даних у вигляді математичного методу та формул.

3. Педченко Є.М., Іванченко І.С. Структурна модель системи оцінювання кібербезпеки хмарних сервісів об’єктів інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2024. Том 1, № 25. С. 505-515. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/667 . DOI: https://doi.org/10.28925/2663-4023.2024.25.505515

Особистий внесок автора: розробка структурної моделі системи оцінювання стану кіберзахисту хмарних сервісів на основі розроблених моделі та методу дослідження.

4. Педченко Є.М., Іванченко І.С. Метод оцінювання кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури. *Сучасний захист інформації*. 2024. Том. 59, №3. С. 75-84. URL: https://doi.org/10.31673/2409-7292.2024.030008

Особистий внесок автора: розробка методу оцінювання стану кіберзахисту хмарних сервісів на основі розробленої моделі дослідження.

5. Педченко Є.М., Іванченко І.С. Аналіз моделей та методів оцінювання стану кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури. *Безпека інформації*. 2024. Том. 30, №2. С. 279-287. URL: https://doi.org/10.18372/2225-5036.30.19240

Особистий внесок автора: проведено аналіз існуючих моделей та методів оцінювання стану кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури на міжнародних ринках та ринках України.

6. Педченко Є.М., Іванченко І.С. Модель захищеного мережевого додатку оцінювання Кібербезпеки постачальників хмарних сервісів. *Наукові записки ДУІКТ*. 2024. Том. 6, №2. С. 116-134. DOI: 10.31673/2518-7678.2024.025842

Особистий внесок автора: на основі проведеного аналізу існуючих моделей та методів розроблено власну модель оцінювання стану кіберзахисту хмарних сервісів, що є базою для розробки системи оцінювання та захищеного мережевого додатку.

Статті у виданнях, які включено до міжнародних наукометричних баз:

1. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. Analysis of modern cloud services to ensure cybersecurity. *Procedia Computer Science*. 2022. Vol. 207. P. 110-117. Mode of access: https://www.sciencedirect.com/science/article/pii/S1877050922009164 . DOI: https://doi.org/10.1016/j.procs.2022.09.043.

Особистий внесок автора: проведено аналіз сучасних типів хмарних сервісів, що використовуються світовими корпораціями, такими, як Amazon, Google, Microsoft, тощо із виділення основних модулів для побудови моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури.

2. Pedchenko Y., Korchenko O., Ivanchenko Y., Ivanchenko I., Petrovska M. The system of secured user's credentials transfer. *CPITS-II 2024 : Cybersecurity Providing in Information and Telecommunication Systems II*. 2024. P. 168-173. URL: https://ceur-ws.org/Vol-3826/short3.pdf . ISSN: 1613-0073.

Особистий внесок автора: представлення роботи системи авторизації користувача розробленого захищеного мережевого додатку, що буде використано в якості середовища проведення оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури.

Наукові праці, які додатково відображають наукові результати дисертації:

1. Pedchenko Y., Bystrova B., Lozova I., Petrovska M. Fuzzy standards system for negative consequences assessment from personal data leaks. *Polit. Challenges of science today, 5-7 April 2022* : abstracts of XXII International conference of higher education students and young scientists. Kyiv. 2022. P. 12-13.

Особистий внесок автора: розглянуто питання оцінювання негативних наслідків від витоку персональних даних.

2. Pedchenko Y., Ivanchenko I., Lozova I., Petrovska M. System incident management using cloud technologies. *Polit. Challenges of science today, 5-7 April 2023* : abstracts of XXIII International conference of higher education students and young scientists. Kyiv. 2023. P. 3-4. URL: http://www.kzzi.nau.edu.ua/wp-content/uploads/2023/05/Polit_2023_FCSSE.pdf

Особистий внесок автора: проведено аналіз роботи системи управління кіберінцидентами в хмарних сервісах.

3. Педченко Є.М., Іванченко Є.В., Іванченко І.С., Лозова І.Л., Петровська М.Г. Архітектура хмарного рішення для централізованого збору та обробки інцидентів інформаційної безпеки. *ITSec-2023: Безпека інформаційних технологій* : матеріали XII міжнар. наук.-тех. конф., м. Київ, 2-4 травня 2023 р. Київ, 2023. С. 69-73. URL: http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf

Особистий внесок автора: представлено роботу системи централізованого збору та обробки інцидентів інформаційної безпеки для хмарних сервісів.

4. Євгеній Педченко. Технології Akamai для доставки веб-контенту та його захисту. *Мережі та безпека : Захист даних*. Київ. 2023. 2 с. URL:

https://www.seeton.pro/en/news/akamai-technologies-delivery-web-content-and-protection/

Особистий внесок автора: висвітлено основні технології доставки та захисту веб-контенту на базі прикладу діяльності компанії Akamai.

5. Педченко Є.М., Іванченко Є.В., Іванченко І.С., Лозова І.Л., Петровська М.Г. Математична модель оцінки захищеності хмарних сервісів. *ITSec-2024: Безпека інформаційних технологій* : матеріали XII міжнар. наук.-тех. конф., м. Київ, 9-11 травня 2024 р. 2024. Київ, 2024. С. 102-105. URL: https://drive.google.com/file/d/1xbCeTF33YjZbgoXcYqAYz3ST-oKRPCgM/view.

Особистий внесок автора: представлено математичну модель оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CSP	**–**	**Cloud Service Provider**
IaaS	**–**	**Infrastructure-as-a-Service**
CaaS	**–**	**Container-as-a-Service**
PaaS	**–**	**Platform-as-a-Service**
FaaS	**–**	**Function-as-a-Service**
SaaS	**–**	**Software-as-a-Service**
SECaaS	**–**	**Security-as-a-Service**
OSI	**–**	**Open System Interconnection**
БД	**–**	**База даних**
ОС	**–**	**Операційна система**
ARPANET	**–**	**Advanced Research Projects Agency Networks**
VPN	**–**	**Virtual Private Network**
NIST	**–**	**National Institute of Standards and Technology**
API	**–**	**Application Programming Interface**
CPU	**–**	**Central Processing Unit**
RAM	**–**	**Random Access Memory**
GDPR	**–**	**General Data Protection Regulation**
HIPAA	**–**	**Health Insurance Portability and Accountability**
ISO	**–**	**International Organization for Standartization**
DLP	**–**	**Data Loss/Leak Prevention**
GCP	**–**	**Google Cloud Provider**
AWS	**–**	**Amazon Web Services**
DevOps	**–**	**Development Operations**
KPI	**–**	**Key Performance Indicator**
SMI	**–**	**Service Measurement Index**
QoS	**–**	**Quality-of-Service**
SLA	**–**	**Service Level Agreement**
VM	**–**	**Virtual Machine**
PCI DSS	**–**	**Payment Card Industry Data Security Standard**

SOC 2	**–**	**System and Organization Controls 2**
CSSR	**–**	**Cloud Service Security Recommender**
REST API	**–**	**REpresentational State Transfer API**
DNS	**–**	**Domain Name Service**
SSH	**–**	**Secure Shell**
2FA	**–**	**Two-factor Authentication**
MFA	**–**	**Multi-factor Authentication**
MITC	**–**	**Man-in-the-Cloud**
CASB	**–**	**Cloud Access Security Broker**
DNSSEC	**–**	**Domain Name System Security Extensions**
SDLC	**–**	**Software Development Life Cycle**
DLP	**–**	**Data Loss/Leak Prevention**
SIEM	**–**	**Security information and event management**
IDS	**–**	**Intrusion Detection System**
IPS	**–**	**Intrusion Prevention System**
DDoS	**–**	**Distributed Denial-of-Service Attack**
NAC	**–**	**Network Access Control**
PAM	**–**	**Privileged Access Management**
WAF	**–**	**Web Application Control**
WAAP	**–**	**Web Application & API Protection**
SAST	**–**	**Static Application Security Testing**
NGFW	**–**	**Next-Generation Firewall**
SSL	**–**	**Secure Sockets Layer**
TLS	**–**	**Transport Layer Security**
NBAD	**–**	**Network Behavior Anomaly Detection**
NDR	**–**	**Network Detection and Response**
VPC	**–**	**Virtual Private Cloud**
VPS	**–**	**Virtual Private Server**
VDS	**–**	**Virtual Dedicated Server**

ВСТУП

Розпочинаючи з 2021 року коли відбулося різне зростання популярності використання хмарних сервісів, виникла проблема забезпечення якісного кіберзахисту даних сервісів, проте питання оцінювання кіберзахищеності хмарних сервісів залишалося відкритим, оскільки в компаній зростають потреби від хмарних потужностей та сервісів опрацювання і зберігання даних.

Саме тому, можна виділити такі основні проблеми:

- Вплив на забезпечення кібербезпеки через невиправлені вразливості застосунку.
- Необхідність постійного моніторингу та перевірок користувацьких налаштувань через наявність «людської похибки».
- Наявність окремої групи осіб в компанії, що будуть відповідати тільки за організацію та підтримку в актуальному стані систем забезпечення кібербезпеки компанії.

Актуальність. На сьогоднішній день більшість компаній як України, так і світу посилаються на стандарт ISO 27001 задля забезпечення відповідно до нього власної кіберзахищеності, а саме тому враховують, які саме рішення з інформаційної безпеки мають бути наявними в інфраструктурі компанії, проте вимоги даного стандарту ніяким чином не надають покрокового плану щодо оцінки та побудови захищеної мережі компанії. Окрім цього, варто звернути увагу, що даний стандарт націлений саме на забезпечення кіберзахищеності Private інфраструктури компанії, проте дія даного стандарту не поширюється на хмарні сервіси, системи, що використовуються в Public мережі світу.

Розпочинаючи з 2004 року на просторах інформації України та світу існують новітні підходи, щодо розбудови та впровадження моделей оцінки стану захищеності інформаційних систем, що були також використані під час написання кваліфікаційної роботи, що повністю націлені на оцінювання ризиків інформаційної безпеки. Проте, варто враховувати, що сучасні стандарти чи методи направлені на надання тільки рекомендацій, що описують як потрібно проводити оцінювання кіберзагроз, але дані стандарти чи методи

не націлені на чітке виправлення проблематик в кібербезпековому середовищі компанії, тому розробка системи для оцінювання стану кібербезпеки хмарних сервісів об’єктів інформаційної інфраструктури є актуальною науковою задачею.

Зв’язок роботи з науковими програмами, планами, темами, грантами.

Результати дисертаційної роботи відображені у науково-дослідній роботі Державного університету інформаційно-комунікаційних технологій за темою «Розроблення алгоритмів для забезпечення функціональної стійкості інтелектуальних систем при прийнятті рішень» (держ. реєстр. № 0125U000865, 2025-2026 рр.).

Метою дослідження кваліфікаційної роботи є оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури для раціонального впровадження заходів кіберзахищеності хмарних сервісів.

Для досягнення поставленої мети необхідно вирішити **задачі**:

- Провести аналіз методів та моделей оцінювання стану кіберзахисту хмарних сервісів на міжнародних ринках.
- Розробити модель оцінювання кіберзахисту хмарних сервісів для подальшої розробки відповідного методу оцінювання.
- Розробити метод оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури для розробки узагальненої структурної моделі системи оцінювання хмарних сервісів.
- Розробити систему для оцінювання стану кіберзахисту об’єктів інформаційної інфраструктури.
- Розробити мережевий застосунок для оцінювання стану кіберзахисту об’єктів інформаційної інфраструктури.
- Провести експериментальне дослідження програмного застосунку.

Об’єктом дослідження кваліфікаційної роботи є процес оцінки стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

Предметом дослідження кваліфікаційної роботи є методи та моделі оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

Наукова новизна одержаних результатів полягає у наступному:

- *вперше* розроблено узагальнену математичну модель оцінювання на підставі теоретико-множинного підходу оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, яка за рахунок комплексного аналізу хмарних сервісів дозволила формалізувати відповідний набір параметрів оцінювання хмарних сервісів об’єктів інформаційної інфраструктури та розробити відповідний метод оцінювання кіберзахисту хмарних сервісів;

- *вперше* розроблено узагальнений математичний метод оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури на підставі теоретико-множинного підходу за рахунок сформульованих параметрів оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, який за рахунок побудови на базі ключових структурних компонентів хмарних сервісів дав можливість розробити структурну модель.

- *вперше* запропоновано структурну модель системи оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, яка за рахунок методу та моделі оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури дозволила оцінити стан кіберзахисту хмарних сервісів з можливістю оцінювання визначених типів сервісів та надання рекомендацій щодо покращення захищеності інформаційної інфраструктури хмарних сервісів.

Практична значення одержаних результатів дисертаційного дослідження полягає в тому, що:

- розроблено алгоритмічне забезпечення для реалізації захищеного мережевого застосунку на базі розроблених моделі, методу та системи

оцінювання стану кіберзахисту хмарних сервісів об’єктів критичної інфраструктури.

- розроблено захищений мережевий застосунок для оцінювання стану кіберзахисту хмарних сервісів об’єктів критичної інфраструктури, що надає змогу чітко та якісно оцінити стан захищеності визначеного вибраного типу хмарного сервісу на кожному із рівнів взаємодії.

Особистий внесок здобувача складається з робіт, що опубліковані в співавторстві, де в дисертаційній роботі використано тільки результати дослідження, що були отриманні виключно здобувачем.

Результати дисертаційної роботи впроваджено в компанії ТОВ «СІТОН ДІДЖИТАЛ» під час розробки програмного забезпечення оцінювання стану кіберзахисту хмарних сервісів.

Апробація результатів дисертації. Основні результати дисертаційної роботи були представлені та обговорені на таких міжнародних науково-технічних та науково-практичних конференціях: «Polit. Challenges of science today» (м. Київ, 2022), «Polit. Challenges of science today» (м. Київ, 2023), «ITSec-2023: Безпека інформаційних технологій» (м. Київ, 2023), «Мережі та безпека : Захист даних» (м. Київ, 2023), «ITSec-2024: Безпека інформаційних технологій» (м. Київ, 2024).

Публікації. Основні наукові результати дисертаційної роботи опубліковані у 15 наукових працях, із них: 2 розділи у колективній монографії, 6 наукових статей, надрукованих у вітчизняних фахових наукових виданнях, 2 публікації, включені до міжнародної наукометричної бази Scopus, а також 5 тез доповідей на науково-практичних конференціях.

Структура роботи та її обсяг. Дисертація складається із анотації, вступу, трьох розділів, загальних висновків, додатків, списку використаних джерел. Повний обсяг роботи становить 254 сторінки друкованого тексту, з них анотація – на 3 стор., зміст – на 2 стор., основний текст – на 184 стор., список із 108 використаних джерел – на 13 стор., додатки – на 34 стор. Дисертація містить 41 рисунок та 7 таблиць.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ОЦІНЮВАННЯ СТАНІ КІБЕРЗАХИСТУ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

1.1. Базові поняття складових хмарних сервісів

В сучасному інформаційному просторі дані знаходяться в загальній доступності та доступ до інформації є важливим для сучасного інформаційного суспільства. Сьогодні ми живемо в ері хмарних сервісів, що дозволяються зменшити затримки отримання даних, допомогти зберегти кошти та забезпечити доступ до даних з будь-якої точки земної поверхні. То яким же чином сучасному суспільству вдалося дійти до такого розвитку [1]?

Розпочинаючи з 1950 років на потреби армії США було розроблено військовий обчислювальний пристрій або «mainframe», що забезпечував об'єднання декількох робочих станцій в єдину мережу, що дозволяла швидко обмінюватися даними, без використання будь-яких зовнішніх носіїв інформації. Дана технологія швидко розпочала поширюватися, як тільки вона стала відомою науковим товариствам. І навіть, незважаючи на те, що на той час, дана розробка коштувала декілька мільйонів доларів, необхідність забезпечення мережевого доступу між двома абонентами стрімко зростала [1].

До 1996 року, дана розробка не мала жодної статичної назви, але з цього часу було затверджено термін «хмарні обчислення», що було опубліковано в документі під назвою «Compaq» [1]. Саме термін «хмара» вперше був використаний компанією Apple в 1990 роках. Відповідно до публікацій «Computerworld» [2], підрозділ Пентагону під назвою ARPA під керівництвом Джозефа Карла Робнетта Ліклайдера, вперше розпочав широко впроваджувати технології обробки інформації для власних внутрішніх обчислень, що були закритими від усього світу і ними користувалися лише внутрішні служби країни [2].

В 1969 році два розробники Боб Тейлер та Ларрі Робертц, надихнулися ідеєю Ліклайдера та розробили сучасний прообраз мережі інтернет, під назвою ARPANET або повна назва – Advanced Research Projects Agency Networks [3].

В 1970 році компанією IBM було вперше розроблено «Віртуальну машину», що стало відправною точкою в побудові сучасних Віртуальних Приватних мереж, або скорочена назва VPN [4].

Розпочинаючи з 1990 року у світі розпочала зростати кількість персональних комп'ютерів, як в установах, так і в домівках, від чого і розпочалася інформатизація суспільства. Саме через це в 1999 році, компанія Salesforce першої розпочала розповсюджувати програмне забезпечення та власні послуги через мережу Інтернет [5]. З цього моменту, розпочався розвиток напрямку – Software-as-a-Service (надалі SaaS), при якому користувачі користуються тільки інтернет сервісом, а всіма роботами по обслуговуванню займається компанія розробник, по типу, як на сьогодні працює більшість інтернет магазинів [5].

Розпочинаючи з середини 2000-х років, хмарні сервіси розпочинали стрімко розвиватися та впроваджуватися в сучасний інформаційний простір, проте все ж більшості компаніям по всьому світу складно було усвідомити значення «хмарних сервісів» в їх робочому процесі по наданню послуг споживачам послуг. Навіть, Ларрі Еллісон – генеральний директор та співзасновник компанії «Oracle», у 2008 році висловив неоднозначні думки щодо «хмарних сервісів», оскільки на той час, він не мав змоги визначити суттєві переваги їх використання в наданні власних послуг [6]. Незважаючи на такі думки генерального директора компанії «Oracle», сьогодні вона посідає одне з лідируючих позицій в наданні послуг з використанням хмарних сервісів у всьому світі та продовжує покращувати свої позиції в даному напрямку для перенесення всіх своїх рішень в хмару [7].

Розпочинаючи з 2011 Національний інститут Стандартизації та Технологій (NIST – National Institute of Standards and Technology) розробив перший стандарт, що став відправною точкою у застосуванні майже всіма провідними компаніями хмарних ресурсів та сервісів, та народженням нових компаній, що базуються лише на використанні хмарних сервісів. Прикладом такої компанії можна представити компанію CrowdStrike Holding, Inc, що

розпочала своє існування в 2011 році та розпочала з розробки сервісу для забезпечення безпеки робочих станцій від шкідливого програмного забезпечення та першою вивела в тренди захисту робочих станцій поняття Next Generation Antivirus та Endpoint Detection and Response [8]. Станом на кінець 2021 року, компанія CrowdStrike посідає лідируючу позицію в захисті робочих станцій за результатами незалежного міжнародного «магічного» квадрату Gartner (Рис. 1.1) [9]:

Рис. 1.1. Демонстрація лідируючих позицій компанією CrowdStrike при використанні лише хмарних сервісів для надання власних сервісів замовникам

На основі вище вказано, NIST в своїй публікації виділяє п’ять основних характеристик, яким повинен відповідати хмарний сервіс:

- Самостійне обслуговування хмарних ресурсів за запитом – означає, що провайдер повинен надавати лише фізичні ресурси, а встановленням, налаштуванням та обслуговуванням має займатися виключно замовник. До даної категорії відноситься також можливість управління за допомогою «API» запитів [10].
- Необмежений доступ до мережі – означає, що доступ до ресурсів повинно надаватися не тільки через мережу Інтернет, але і з внутрішньої мережі провайдера для можливості обслуговування у випадку збоїв в роботі обладнання [10].
- Виділення фізичних ресурсів – означає, що на одних і тих же фізичних ресурсах (CPU, RAM) можуть базуватися різні замовники і ресурси повинні надаватися виключно за запитом [10].
- Гнучкість – означає, що провайдер, у разі необхідності та «просіданні» роботи сервісу зобов'язаний надати ресурси для забезпечення стабільності роботи та попередження виходу із ладу власного обладнання [10].
- Ресурси як послуга – всі використання ресурсів чітко фіксуються, додаються та повідомляються орендарям [10].

Саме тому, на основі даних п'яти характеристиках, було виділено три основні моделі надання послуг в хмарних сервісах:

- Infrastructure-as-a-Service (надалі IaaS) – модель розгортання на базі провайдера хмарних послуг, що дозволяє повністю розгортати та управляти ресурсами власних обчислювальних потужностей із налаштуванням мережевого доступу та просторі для зберігання даних. Управління розпочинається з рівня операційної системи [10].
- Platform-as-a-Service (надалі PaaS) – модель розгортання на базі провайдера хмарних послуг, що дозволяє встановлювати та налаштовувати програмне забезпечення на вже встановлені та попередньо-налаштованій операційні системи [10].

- Software-as-a-Service (надалі SaaS) – модель розгортання на базі провайдера хмарних послуг, що дозволяє лише користуватися розгорнутим програмних забезпеченням без можливості зміни його програмного коду чи налаштування на рівні операційної системи, а лише в межах програмного забезпечення (Рис. 1.2) [10].

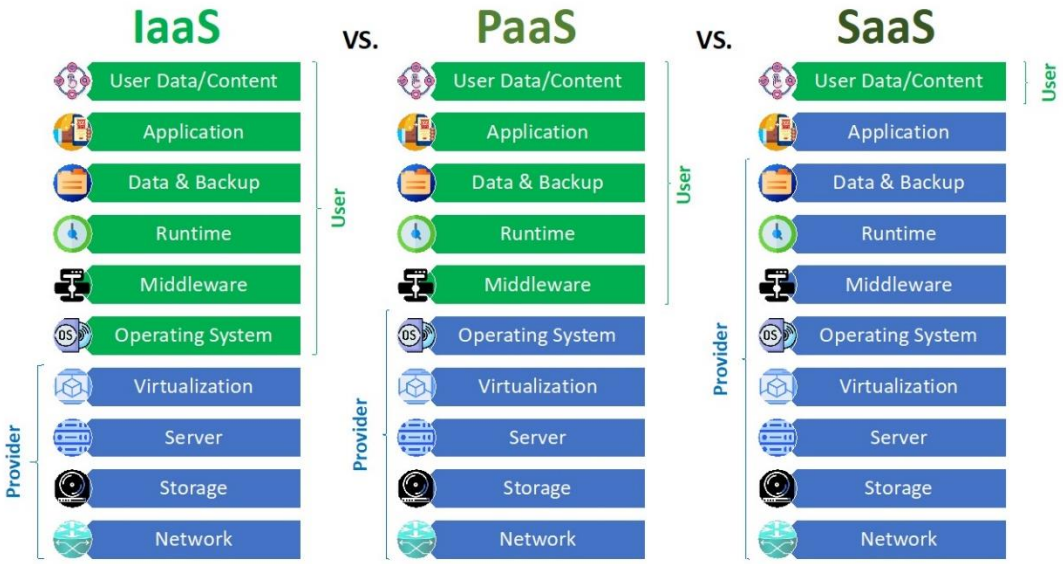


Рис. 1.2. Візуальне представлення порівняння трьох основних моделей надання доступу до хмарних сервісів: IaaS, PaaS та SaaS

Додатково, при використанні трьох, вище описаних моделей надання доступу до хмарних сервісів розрізняють чотири моделі розгортання сервісів, що є базою у сучасному інформаційному просторі:

- **Public Cloud** – це публічні хмарні сервіси, що дозволяють будь-кому скористатися його послугами оплативши певну вартість підписки, що залежить від кількості ресурсів, що виділяються. Вони управляються постачальниками та поширені серед більшості організацій по мережі Інтернет. Це в більшості випадків віртуалізований простір, налаштований на базі VMware чи HyperV, що дозволяє розташовувати на власних обчислювальних ресурсах різноманітні системи та надавати сервіси замовникам/клієнтам. До таких хмарних сервісів відносяться – AWS, Azure, Google та Salesforce [11].
- **Private Cloud** – це модель хмарних технологій, де інфраструктура визначається для кожної організації окремо та залежить від її потреб

бізнесу. Вона розміщується на фізичних віртуальних ресурсах компанії або ж фізичних серверах, які об'єднуються в єдиний Datacenter або Datacenters, що здійснюють обробки всіх необхідних даних компанії, і виконують роль закритого хмарного сервісу лише для працівників компанії. До приватного хмарного сервісу відносять такі типи сервісів, як OpenStack, Cloudstack та VMware. Даний тип хмарного розміщення вирізняється своїми перевагами, такими як:

- *Безпека* – Приватні хмарні сервіси завжди залишаються закритими від зовнішнього світу та управляються адміністраторами із середини мережі компанії [12].
- *Продуктивність* – в основі даного типу сервіси лежать фізичні сервери компанії, що виступають ядром компанії та управляються не віртуальними комутаторами, а фізичним обладнанням, що рознесено по різним локаціям діяльності бізнесу [12].
- *Економія на довгостроковому використанні* – приватні хмарні сервіси завжди дорожчі в придбанні на першому етапі їх впровадження, але з використанням обладнання протягом 5-7 років, їх вартість окупається і вони розпочинають приносити заощадження бізнесу, в порівнянні з публічними хмарними сервісами, що з кожним роком, можуть навіть дорожчати [12].
- *Вимоги міжнародних регуляторів* – більшість міжнародних регламентів, вимагають наявність в компанії різної кількості програмного та фізичного забезпечення, для надання якісного та безпечного контенту своїм замовникам/клієнтам. Приладами таких регуляторів виступають GDPR, HIPPA, ISO 27001 і т.д [12].

- **Community Cloud** – це тип спільного середовища хмарних обчислень, що використовується в більшості обмеженим колом осіб чи організацій, яким необхідна спільна робота з певним типом чи класом рішень для вирішення виявлених проблем чи удосконаленні під потреби бізнесу. Типи розгортання спільних хмарних сервісів можуть

відрізнятися, але будуть мати схожіть між членами даного клубу, які в більшості мають схожі вимоги до організації безпеки, продуктивності тощо. Прикладами таких хмарних сервісів виступають Azure Government, AWS GovCloud, Salesforce Government Cloud та навіть AWS China [13].

- **Hybrid Cloud** – це тип хмарного розміщення, що поєднує в собі декілька комп'ютерних середовищ: локального розгортання різного комплексу рішень замовника в Datacenters (тобто Private Cloud) в поєднанні з рішеннями, що розгорнуті в публічному середовищі (тобто Public Cloud), будуючи захищений канал між даними хмарними сервісами, що дозволяє обмінюватися даними між ними, для забезпечення швидкої взаємодії та передачі даних. Даний тип хмарних сервісів досить складний в обслуговуванні та впровадженні, оскільки вимагає детального прорахунку з боку мережевих архітекторів, щоб організувати коректне мережеве з'єднання між різними типами хмарних сервісів. Даний тип розгортання, допомагає поєднати різні переваги кожного із типів розгортання чи рішень. Як приклад, можна привести, що доцільніше використовувати поштові сервіси, типу Office 365 в хмарі провайдера і власника Microsoft, а рішення для попередження витоку конфіденційних даних, типу DLP (Data Loss/Leak Prevention) краще всього розташовувати в приватному середовищі компанії, для попередження витоку конфіденційних даних компанії за її межі [14].

Говорячи про кожний із даних чотирьох типів розміщення сервісів чи рішень замовника чи бізнесу, може скластися думка, що кожній компанії потрібно впроваджувати кожний із даних типів розміщення рішень. Насправді це не так, і кожна компанії визначає, який із даних типів розгортання їм більше всього підходить. Наприклад, для компанії по розробці програмних продуктів немає сенсу тримати приватні хмарні сервіси та Datacenters, і для них дешевше всього розгортати різні рішення на базі Public Cloud. В той же час для

провайдерів мережевого зв'язку необхідне використання Hybrid Cloud, оскільки за допомогою даного розгортання даний тип компаній забезпечує послугами велику кількість клієнтів у кожній конкретній країні чи світу [14].

Нижче, на Рис. 1.3 візуально представлене порівняння кожного із чотирьох типів розгортання для кращого розуміння відмінностей кожного з них [14]:

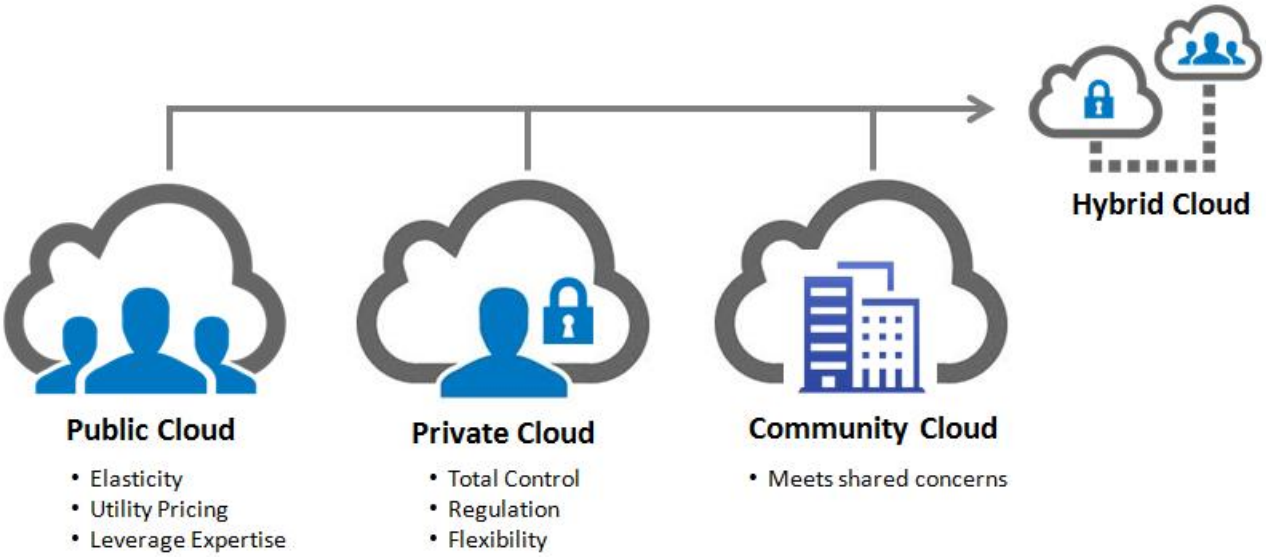


Рис. 1.3. Чотири основні типи розміщення сервісів бізнесу

На початку 2000 року було зафіксовано проблему Y2K (проблема Year 2000). Це проблема, при якій всі застарілі пристрої та програмне забезпечення не могли розпізнати дати після 2000 року. Основна причина була в тому, що оскільки рік зберігався лише у вигляді двох цифр, наприклад 12 вересня 1907 року в базах даних зберігалося у вигляді 09-12-07, замість 09-12-1907, то після 2000 року незрозуміло було, який зараз рік 1907 чи все ж таки 2007 рік [15]. Дану проблему вдалося швидко локалізувати та виправити, тому всі прогнози краху інформаційного простору не здійснилися [15].

Однією з компаній, які допомогли вирішити дану проблему та започаткувати сучасний простір хмарних обчислень стала компанії під назвою Amazon [15].

До сьогодні не відомо, яким чином компанія Amazon розпочала своє існування, як Cloud Service Provider, але існують припущення, що в один прекрасний момент компанія розпочала здавати в оренду власні надлишкові

обчислювальні потужності, що взагалі не використовувалися після піку продаж у святкові дні [15].

Розпочинаючи з 2002 року компанія Amazon або AWS, розпочала пропонувати лише декілька власних послуг, що орієнтувалися на допомогу власним партнерам при інтеграції їх сервісів зі своєї платформою типу e-commerce (онлайн магазину), що до сьогодні функціонує в повній мірі під назвою Amazon Marketplace [15].

Із 2004 року компанія Amazon представила світу в бета-версії власну платформу для відслідковування черги розробників в онлайн режимі під назвою Amazon Simple Queue Service (SQS) [15].

В 2006 році, компанія AWS ввела в експлуатацію два корисних сервіси – Amazon Simple Storage Service (S3) для надання послуг хмарних джерел збереження даних (файловий сервер із сукупності різного масиву HDD дисків та магнітних накопичувачів для зберігання журналів подій протягом тривалого часу) та Amazon Elastic Compute Cloud (EC2) як IaaS сервіс, що надавав можливість орендувати фізичні ресурси для розгортання на них будь-якого типу програмного забезпечення із можливістю повного його адміністрування та налаштування [15].

Розпочинаючи з 2009 року компанія Amazon поширила на ринок відомі на сьогодні всім сервіси, такі як:

- **Amazon CloudWatch** – це рішення забезпечує спостереження та моніторинг для систем розробки та DevOps фахівців/команд. Завдяки використанню даного програмного забезпечення компанії мають змогу отримувати сповіщення про знайдені компоненти розроблюваних ПЗ, та здійснювати реагування на отримані сповіщення. За допомогою даного хмарного сервісу, команди розробки мали можливість автоматизовано збирати події зі своїх систем та проводити автоматичні реагування на інциденти, що виявлялися в роботі розробленого програмного забезпечення [16].

- **Amazon Virtual Private Cloud (VPC)** – дане рішення дозволяє запускати ресурси, орендовані в хмарі AWS, в безпечному середовищі на підготовленому віртуальному середовищі. Рішення розгорнуті на базі Amazon EC2, тобто на фізичних ресурсах AWS, що дозволяє повністю контролювати виділеним середовищем та визначати ресурси під конкретну задачу зі сторони бізнесу. Завдяки використанню даного сервісу, бізнес має право запустити свій перший веб-додаток досить швидко та з безпечного ізольованого простору AWS, що є закритим від сторонніх нелегітимних користувачів [17].
- **Amazon Relational Database Service (RDS)** – це рішення призначене для швидкого та безпечного розгортання баз даних в хмарні AWS. Завдяки даному сервісу, існує можливість масштабування традиційних реляційних баз даних. Даний сервіс підтримує роботу з такими базами даних, як: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle BD, Microsoft SQL Server [18].
- **AWS Auto Scaling** – дане рішення націлене на моніторинг додатків та автоматичне виділення додаткових ресурсів, у випадку виявлення недостатньої кількості виділених ресурсів. За рахунок динамічного виділення ресурсів та їх зменшення, бізнес має можливість зекономити на оплаті вартості послуг AWS. Кількість ресурсів, які можна виділити – адміністратор регулює автоматично та його вибір від вартості ресурсів для даних сервісів [19].

Саме, за допомогою вище описаних чотирьох хмарних сервісів, компанія Amazon стрімко розпочала свій розвиток в галузі провайдерів хмарних сервісів та на сьогодні, це один із найбільших CSP провайдерів у всьому світі. Як видно з Рис. 1.4, дана компанія займає лідируючу позицію серед усіх CSP на міжнародному ринку станом на 2021 рік відповідно до Gartner Magic Quadrant [19]:

Рис. 1.4. Рейтинг Cloud Infrastructure & Platform Services за версією Gartner

Розпочинаючи з 2007 року, компанія IBM розпочала розвиток свого власного хмарного сервісу, який сьогодні відомий як IBM Cloud. На власних обчислювальних ресурсах компанія IBM планувала поширювати послуги для клієнтів по автоматизації та захисту інформаційного простору. За увесь час існування даного хмарного сервісу, компанія поширює виключно власні програмні засоби та не надає можливості стороннім рішенням розташовуватися на ресурсах сервісу IBM Cloud [20].

У 2008 році на ринок хмарних провайдерів розпочала впроваджуватися компанія під назвою Google, Inc. У цьому році на ресурсах даної компанії було розгорнуто хмарні обчислення у вигляді PaaS інфраструктури, а саме сервіси від компанії Google. На сьогоднішній день даний провайдер відомий під назвою Google Cloud: Cloud Computing Services (GCP) [21].

Того ж самого 2008 року, на ринок хмарних сервісів вийшла компанія під назвою Microsoft, щоб презентувати всім відоме рішення під назвою Windows Azure, що дозволило користувачам і бізнесу розміщувати власні веб-додатки на ресурсах центрів обробки даних компанії Microsoft, тим самим дозволяючи

свої клієнтам заощадити на утриманні фізичних пристроїв та їх постійного оновлення та підтримки в актуальному стані [22].

Також, розпочинаючи з 2009 року на ринок хмарних сервісів увійшла компанія, під назвою Alibaba Group. Вона представила свою власну розробку під назвою Alibaba Cloud та розмістила перший свій Datacenter у Китаї [23].

Розпочинаючи з 2009 року Gartner Magic Quadrant випустив свій перший квадрат, в якому розподілив Хмарних сервіс провайдерів розпочинаючи із лідерів та завершуючи новачками. Серед лідерів було визнано такі компанії, як: AT&T, Savvis, Terremark та IBM. А компанія, яка на сьогодні лідером, це Amazon – на 2009 рік посіла місце тільки в квадраті Visionary.

Уже в 2011 році компанія Gartner випустила свій оновлений Magic Quadrant, що визначав лідерів IaaS послуг, і до лідерів віднесли AWS, Terremark, Savvis, Bluelock. В даному квадранті, компанія IBM дещо послабила свої позиції та перемістилася в категорію Challengers, а от компанії Microsoft та Google взагалі не ввійшли в даний розподіл, оскільки на той момент ще не мали повноцінної функціонуючої IaaS інфраструктури [24].

Для розвитку хмарних сервісів, 2010 рік був наймасовішим, оскільки в даний рік вийшло на ринок досить цікавих та відомих постачальників CSPs. Першим варто відзначити компанію Microsoft, яка офіційно перезапустила платформу Azure та зробила її доступною для 41 країни по всьому світу. Станом на 2010 рік платформа Azure містила в собі такі сервіси, як: Windows Azure, SQL Azure та AppFabric [25].

Також, цього ж року на ринок приватних хмарних сервісів вийшла компанія під назвою OpenStack, що мала відкритий код власного програмного забезпечення та вважалася спільним проектом NASA та Rackspace. Головної місією компанії OpenStack було створення вільної платформи для хмарних обчислень із відкритим кодом, для забезпечення простори реалізації, гнучкості в налаштуванні та адаптації до потреб бізнесу, в якому планується впровадження даного сервісу [26].

Разом із вищеперерахованими компаніями на ринок хмарних сервісів увійшла і компанія CloudStack, що позиціонувала себе також як платформа для приватних хмарних сервісів із відкритим вихідним кодом. Незважаючи на те, що більша частина коду все ж знаходиться у відкритому доступі, то 5% відкритого коду лишилося у приватній власності розробників даного рішення. Наразі дана компанія є частиною компанії Apache [27].

Розпочинаючи з 2011 року конкуренція на ринку хмарних сервісів розпочала збільшуватися і сформувалася нова компанія під назвою DigitalOcean. З 2012 року дана компанія запустила свою першу beta-версію рішення і відразу ж отримала до 500 перших клієнтів. Протягом свого існування дана компанія робила акцент на забезпечення безперебійної роботи розробників програмного забезпечення [28].

В цьому ж 2011 році компанія IBM представила свій варіант хмарного сервісу IBM SmartCloud, що була націлена на Enterprise рівень замовників, забезпечувала підтримку AIX систем та технології Hadoop для випадків по використанні великих об’ємів обчислювальних даних [29].

Також, 2011 року компанія VMware анонсувала випуск багатохмарного рішення на базі PaaS технології з відкритим вихідним кодом, що отримав назву Cloud Foundry. Дане рішення дозволяло завдяки технологіям компанії Apache, розробити рішення для спрощення та пришвидшення DevOps команди та випуск рішень на ринок IT послуг [30].

Розпочинаючи з 2012 року компанія Microsoft оновила свою лінійку продуктів під назвою Windows Azure, та додала підтримку віртуальних машин на базі Windows та Linux, та ввела можливість придбати підписку типу IaaS. Розпочинаючи з цього року, розпочав розвиватися окремий веб-сайт для управління опублікованими веб-сайтами в хмарі Microsoft, під назвою Azure Web Sites, що працює в режимі PaaS та з 2015 року і до сих пір носить назву App Service [31].

Напочатку 2012 року, комітет компанії Google додав до ради директорів компанії колишнього директора та президента компанії VMware – Даяна

Гріна. Цього ж року, компанія Google запустила свій перший сервіс – IaaS, що мав назву Google Compute Engine та необхідний був, щоб розділити ринок з сервісами від таких компаній, Amazon та Azure. Сервіс Google Compute Engine став загальнодоступним для своїх клієнтів в кінці 2013 року, але до цього моменту був доступнім в закритому бета тесті [32].

До гігантів хмарних сервісів, що перелічені вище, в 2012 році вирішила приєднатися і компанія HP із анонсованим власним сервісом в 2011 під назвою HP Public Cloud [33].

Напочатку 2013 року компанія Amazon розпочала розширення своїх послуг на міжнародний ринок і зробила це з частиною Китая, що не є частиною глобальної мережі. Для даного ринку, компанія Amazon анонсувала два рішення – AWS CloudTrail та Amazon Kinesis, для роботи з API запитами та сервісом повного збору та управління потоковими даними, типу IoT телеметрії [34].

В кінці 2012 року і напочатку 2013 років компанія IBM придбала компанію SoftLayer, та з цього моменту розпочалася нова ера під назвою Cloud Services Division для компанії IBM. Компанія SoftLayer обслуговувала більше 20000 клієнтів і мала по всьому світу 13 Datacenters. Тільки у 2018 році, компанія IBM перейменувала компанію SoftLayer an IBM company в назву, яка відома і до сьогодні – IBM Cloud [35].

Цього ж, 2013 року компанія VMware оголосила про запуск своєї нової платформи, під назвою vCloud Hybrid Service, що дозволяє об’єднувати рішення для віртуалізації на базі vSphere та можливості IaaS сервісів [36].

Розпочинаючи з 2014 року, компанія Microsoft переглянула свої цілі та позиції на ринку хмарних сервісів, та внесла деякі конструктивні зміни до власних сервісів, щоб підвищити власну конкурентоспроможність. Зміни також стосувалися і назви рішення, саме тому в 2014 році, компанія перейменувала продукт із Windows Azure в Microsoft Azure, де під даною назвою сервісів відомий і до сьогодні [37].

В 2014 році Google запровадила новий підхід до ліцензування Google Cloud Engine та ввела систему знижок, що відома під назвою Sustained Use Discounts, що залежала від кількості розгорнутих віртуальних машин та використовуваних ними обчислювальних ресурсів [38].

Також, в 2014 році AWS опублікувала запуск нової платформи для роботи з базами даних під назвою Amazon RDS for Aurora, що працює на базі рішення від компанії MySQL. Було запущено ще два сервіси – AWS Key Management Service (сервіс для контролю та створення криптографічних ключів) та Amazon EC2 Container Service (сервіс, що дозволяв на базі ресурсів Amazon EC2 розгортати контейнери від компанії Docker) [39].

Саме тому, можна стверджувати, що з 2014 року стартує ера технологій на базі контейнерів, що дозволяє клієнтам чітко виділяти ресурси для певного моменту часу і необхідності того чи іншого сервісу, заощаджуючи час на його повне встановлення та налаштування, оскільки в контейнері вже проведено налаштування кожного сервісу і закладено технологію використання Plug&Play [40].

Розпочинаючи з 2015 року, на ринку з’являється платформа Kubernetes для управління контейнерами на базі Docker, щоб забезпечити візуальне представлення того, які контейнери виконуються, а які з них вже завершили своє виконання. Розвиток даної платформи підтримали такі компанії, як Google, Microsoft, Red Hat, IBM та Docker [41]. Компанія Google разом із Linux Foundation, анонсували про створення Cloud Native Computing Foundation для перенесення можливостей контейнерної технології на ресурси хмарних сервісів. Саме розпочинаючи з цього часу, хмарні сервіси компанії Google працюють з використанням контейнерної технології [41].

Також, ініціативу перейняла і компанія Amazon та в 2015 році впровадила використання контейнерів та рішенням Kubernetes, що дозволило принести прибутку компанії в розмірі $7.88 млрд [42].

В 2016 році, конкуренція на ринку хмарних сервісів зросла до критичної точки, що декілька невеликих CSPs вирішили припинити свою роботу,

оскільки вони були не здатними конкурувати з Google, Amazon та Azure. Про свої закриття заявила компанія Verizon [43] та HP Helion Cloud [44].

В 2017 році компанія Amazon продовжує створювати нові сервіси та оновлювати наявні, та постійно змінює політику ціноутворення, для забезпечення гнучкості для клієнтів та допомога в отриманні знижок. Додатково, Amazon випускає ще два нових продукти: AWS Fargate [45] (рішення побудовано як serverless і дозволяє клієнтам управляти контейнерами без необхідності управління стеками контейнерів) та AWS SageMaker (рішення для розробників та науковців, що здатне надати можливість створення, навчання та налаштування моделей машинного навчання) [46].

В 2017 році компанія VMware оголосила про продаж власного хмарного сервісу vCloud Air європейському провайдеру. Того ж року, компанії AWS та VMware оголосили про технологічне партнерство, що стало доступне для користувачів. Це дозволило використовувати VMware vSphere на ресурсах компанії Amazon та об'єднувати дві консолі управління (Cloud та On-premise) [47].

В 2017 році компанія Microsoft випустила фінальний реліз Azure Stack. Дане рішення використовується в компанії для роботи з Hybrid-інфраструктурою та поєднання роботи між такими виробниками мережевого обладнання, як Cisco, Dell [47].

В 2018 році компанія IBM оголосила про придбання компанії Red Hat за $34 млрд. Компанія змінила свої погляди та підходи до ринку хмарних сервісів. У завдяки придбанню компанії Red Hat, наступне оновлення хмари IBM, отримало назву Cloud Pack, що містило в основі рішення від компанії Red Hat [48].

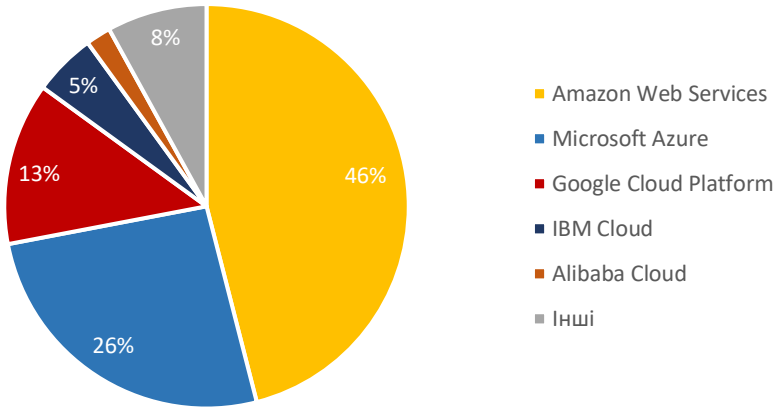
Іншою гучною подією 2018 року було придбання компанією Microsoft компанії GiHub за $7.5 млрд. Саме з цього моменту більшість рішень компанії Microsoft отримали нативну підтримку GitHub сервісу [49].

У 2019 році компанія Google анонсувала про вихід рішення під назвою Google Anthos, що дозволяло користувачам керувати та розгортати додатки на базі контейнерів, в будь-якому Kubernetes середовищі, незалежно від типу його розгортання (Cloud чи On-Premise), з підтримкою розгортань на базі сторонніх провайдерів хмарних сервісів [50].

Цього ж року компанія Microsoft випустила рішення під назвою Azure Arc, що надало змогу користувачам керувати віртуальними машинами, незважаючи на платформу (Cloud чи On-Premise) в кластерах Kubernetes [51].

Завдяки проведеному дослідженню ми можемо спостерігати, яким чином змінювалися хмарні сервіси різних хмарних сервісних провайдерів, таких як Amazon, Google, Microsoft, IBM, VMware, та їх підхід до надання послуг своїм клієнтам за допомогою пропонованих сервісів [52].

Незважаючи на функціональну схожість кожного із хмарних провайдерів, частка кожного із них суттєво відрізняється. Для визначення лідера ринку, побудуємо Діаграму 1.1 опираючись на рейтинги компанії Gartner станом на початок 2022 року [53]. За результатами проведеного аналізу маємо, що лідируючі позиції займає компанія Amazon – 46%, далі йдуть Microsoft Azure – 26%, Google Cloud Platform – 13%, IBM Cloud – 5%, Alibaba Cloud – 2% та всі інші хмарні сервіси разом займають близько 8% всього міжнародного ринку [94].



Діаграма 1.1. Частка хмарних сервісних провайдерів (в %) станом на початок 2022 року

1.2. Міжнародні дослідження в сфері безпеки хмарних сервісів

Опираючись на міжнародний досвід можна знайти досить багато цікавих фактів, що стосуються розвитку безпеки хмарних сервісів в відомих провайдерах, що дозволяє оцінити яких заходів було вжито відомим на сьогоднішній день хмарним сервісам для забезпечення безпеки даних своїх клієнтів та уникнути падінь власної репутації на міжнародній арені хмарних сервісів [54].

Розпочинаючи з 2011 року, коли хмарні сервіси та провайдери розпочинали набирати обертів, розпочали з'являтися корисні публікації, статті та доповіді, що дозволяли оцінити можливості кожної платформи, в залежності від їхнього функціоналу, стану захищеності сервісів та часу реакції на кожний запит користувачів [54].

Однією з таких публікацій можна вважати статтю під назвою «SMICloud: A Framework for Comparing and Ranking Cloud Services» презентованою трьома дослідниками S. K. Garg, S. Versteeg та Rajkumar Buyya із Мельберського університету в Австралії в 2011 році. В даній статті дослідники використали напрацювання Міжнародної компанії по Стандартизації (ISO), що дозволяли визначити Key Performance Indicators (KPI's) для потреб бізнесу виходячи із можливостей хмарних сервісів того часу. Вони назвали власну оцінку – Service Measurement Index (SMI) – Індекс Вимірювання Послуг, що дозволяла отримати повноцінне уявлення про Якість обслуговування (або Quality-of-Service (QoS)) кожного із сервісів, що бере участь в порівнянні шляхом використання наступним KPI:

- **Підзвітність** – дана група категорій QoS необхідна для оцінки можливостей хмарного сервісу, що дозволяє побудувати довіру до клієнта. Це необхідно для того, щоб клієнти повірили, що у вибраному хмарному сервісі безпечно зберігати персональні дані своєї компанії чи власних клієнтів. Одним у ключових потреб, які визначають дослідники, є можливість проведення аудиту, адекватність

постачальника послуг та стійкість до кібератак, що прагнуть отримати конфіденційні дані компанії [54].

- **Адаптація до потреб бізнесу** – завдяки перевагам використання хмарних сервісів, бізнес має змогу адаптувати свої сервіси в будь-який момент часу під потреби власних замовників, без необхідності вкладатися в додаткові обчислювальні ресурси. Як зазначають дослідники, відповідно до QoS дані сервіси наділені такими перевагами, як: еластичність, портативність та гнучкість [54].
- **Безвідмовність** – як зазначається, даний атрибут відповідає за мінімізації відмови хмарного сервісу в обслуговуванні, навіть, при виході із ладу кластеру обчислювальних серверів шляхом забезпечення відмовостійкості сервісу та дотримання затвердженого рівня в Угоді про рівень обслуговування (Service Level Agreement (SLA)). Оскільки всі компанії хочуть забезпечити роботу власних сервісів 24/7, то даний атрибут є критичним та дозволяє бізнесу проводити операції із сервісом в незалежності від доби часу чи пори року [54].
- **Вартість** – як говориться в проведеному дослідженні та є реальністю до сьогоднішнього дня, бізнес та керівники підрозділів окрім функціональних можливостей, опираються на вартість хмарних обчислювальних ресурсів, то даний атрибут відіграє інколи ключову роль в прийнятті рішень. Наприклад, для малого бізнесу даний атрибут відіграє ключову роль та обмежить у наданні певного функціоналу замовникам на початковому етапі запуску сервісу, що може зменшити конкуренто спроможність рішення [54].
- **Безпека та Конфіденційність** – оскільки як і в 2011 році, так і в сучасному світі, кожна компанія турбується за захист власних персональних даних і даних клієнтів, тому як зазначається, важливим атрибутом є саме захист даних та їх конфіденційна обробка. Перед тим, як кожна компанія закуповує послуги в хмарним провайдерів,

першочергово кожна з ним просить CSPs надати пакет документів, що підтверджують відповідність міжнародним стандартам, таким як ISO 27000, HIPPA, GDPR тощо [54].

- **Зручність у використанні** – як зазначають дослідники, останнім атрибутом вважається саме зручність використання хмарних сервісів, оскільки саме від цього залежить швидкість їх адміністрування наявність додаткових витрат на залучення спеціалізованого персоналу. Як зазначається, хмарний сервіс повинен відповідати таким ключовим факторам, як: доступність інтерфейсу, можливість простого налаштування сервісу, можливість швидкого навчання роботи з сервісом та функціональна працездатність хмарного сервісу в незалежності від потреб бізнесу та сервісу, який необхідно розгорнути [54].

Саме тому, в даній статті дослідники визначають наступну архітектуру (Рис. 1.5), що надає змогу бізнесу порівняти з атрибутами, описаними вище, ключові хмарні сервіси та вибирати те, що задовольняє потреби бізнесу [54]:

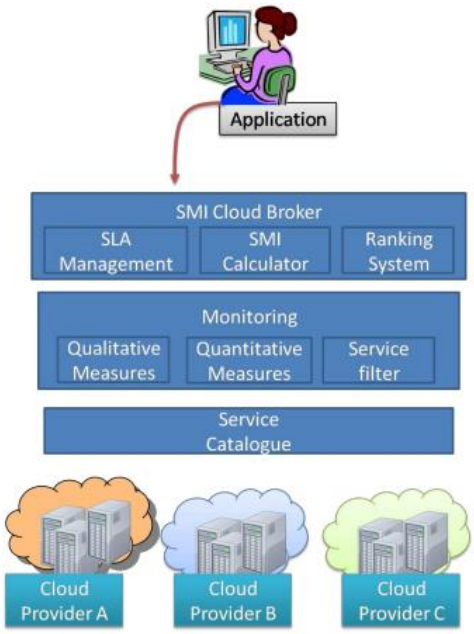


Рис. 1.5. Архітектура вибору CSPs від SMICloud

Повертаючись в 2016 рік, відомі дослідники Абдулла Абухусейн та Фредерік Т. Шелдон вперше розробили чіткі рекомендації, які дозволяли користувач хмарних сервісів описати важливість побудови захищеності

орендованих сервісів та як саме потрібно підходити до організації кіберзахисту хмарних сервісів [55].

Вперше, дані дослідники намагалися просунути свої рекомендації для захисту хмарних сервісів в 2013 році, але на той момент більшість компаній та користувачів, що користуються послугами CSPs не розуміли, навіщо їм купувати додаткові послуги, якщо бізнес процеси працюють безперебійно та виконують свої функції на 100%, приносячи прибуток компанії. Але в період із 2013 по 2016 роки було проведено різноманітну кількість кібератак на хмарні сервіси та веб-додатки, що функціонують на ресурсах хмарних сервісів, таких провайдерів, як Amazon, Azure, то дослідники зробили другу спробу опублікувати власну статтю про доцільність забезпечення захищеності хмарних сервісів, побудови гнучкої системи захисту із мінімальними грошовими витратами та підвищення ефективності бізнесу завдяки підвищення репутації компанії [55].

Абдулла Абухусейн та Фредерік Т. Шелдон запропонували два мотиваційні сценарії, що демонструють складності при роботі з хмарними сервісами зі збільшенням кількості бізнес-процесів [55]:

- **Проблеми Cloud Computing.** Оскільки, чим більше бізнес процесів виконується на базі хмарних сервісів, контролювати та відстежувати кожний із них стає все складніше і це, в першу чергу, пов’язано з: різноманітністю правил та регуляторних обмежень країн щодо забезпечення логування кожного процесу (вразливостями безпеки, катастрофами, репутацією); поєднанням різних форм розгортання хмарних сервісів (SaaS, PaaS, IaaS), що вимагають різного рівня обслуговування та навичок адміністраторів; різноманітністю видів хмарних сервісів (Public, Private, Hybrid та Community). Опираючись на ці пункти, станом на 2016 рік побудова безпечного середовища для хмарних сервісів інколи вимагала навіть перебудови бізнес процесів. Найпростішим рішенням, що пропонувати CSPs для покриття базового рівня захисту даних замовників та відповідності міжнародним

регуляторам, було саме запровадження плану аварійного відновлення сервісу у разі його «падіння», а іншими словами проведення регулярних BackUp процедур розгорнутих сервісів замовників [55].

- **Проблеми зацікавлених сторін**. Незважаючи на всі спроби CSPs зменшити потенційні падіння сервісів замовників хмарних сервісів та кібератаки, всі налаштування продовжують залежати саме від користувачів/орендарів хмарних сервісів. Більшість орендарів намагаються зменшити витрати на безпеку та підвищити продуктивність сервісу за рахунок розширення ресурсів хмарних обчислювальних потужностей. Через те, що орендарі нехтують організацією безпеки хмарних сервісів, то виникає так звана загроза «Cloud Security Alliance», чи «Недостатня захищеність хмарних обчислень». Як прикладом даної загрози можна навести інцидент 2013 року, що стався з більшістю замовників сервісу Amazon S3, коли дані були залишеними без захисту і будь-який Інтернет користувач мав змогу отримати доступ до 126 млрд. конфіденційних даних компаній та логів запущених сервісів. Це все було пов’язано з тим, що компанії мали недостатній рівень знань та обізнаності в налаштуванні вбудованого функціоналу організації конфіденційності в рамках розгорнутих хмарних сервісах [55].

Саме тому, коли дослідники визначили дані дві ключові проблеми в організації роботи та захищеності хмарних сервісів, вони отримали чітке бачення, яким саме чином можна надати рекомендації по забезпеченню хоча б базової захищеності розгорнутих сервісів бізнесу на базі ресурсів провайдерів хмарних сервісів. На міжнародній арені дані рекомендації мають скорочення CSSR або «Рекомендації для забезпечення безпеки хмарних сервісів» [55].

Як вказують дослідники, хмарні сервіси включають загальновідомі та нові вразливості, що відомі при організації безпеки віртуальних машин, оскільки кожний сервіс, що розміщується на ресурсах CSPs, розгортається на

базі віртуальних машин і для них відомі такі проблеми, як: атаки на канали управління VM, нестача ресурсів для роботи VM та інші [55].

На сьогоднішній день на ринку інформаційних технологій присутні компанії, що надають послуги Безпека як послуга (SECaaS) для забезпечення безпечного функціонування хмарних сервісів в інформаційному просторі. Дані компанії зазвичай наймають для підвищення рівня безпеки сервісів розміщених на ресурсах CSPs та для забезпечення відповідності таким міжнародним стандартам як: HIPPA, PCI DSS, SOC 2, ISO 27001 тощо [55].

Як зазначають Абдулла Абухусейн та Фредерік Т. Шелдон, що окрім стандартів та рішень для забезпечення безпеки хмарних сервісів, необхідно також покладатися на рекомендації від провайдерів хмарних послуг. Вони мають на меті надати найкращі рекомендації для забезпечення безпеки хмарних сервісів, що найкраще підходять для вибраного CSP [55].

Саме час поговорити про рекомендації розроблені Абдуллом Абухусейном та Фредеріком Т. Шелдоном, що рекомендується виконувати для розгорнутих сервісів на базі ресурсів провайдерів хмарних сервісів. «Рекомендації для забезпечення безпеки хмарних сервісів» містять у собі 4 основні цілі [55]:

- **Створення сценарію**. Розробка гіпотез для вирішення поставлених задач на базі ресурсів CSPs та оцінювання операційних витрат та сценаріїв, які повинні виконуватися на ресурсах хмарних сервісів для досягнення вищої ефективності бізнес-процесів при наданні послуг клієнтів даної компанії. Завдяки такому підходу, відповідальна особа зможе чітко і якісно оцінити для яких саме потреб необхідно оплачувати ресурси хмарних сервісів [55].
- **Порівняння хмарних сервісів**. Дані рекомендації необхідні для здійснення сортування функціоналу хмарних сервісів для забезпечення можливості вибору правильного хмарного сервісу. При накладанні вимог до необхідного сервісу на ресурси хмарних сервісів,

відповідальна особа має змогу краще дослідити власний сервіс та можливості CSPs для розширення функціоналу в майбутньому [55].

- **Вимоги до хмарних сервісів повинні відповідати стандарту NIST**. Рекомендації, розроблені дослідниками чітко слідують рекомендаціям, описаним міжнародними практиками для забезпечення максимально-можливого рівня захищеності хмарних сервісів, що забезпечують працездатність бізнес процесів бізнесу [55].
- **Орієнтація на зацікавлених сторін**. Зацікавлені сторони є важливими при виборі хмарних сервісів, оскільки вони в першу чергу зацікавлені у належному функціонуванню наданого сервісу замовникам та відпрацювання бізнес процесів замовників. У випадку, якщо на вибраному CSPs буде витік даних чи масштабний збій за вини провайдера, рівень довіри та репутація даного CSPs буде стрімко падати. Саме тому, зацікавлені сторони постійно проводять перевірки працездатності хмарних сервісів та аудити відповідності міжнародним стандартам для надання якісних послуг замовника та бізнесу [55].

Саме тому, за допомогою даних чотирьох цілей, дослідники пропонують три уніфікованих етапи для забезпечення захищеності сервісів на базі хмарних сервісів [55]:

- Залучення зацікавлених сторін у виборі та забезпечення безпеки бізнес процесів [55].
- Залучення зацікавлених сторін для вибору надійних постачальників хмарних послуг [55].
- Залучення зацікавлених сторін для визначення відповідальності кожної із сторін за порушення рівня безпеки бізнес процесів розгорнутих на ресурсах хмарних сервісів [55].

На основі розроблених рекомендацій, дослідники Абдулл Абухусейн та Фредерік Т. Шелдон представили спрощену ілюстрацію, що зображена на Рис. 1.6, що дозволяє замовника та бізнесу чітко визначити основі цілі при виборі провайдера хмарних послуг та вимог до ресурсів, що повинні

забезпечувати належне функціонування бізнес процесів бізнесу для надання належного сервісу клієнтам [55].

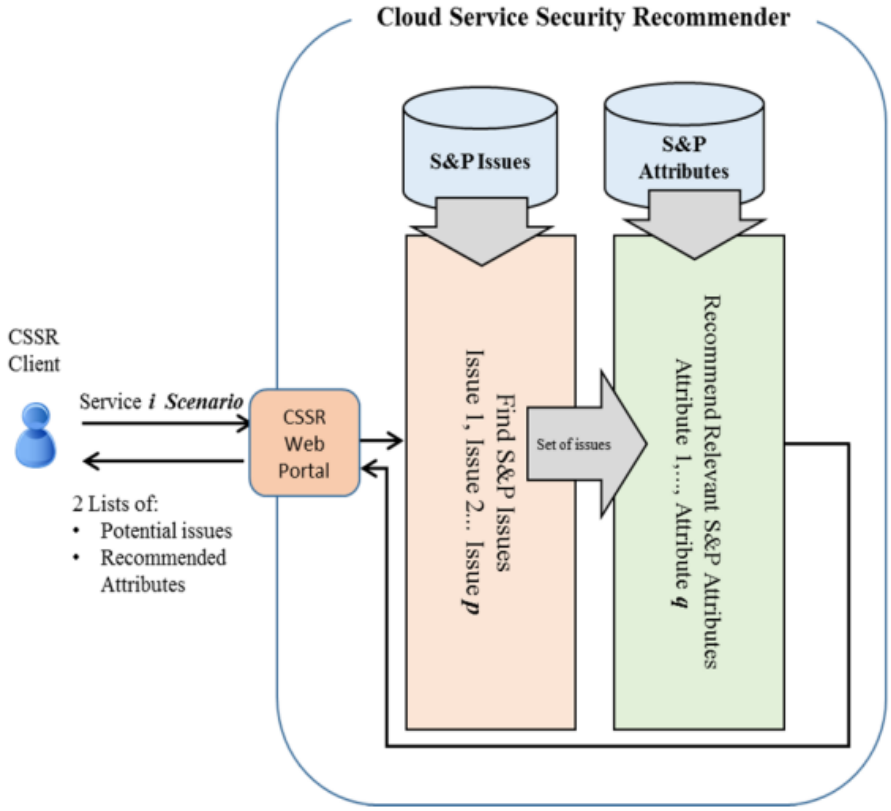


Рис. 1.6. Компоненти CSSR

Для з’ясування основних методів біометричної аутентифікації звернемося до проведеного дослідження двома професорами з Індії, а саме Махадева Картіка та М. Реваті [56].

Дослідники зазначають, що хмарні сервіси, станом на 2021 рік, стали нормою для сучасного світу, коли всі обчислення розпочинають мігрувати в хмару для забезпечення доступу до бізнес процесів компанії з будь-якої точки земної поверхні. Але, для того, щоб сервіси працювали без втручання зі сторони зловмисників, необхідно забезпечити безпечний доступ до хмарних служб за допомогою надійної аутентифікації, авторизації та отримання доступу до сервісів. Як вони зазначають, на сьогоднішній день використовуються такі засоби аутентифікації, як Kerberos, OAuth та OpenID. Це три основні протоколи для проведення аутентифікації та авторизації легітимних осіб до певного сервісу, що розташовується як в хмарні так і на локальних серверах бізнесу, тобто ці протоколи націлені саме на забезпечення

встановлення безпечного доступу між двома комунікативними об’єктами. Дані протоколи працюють за принципом, що за аутентифікацію відповідає віддалений сервер, що проводить автентифікацію користувача та сервер [56].

Головною проблемою в даних протоколах аутентифікації є те, що облікові дані користувачів зберігаються на сервері аутентифікації, і у випадку зламу бази даних серверу аутентифікації дані користувачів можуть бути викрадені та використані для несанкціонованого доступу до ресурсів нелегітимними користувачами. Тому, щоб підвищити рівень захищеності передачі даних між користувачами та серверами аутентифікації, а також захисту бази даних, використовується симетричне шифрування. Саме тому, в своїй роботі, дослідники представляють концепцію побудови безпечного спілкування між сторонами взаємодії із залученням одного із протоколів аутентифікації користувачів без необхідності попереднього завантаження жодної конфіденційної інформації сервера та користувача, що беруть участь в аутентифікації [56].

Як зазначають дослідники, протокол OAuth 2.0, це протокол делегування, що необхідний для передачі авторизаційних даних для веб-застосунків та протокол автоматизації API. На сьогоднішній день, даний протокол є досить поширеним та використовується великою кількістю розробників по всьому світу. Головною проблемою, якої припустилися більшість розробників по всьому світу було те, що даний протокол використовують як протокол аутентифікації. Це неправильно, оскільки OAuth 2.0 містить у собі компоненти для проведення аутентифікації сторін взаємодії, але не є протоколом аутентифікації. Тому можна зазначити, що в сучасному світі, розробники використовують лише один із компонентів даного протоколу [56].

Махадев Картік та М. Реваті у власному дослідженні представляють розроблений новий протокол для аутентифікації користувачів на основі використання біометричних даних для забезпечення безпечного доступу до віддаленого хмарного сервісу. У даному прикладі, дослідники розглядають біометричні дані користувача, як секретні дані користувача, які необхідно

захищати. Біометричні дані в даному випадку виступають як унікальні дані кожного користувача та дозволяють створити унікальний ключ для кожного користувача, забезпечуючи безпечне підключення до хмарного сервісу. У випадку, коли відбувається handshake між двома сторонами (клієнтом та сервером), створюється унікальний сесійний ключ, що базується на біометричних даних користувача та даними, отриманими із серверу аутентифікації. Тому, в даному випадку, відсутня будь-яка необхідність зберігати закритий ключ користувача і ключ сесії генерується унікальний для кожної сесії без отримання будь-якої попередньої інформації від користувача, що зменшує ризики його перехоплення каналами зв'язку [56].

В даній комунікації беруть участь лише три об'єкти: Власник даних (Data Owner), Хмарний сервер (Cloud Server) та Користувачі (Users) [56].

Власник даних одноразово завантажує власні біометричні дані на хмарний сервер. Для забезпечення безпеки власних персональних даних, він також присвоює біометричним даним цифровий підпис. Додатково, до завантаження біометричних даних, власних даних вказує назву, задає опис, здійснює їх перевірку та, за необхідності, він може видалити власні дані з ресурсів хмарного сервісу [56].

Хмарний сервер виступає в ролі місця, де зберігаються всі біометричні дані власників даних в шифрованому вигляді із заданим цифровим підписом. Даним сервером керує постачальник хмарних послуг та може мати змогу керувати ресурсами хмарного сервісу, та проводити його адміністрування. Має можливість лише переглядати власників біометричних даних та їх опис, без можливості переглянути вміст біометричних даних у відкритому вигляді [56].

Користувач в даному випадку виступає саме власником даних, що має доступ до консолі адміністрування власними біометричними даними, що дозволяє йому здійснювати їх аналіз, перевірку та видалення. Це необхідно для того, щоб, у випадку, якщо користувач проводить авторизацію на різноманітних хмарних сервісах, не вводим кожного разу власні дані та не

передавав біометричні дані, а лише скористався вже готовою парою шифрованих біометричних даних та цифровим підписом на іншому хмарному сервісу [56].

Для більш детального розуміння, можна переглянути Рис. 1.7, що архітектурно демонструє взаємодію даних об'єктів між собою та хмарним сервісом [56]:

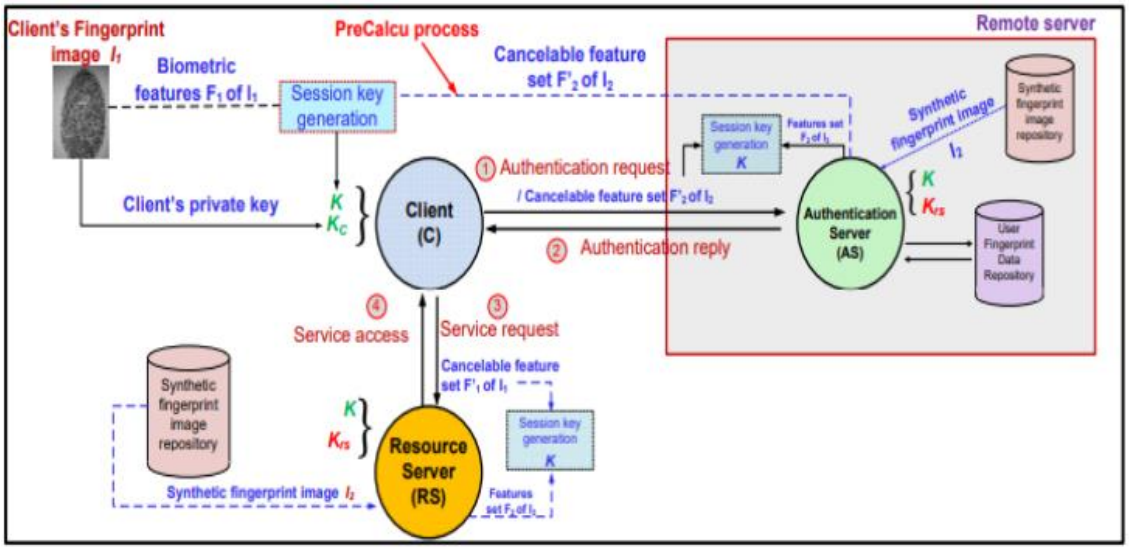


Рис. 1.7. Архітектура модель дослідників Махадева Картіка та М. Реваті

1.3. Сучасні технології розгортання хмарних сервісів

На сьогодні найперспективнішою технологією розгортання хмарних сервісів є контейнеризація. Враховуючи, що сучасний світ хмарних технологій є досить різноманітний і містить у собі величезну кількість різних технологій для надання користувачам та бізнесу послуг з розгортання власних бізнес-процесів на ресурсах CSPs, проте головною проблемою всіх CSPs є кількість фізичних ресурсів, які можна виділити під задачі клієнту та швидкість розгортання нового сервісу для підтримки діяльності процесів в працездатному стані. Саме тому розробники винайшли новітній спосіб переходу від складно розгортуваних систем на базі віртуальних машин, які необхідно кожного разу налаштовувати з «нуля» і підлаштовувати під роботу кожного окремого сервісу, і було розроблено технологію контейнеризації, що надає клієнтам та бізнесам гнучкість в розгортанні та дозволяє за декілька

хвилин розгорнути новий контейнер, і так само швидко вимкнути контейнер, щоб вивільнити фізичні ресурси під нові задачі [57].

Що таке «Контейнер»? Контейнер – це пакет додатку чи програмного забезпечення, що включає в себе всі необхідні компоненти та залежності, файли конфігурації, бібліотеки та всі інші необхідні компоненти, що необхідні для належного функціонування. Завдяки даній технології вирішується основна проблема під час міграції бізнес-процесів та додатків, що розміщуються на локальних обчислювальних ресурсах компанії на хмарні обчислювальні ресурси, що забезпечує можливість перенесення сервісу чи додатку за моделлю «As-Is», тобто «Як є». Завдяки технології контейнеризації, до відомих моделей розгортання, таких як IaaS / PaaS / SaaS, додається ще одна модель, що носить назву CaaS (Containers-as-a-Service). Дана технологія забезпечується лише за допомогою використання віртуальних середовищ та серверу управління, що також розміщується в межах контейнеру [57].

Основні переваги використання включають в себе можливість по простому розгортанню сервісу лише за «декілька натиснень клавіші миші» та містять [57]:

- **Портативність**. Додаток чи програмне забезпечення в контейнерах включають всі необхідні компоненти для розгортання. Дана портативність допомагає клієнтам та бізнесу запускати сервіси в приватних чи публічних середовищах [57].
- **Безпека**. Незалежність контейнерів та ризиків в прогалинах безпеки хмарних сервісів. У випадку, якщо додаток підпадає під атаку чи компрометацію зловмисниками, то контейнери залишаються неінфікованими, оскільки розташовуються в ізольованих середовищах сервісу [57].
- **Висока ефективність та економічність**. Контейнери запускаються на мінімальній кількості ресурсів в порівнянні з віртуальними машинами, оскільки вони не залежать від розгорнутої операційної системи. Додатково, контейнери споживають мінімальну кількість оперативної

пам’яті, що дозволяє бізнесу на доступних ресурсах розгортати більшу кількість сервісів [57].

- **Масштабованість**. Технологія контейнеризації дозволяє легко проводити масштабування через простоту розгортання та власний розмір. Для розгортання сервісу, достатньо лише вказати, яку ОС/сервіс необхідно завантажити, що є абсолютно безкоштовно та доступно для кожного [57].
- **Можливості**. Контейнери мають змогу генеруватися, розгортатися та вимикатися за секунди, оскільки вони не вимагають попереднього розгортання операційної системи. Дана функція дозволяє швидко налаштувати процес розробки, бізнес-процеси та розгорнути нову версію додатку за короткий проміжок часу [57].

Контейнери в загальному вигляді мають три фази впровадження в життєвий цикл компанії (Рис. 1.8):

- Створення, тестування та затвердження образу.
- Зберігання та пошук образів для контейнерів необхідних для розгортання сервісу.
- Розгортання та управління визначеними контейнерами [58].

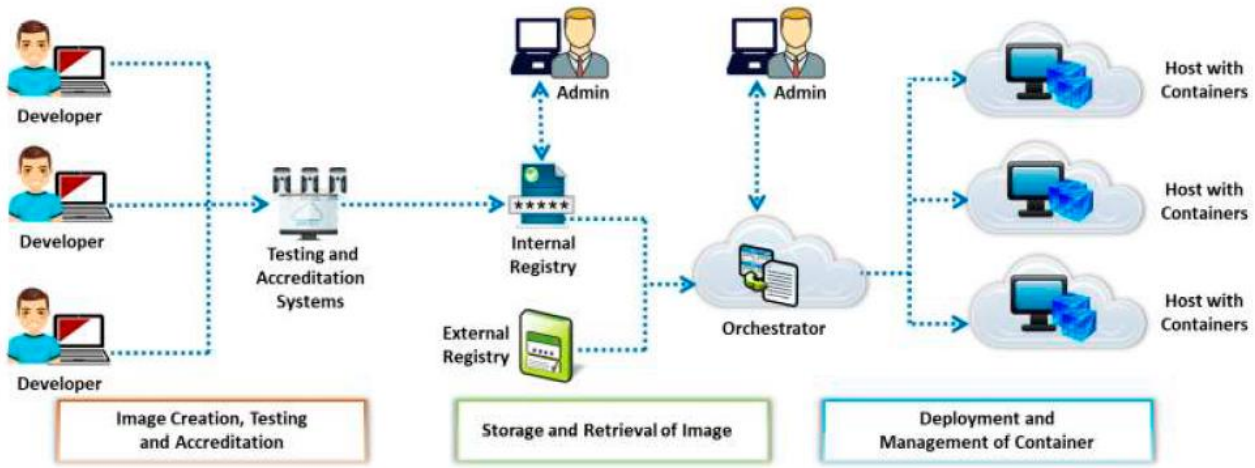


Рис. 1.8. Архітектура розгортання контейнерів

Порівнюючи середовище розгортання віртуальних машин та контейнеризації, варто враховувати те, що в основі сучасних хмарних сервісів лежить саме віртуалізація без розгортання окремого серверу під кожний

окремий сервіс. Завдяки такому підходу, є можливість заощадити місце в Datacenters та зменшити кількість використання обчислювальних ресурсів для забезпечення працездатності різноманітних сервісів. До середовищ віртуалізації відносять рішення від таких компаній, як: VMware vCloud Suite, VMware vSphere, VirtualBox, Microsoft Hyper-V, та інші [59].

Повертаючись до традиційних засобів віртуалізації, можна сказати, що для таких систем необхідно проводити оптимізацію хмарної IT інфраструктури. До недоліків даної інфраструктури можна віднести обсяги даної інфраструктури та ресурси необхідні для функціонування даних систем. Контейнери в свою чергу розміщуються на ресурсах фізичного серверу на базі однієї хостової операційної системи. За допомогою даної архітектури, на базі однієї ОС існує можливість розгортання декількох необхідних бізнес-процесів компанії без збільшення обсягів використовуваних обчислювальних ресурсів.

В Табл. 1.1 та на Рис. 1.9. представлено порівняння функціоналу віртуальних операційних систем та технології контейнеризації [59]:

Таблиця 1.1.

Порівняння можливостей віртуальних машин та контейнерів

Віртуальні машини	**Контейнери**
Займають багато місця	Займають мінімум місця з можливість plug-and-play
Запуск VM в межах незалежного віртуального середовища	Запуск контейнерів в межах єдиної операційної системи
Віртуалізація залежить від кількості фізичних ресурсів (CPU, RAM)	Віртуалізація залежить від операційної системи
Повільне розгортання ОС	Гнучкість в розгортанні контейнерів
Обмежена виробнича потужність	Виробнича потужність залежить лише від потужності серверу
Повноцінна ізоляція із повною захищеністю	Вибір рівня ізоляція із частковою захищеністю
Створення та запуск систем за хвилини	Створення та запуск контейнерів за секунди

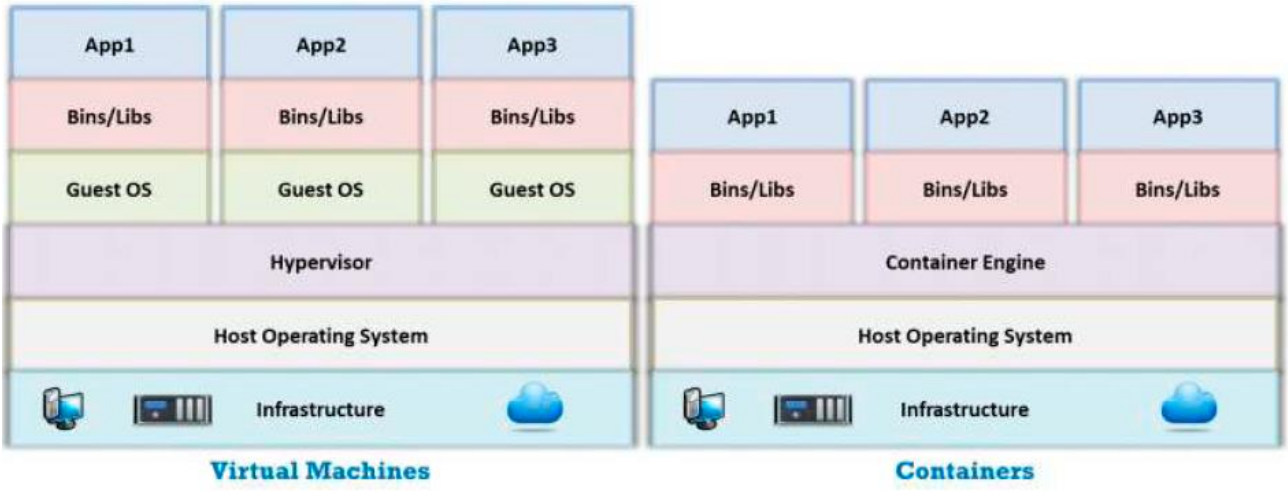


Рис. 1.9. Порівняння можливостей віртуальних машин та контейнерів

Основним рішенням, що забезпечує технологію контейнеризації, є рішенням під назвою Docker. Це програмний продукт з відкритим програмним кодом, що використовується для розробки, створення пакетів даних та швидкого запуску різних застосунків. Docker постачається як PaaS рішення, що розміщується на рівні ОС. В сучасному світі, більшість розробників використовують технологію контейнеризації для запуску власних додатків для уникнення необхідності розгортання повноцінної ОС для тестування повного функціоналу розроблюваного рішення [60].

Рішення Docker складається з декількох основних компонентів, що забезпечують його роботу, а саме [60]:

- **Docker Engine**. Це клієнт/серверний застосунок, що встановлюється на ПК, де планується розробка, збірка та запуск застосунків. В даному компоненті використовується такі модулі, як: сервер, командний рядок для клієнта та REST API [60].
- **Docker Swarm**. Це компонент, що забезпечує можливість управління декількома розгорнутими Docker рішеннями чи образами [60].
- **Docker Architecture**. Це компонент, що включає в себе повноцінну побудову технології контейнеризації на ресурсах розробника, що дозволяє розподіляти виконання процедур під час створення програмного продукту (Рис. 1.10) [60].

- **Docker Operations**. Це компонент, що включає в себе команди, необхідні для управління технологією контейнеризації. До них відносяться: створення контейнерів із Dockerfile, перегляд списку всіх завантажених образів, індивідуальне найменування кожного образу, отримання готового образу із реєстру образів, завантаження нового образу в реєстр та пошук необхідних образів у списку доступним [60].

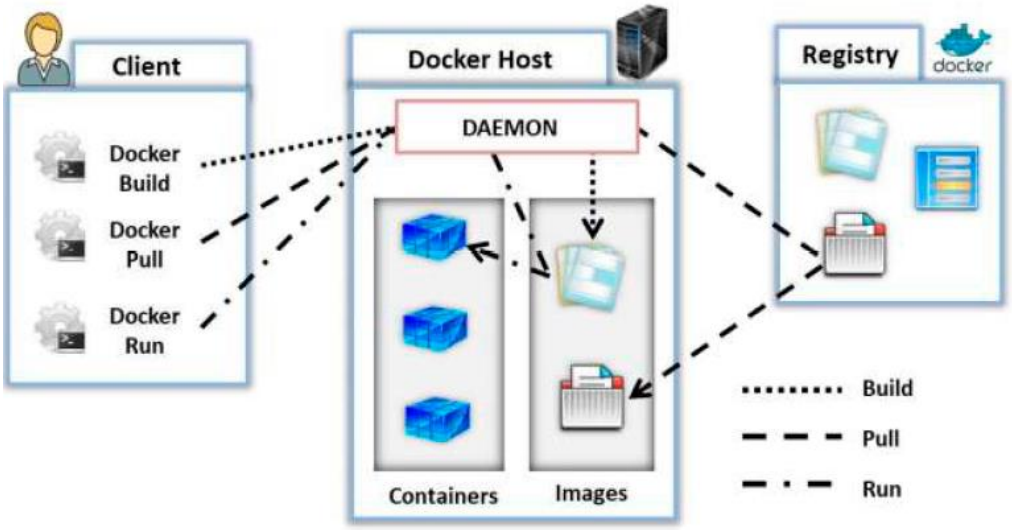


Рис. 1.10. Архітектура рішення Docker

Аналізуючи всі вище описані методи побудови технології контейнеризації у власній інфраструктурі компанії чи на ресурсах хмарних сервісах, і з достатньою захищеністю може здатися простою задачею для одного розгортання серверу, але управління великою кількістю сервісів контейнеризації може бути неможливою задачею. Саме тому, для управління декількома серверами контейнеризації та побудови відмовостійкої системи використовуються технології управління контейнерами чи «Container Orchestration» [61].

«Container Orchestration» – це процес із автоматизованим управлінням життєвого циклу роботи контейнерів та побудови динамічного середовища встановлення контейнерів із попередньо розгорнутим програмним забезпеченням [61].

За допомогою використання технології «Container Orchestration», вирішуються автоматично наступні задачі:

- Автоматичне збільшення кількості контейнерів [61].
- Автоматичне розгортання контейнерів за розкладом чи для підвищення продуктивності [61].
- Автоматичне налаштування кожного контейнеру на основі попередньо налаштованих політик [61].
- Постійний доступ до кожного контейнеру [61].
- Автоматичне забезпечення встановлених засобів безпеки для кожного контейнеру [61].
- Автоматична перевірка стану кожного із контейнерів для забезпечення безперервної роботи сервісу [61].
- Автоматичне забезпечення балансування навантаження на кожний контейнер в рамках одного розгорнутого додатку чи сервісу [61].
- Автоматичний перерозподіл ресурсів в залежності від потреб того чи іншого додатку чи сервісу [61].

На сьогоднішній день в світі використовуються три найпопулярніших сервіси для управління кластерами контейнерів або, іншими словами, забезпечення технології «Container Orchestration». До них відносять такі рішення, як: Docker Swarm, OpenShift та Kubernetes [61].

На сьогоднішній день найпопулярнішим із трьох вище описаних сервісів є саме Kubernetes. Дане рішення також відоме під іншою назвою – K8s. Рішення представлене у вигляді програмного продукту з відкритим кодом, є портативним та розроблене компанією Google для управління контейнерами для миттєвого розгортання розроблених програмних продуктів та мікросервісів для забезпечення діяльності затверджених бізнес процесів [62].

Рішення Kubernetes працює наступним чином:

1) За допомогою розробленого фреймворку, відбувається розповсюдження готових контейнерів для розгортання сервісів та додатків [62].
2) Потім на стороні Kubernetes відбувається створення необхідного набору конфігурацій для коректного розгортання контейнерів [62].

3) Відбувається розповсюдження файлів конфігурації на всі площадки, що підключені до Kubernetes, та здійснюється запуск розповсюдженого образу контейнерів [62].
4) Забезпечення відмовостійкості для всіх контейнерів, що обслуговують клієнтські запити та розташовані в різних Datacenters чи країнах [62].

Основні функції, що забезпечуються рішенням Kubernetes:

- **Доступність сервісу**. Дане рішення дозволяє доступ до сервісів на рівні DNS імені чи IP адреси [62].
- **Забезпечення відмовостійкості**. У випадку, як тільки один із контейнерів отримуємо критичну кількість запитів від користувачів, дане рішення розгортає новий контейнер та перенаправляє новий трафік від користувачів на даний контейнер [62].
- **Управління місцем**. Рішення дозволяє розробникам самостійно визначати місце, де буде відбуватися збереження контейнерів. Чи будуть це локальні ресурси, чи – хмарні ресурси провайдера, різниці немає, оскільки обидва типи управляються за допомогою Kubernetes та модулів, що розміщуються в місцях розташування кожного окремого розгортання Docker контейнерів [62].
- **Автоматичне розгортання та відновлення**. Рішення дозволяє в автоматичному режимі розгортати нові контейнери та, за необхідності, передавати фізичні ресурси із одного контейнера на інший, якому необхідно підвищити продуктивність [62].
- **Авто-відновлення**. Рішення дозволяє в автоматичному режимі виявляти відмову в роботі кожного окремого контейнеру та забезпечує можливість створення нових аналогічних контейнерів, щоб відновити роботу сервісу, що був недоступний та не забезпечував виконання затверджених бізнес процесів організації [62].
- **Управління безпекою та конфігураціями**. Рішення Kubernetes забезпечує можливістю користувачів керувати конфіденційними даними, такими як дані для входу в обліковий запис (логін та пароль),

паролі для входу на secure shell (SSH) чи токени для протоколу аутентифікації OAuth 2.0 [62].

Тому, як ми можемо спостерігати рішення від компанії Kubernetes при належному підході та проведення коректних налаштувань по автоматизації роботи із контейнерами забезпечує можливістю мінімізувати кількість рутинної роботи для адміністраторів систем контейнеризації, та допомогти автоматизувати процеси виявлення та відновлення роботи контейнерів, які по тим чи іншим причина перестали працювати належним чином [62].

Додатково, що оцінити масштаби розгортання рішення Kubernetes та зрозуміти, де мають розміщуватися основні компоненти рішення, пропонується розглянути Рис. 1.11, на якому представлено докладну архітектуру проаналізованого рішення [62]:

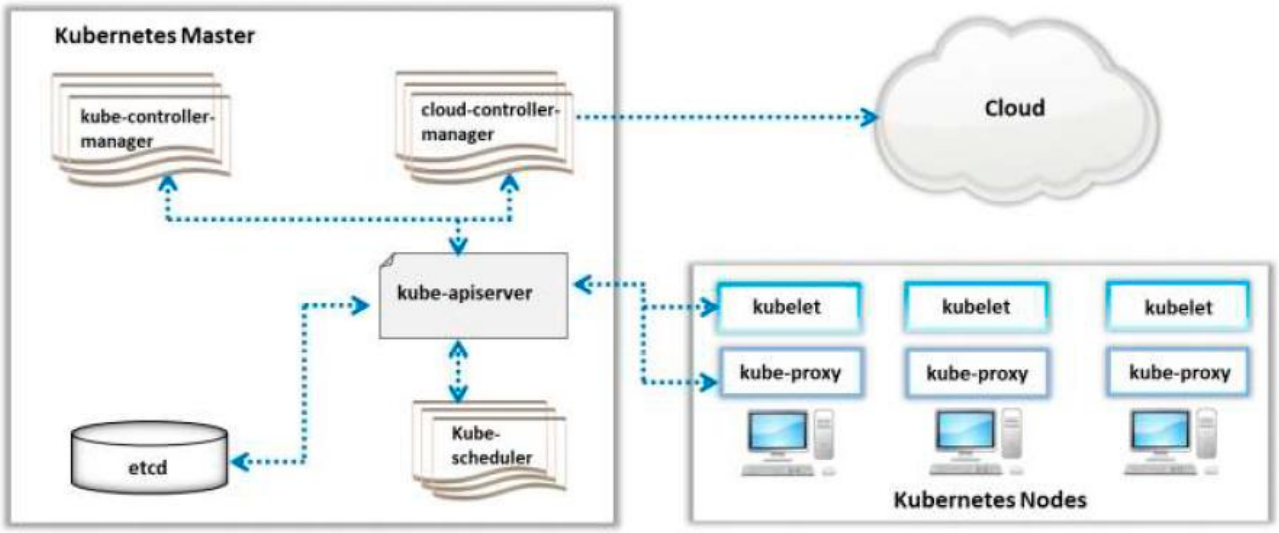


Рис. 1.11. Архітектурна складова рішення Kubernetes.

1.4. Вразливості хмарних сервісів та веб-ресурсів

Розпочинаючи говорити про вразливості та атаки, які виконуються на хмарні сервіси, слід пам’ятати, що в сучасному світі, зловмисники майже не користуються звичайними способами зламу користувацьких облікових записів чи серверів за допомогою Brute Force атаки, або методу підбору паролів. Методи викрадення облікових даних стали виразнішими і продуманими [63].

Першим із таких методів ми розглянемо можливо найпростіший варіант викрадення даних, який використовується до осіб, які є досить довірчими чи не знають основ захисту власних даних при користуванні інтернет ресурсами – це **Соціальна інженерія** [63].

При використанні даного типу атаки, зловмисник викрадає облікові дані в клієнтів чи CSPs завдяки застосування phishing-атак, підробки легітимних веб-сторінок та експлуатації знайдених вразливостей в серверній/клієнтській частині. В більшості випадків, в основі лежить принцип соціальної інженерії, коли персональні дані незаконним шляхом виманюються у власника чи тримача даних. Після отримання облікових даних, зловмисник має змогу отримати доступ до хмарних ресурсів та здійснити порушення їх конфіденційності, цілісності чи доступності [63].

Зловмисники для реалізації методу соціальної інженерії використовують прості засоби та підходи [63].

Наприклад, для викрадення банківських даних клієнта банку ПАТ «Приватбанк», зловмисник розроблює копію сторінки входу в next.privat24.ua і називає її next.prival24.ua, змінюючи лише одну букву в на другому рівні домену із privat24 на prival24. Візуально, для користувача, може здатися, що все вірно і сторінка правдива, але насправді, коли клієнт розпочне вводити дані на даному веб сайті, його копію облікових даних буде відправлено в базу даних зловмисника, а користувача буде перенаправлено на оригінальний веб сайт, де користувачу знову буде запропоновано ввести власні облікові дані [63].

Оскільки при використанні методу соціальної інженерії, існує безліч варіантів викрадення даних, рекомендується:

- Уважно перевіряти веб-сайти, які відвідуються [63].
- Нікому не передавати власні облікові дані, в тому числі рідним та близьким людям [63].
- Застосовувати технологію 2FA (two-factor authentication) або MFA (multi-factor-authentication) [63].

- Уважно перевіряти відправника листа в електронній пошті [63].
- Ніколи не авторизуватися при використанні публічних інтернет мереж [63].

При застосуванні даних п’яти рекомендацій на практиці, користувач має змогу мінімізувати ризик викрадення власних облікових даних [63].

До наступного популярного типу викрадання персональних даних користувачів відноситься атака, в якій зловмисник виступає сервером для клієнта, наприклад Google Drive чи Box, та має назву – **Man-in-the-Cloud (MITC)**.

Атака типу MITC – це удосконалена версія атаки Man-in-the-Middle, що дозволяє зловмисникам використовувати вразливості, що присутні в комунікаціях між двома об’єктами, територіально розділених між собою. Дана атака застосовується у той час, коли відбувається синхронізація даних користувача з хмарними сервісами, наприклад, Google Drive чи Box. В момент, коли відбувається синхронізація токену між клієнтом і сервером хмарного сервісу, зловмисник має можливість перехопити та обробити даний токен за лічені мілісекунди та відправити отримувачу, інакше даний токен буде змінено і потрібно буде робити все заново.

У випадку, якщо зловмисник встигає за лічені мілісекунди обробити токен, він отримує можливість дублювати у себе на локальному сервері всі дані, що синхронізуються між клієнтом та сервісом, наприклад, Google Drive чи Box. Єдиний нюанс, який потрібно виконати зловмиснику, це змусити клієнта завантажити на сервіс файл із виконуваним зловмисним кодом. Це навіть може бути текстовий файл із макросом.

Тому, щоб захиститися від даного типу атак, необхідно:

- В межах компанії використовувати шлюзи, які мають можливість відслідковувати атаки типу соціальної інженерії та здійснювати перевірку файлів, що відправляються на віддалений сервіс.
- Політиками сервісу встановити час дії токену синхронізації, щоб попередити перехоплення трафіку.

- Використовувати антивірусне програмне забезпечення, що матиме змогу виявити зловмисне програмне забезпечення в файлах, що будуть синхронізуватися на хмарний сервіс.
- Використовувати Хмарні брокери (CASB) для перевірки трафіку між користувачами і хмарними сервісами.
- Впроваджувати шифрування файлів, що зберігаються на ресурсах хмарних сервісів.
- Використовувати 2FA чи MFA при вході на хмарний сервіс та для отримання токену синхронізації.

При використанні хоча б частини із вище наданих рекомендацій, компанія чи клієнт хмарних сервісів матиме змогу попередити викрадення власних персональних даних та отримає можливість виявити зловмисника в момент синхронізації даних [64].

Але, якими б не були нові типи атак, минулі все ж лишаються. Нижче можемо навести приклад із дев'яти типах атак, що користуються популярністю серед усіх зловмисників, які розпочинають шукати вразливості в хмарних сервісах, перед тим як застосовувати більш складні і продумані атаки, що потребують величезних знань та умінь.

1) Перший тип атаки має назву – **Session Hijacking using XSS Attack**. При даному типі атаки, зловмисник впроваджує XSS в викрадені cookie-файли, що використовуються в процесі аутентифікації користувача. За допомогою даного XSS зловмисний код впроваджується в веб-сторінку, що доступна користувачеві та використовується для відображення даних, отриманих із серверу. Використовуючи викрадені cookie-файли, зловмисник має змогу скомпрометувати активну сесію користувача, перехоплювати конфіденційні дані та змінювати їх, порушуючи їх цілісність.

   Для попередження даного типу атак, рекомендується використовувати SSL (secure socket layers) шифрування, мережеві екрани перед користувачами та серверами веб-сервісів, антивірусне програмне

забезпечення та сканери відкритого коду для виявлення вразливостей [65].

2) Другий тип атаки має назву – **Session Hijacking using Session Riding**. Зловмисник впроваджує в веб-сайт XSS запит для передачі неавторизованих команд. В активній сесії користувача, зловмисник відправляє електронний лист та підводить користувача до відвідування зловмисної веб-сторінки, що виглядає як справжній веб-сайт. В той час, коли користувач натискає на посилання на зловмисному веб-сайті, запити на веб-сайті виконуються для видалення даних користувача, перехоплення конфіденційних даних, відправки повідомлення на зміну пароля і т.д.

   Для того, щоб попередити виконання даної атаки, рекомендується не дозволяти браузерам чи веб-сайтам зберігати дані про логіни і паролі [66].

3) Третій тип атаки має назву – **Domain Name System (DNS) Attacks**. DNS-сервера працюють таким чином, що веб-сайт надається користувачів у зручному для запам’ятовування вигляді (наприклад, apple.com), а сервери перетворюють даний запит в вигляд IPv4 адреси, типу X.X.X.X, де X це цифра не більше 255, - та відправляє на сервер запит. Бувають такі типи DNS атак:
   - DNS Poisoning.
   - Cybersquatting.
   - Domain Hijacking.
   - Domain Snipping.

   Як працює DNS атака, можна описати на прикладі. Зловмисник, при відслідковуванні запитів користувачів, має можливість перехвату пакетів даних та перенаправити користувача на зловмисний веб-сайт, і вся комунікація користувача із веб-сервером, буде відбуватися через зловмисний веб-сайт. Це працює таким чином, що зловмисник блокує

відповіді від хмарного веб-сервісу до користувача на рівні DNS і відправляє видозмінені відповіді користувачу із власного серверу.

Саме тому, щоб попередити даний тип атаки, рекомендується використовувати технологію DNSSEC (domain name system security extensions), щоб побудувати захищений тунель між користувачем і DNS сервером, що, зловмисник не mad змоги відслідкувати DNS запит користувача до хмарного веб-сервісу і попередити його блокування та видозмінення [67].

4) Четвертий тип атаки має назву – **SQL Injection Attack**. Даний тип атаки в сучасному інформаційному світі завдає найбільше збитків по витоку персональних даних клієнтів чи користувачів інтернет послуг, що використовують логін та пароль для входу на публічні ресурси.

   Мова програмування, що використовується для здійснення запитів в базу даних має назву SQL. При здійсненні атаки даного типу, зловмисники користуються запитами, даної мови програмування та мають змогу отримати необхідну таблицю чи дані через відсутність перевірок запитів, що передаються від клієнта до серверу, та через наявні незакриті вразливості у системах управління базами даних. Атаку типу «SQL ін’єкції» найпростіше застосувати до сервісу, що використовує динамічні запити SQL запити в базу даних, що генеруються в процесі роботи користувача. Прикладом, де даний тип атаки можна зробити, це інтернет магазини та створення динамічної добірки товарів, які користувач прагне відобразити на екрані. У випадку отримання зловмисником доступу до бази даних, він має змогу маніпулювати даних в таблицях, змінювати чи видаляти їх, відправляти віддалені команди на сервер, на якому запущено базу даних чи навіть здійснювати управління веб-сервером, до якого підключено дану базу даних, що може потягти за собою компрометацію конфіденційних даних користувачів.

Для того, що попередити виконання даного типу атак з боку зловмисників та попередити витік конфіденційних даних за межі бази даних, необхідно: здійснювати перевірку даних, що вводяться користувачами; дозволяти введення тільки визначених форматів чи типів даних, щоб уникнути виконання зловмисного запиту; своєчасно здійснювати оновлення серверів та застосунків; проводити моніторинг баз даних тощо [68].

5) П’ятий тип атаки має назву – **Cryptanalysis Attacks**. Є не поодинокі випадки, що в хмарних сервісах взагалі не використовується шифрування або використовується слабкий захист, що робить вразливим хмарний сервіс та надає змогу проводити критоаналіз захищеності, що може бути сприятливим до проведення Bruteforce атаки, або атаки методом підбору. Для забезпечення захищеності даних від зловмисників чи нелегітимних користувачів, дані мають зберігатися в шифрованому вигляді, та розшифровуватися лише унікальним ідентифікатором кожного окремого користувача хмарним сервісом. Але, в будь-якому випадку, кожний алгоритм шифрування має свої недоліки та вразливості, що закриваються декілька шляхами, це збільшенням довжини ключа або удосконаленням програмного коду, що здійснює шифрування/дешифрування даних користувачів.

   Саме тому, щоб попередити експлуатацію даного типу вразливості в хмарних сервісам та бізнес-процесах компанії, рекомендується: використовувати унікальний набір для створення ключів доступу до управління хмарними сервісами (SSH) із мінімальною кількістю символів в 16 елементів; не уникати використання криптографічних алгоритмів і використовувати поєднання симетричної та асиметричної криптографії для з’єднання між клієнтом та сервісом [69].

6) Шостий тип атаки має назву – **DoS & DDoS Attacks**. Кожний хмарний сервіс розрахований на певну кількість клієнтів 1000/100000/10000000, але при досягненні умовної відмітки, сервіс розпочинає не справлятися

з трафіком, що на нього надходить і розпочинаються затримки у відповідях клієнтів. В звичайний період часу, сервіс з легкістю справляється із піковими завантаженостями, що створюють клієнти, але інколи трапляються випадки, що цілеспрямовано виводять із строю сервіси. Як тільки на службах моніторингу з'являється скачок трафіку в 2-3 рази, то це безумовно проводиться кібератака. Дана атака має назву DoS або DDoS. Даний тип атаки проводиться без доступу до сервісів через використання облікових даних користувачів. Кожний хмарний сервіс споживає певну кількість CPU / RAM / Storage / Bandwidth, але дані ресурси в більшості випадку виділяються для опрацювання запитів від клієнтів в пікових навантаженнях, але при здійсненні DoS / DDoS атаки, зловмисник генерує велику кількість запитів із одного чи декількох пристроїв із різних точко світу, що створює навантаження на сервери і може призвести до збоїв чи відмови в обслуговуванні сервісу. Різниця між DoS та DDoS атаками полягає в тому, що DoS завжди здійснюється з одного пристрою, але коли DoS атака відбувається одночасно із декількох пристроїв (так званої botnet мережі), даний тип атаки вже має назву DDoS. Для того, що попередити виникнення додаткового навантаження на хмарні сервіси обробки даних та відмови в обслуговуванні, рекомендується використовувати IDS системи на периметрі мережі компанії, де розташовується сервер обробки даних сервісу та встановлювати між користувачами та серверами рішень для виявлення та блокування DoS/DDoS атак [70].

7) Сьомий тип атаки має назву – **Man-in-the-Browser Attack**. Даний тип атаки має принцип використання вразливостей браузеру користувача та його експлуатацію. Зловмисник впроваджує зловмисний код або бот в браузер користувача, що перехоплює будь-який трафік, що передається між користувацьким ПК та сервером веб-сервісу. Дане впровадження дозволяє зловмиснику перехоплювати користувацькі

облікові дані, конфіденційні дані, де в подальшому зловмисник отримає змогу несанкціонованого віддаленого доступу до серверу та отримання даних інших користувачів, чи навіть компрометації роботи веб-серверу. Для того, що попередити експлуатацію даного типу вразливості, рекомендується на стороні веб-серверу впроваджувати рішення для виявлення аномальної діяльності користувачів та, при використанні веб-серверів для внутрішніх користувачів компанії, обмежувати доступ через використання захищеного VPN каналу [71].

8) Восьмий тип атаки має назву – **Metadata Spoofing Attack**. На сьогоднішній день, всі хмарні сервіси збирають дані про користувачів, а саме їх місце розташування, потужності пристрою користувача та інші дані. Процес підробки метаданих користувача, це підміна чи заміна метаданих, що зберігаються в WSDL файлі, де міститься інформація про користувача та хеші логінів/паролів. При виконанням зловмисником підміни метаданих, він має змогу здійснити перенаправлення користувача із легітимною веб-сторінки на зловмисну, що допоможе йому змусити користувача ввести конфіденційні дані та викрасти їх, в тому числі й дані банківських карт. Для того, що попередити експлуатацію даного типу вразливості, рекомендується забезпечувати шифрування метаданих і збереження їх на хмарних ресурсах, а також впроваджувати технології перевірки хешів файлів, що надходять [72].
9) Дев’ятий тип атаки має назву – **Cloud Malware Injection Attack**. Як відомо, в мережі інтернет відсутній жодний веб-сайт, що немає жодної вразливості. Саме тому, більшість зловмисників намагаються знайти все нові й нові zero-day вразливості, що допоможуть їм отримати нелегітимний доступ до конфіденційних даних, що зберігаються на серверах хмарного веб-сервісу чи перехопити дані. Даний тип атаки працює таким чином, що зловмисник за допомогою експлуатації знайденої вразливості на веб-сервері, має можливість впровадити

власний зловмисний код. Дане впровадження може змусити сервіс при вході користувача на легітимний сайт перенаправити користувача на зловмисний веб-сайт, де користувачу необхідно буде ввести авторизаційні дані чи дані карти для продовження, що може потягти за собою витік конфіденційних даних користувачів та порушити репутацію веб сервісу. Для того, що попередити експлуатацію даного типу вразливості, рекомендується використовувати рішення для перевірки безпечного написання коду при статичному аналізі та здійснення динамічного аналізу при розгорнутому веб-сервісі [73].

В сучасному інформаційному просторі, для простоти розуміння кожного типу вразливості та співставлення з поточною атакою, використовується декілька сервісів, що допомагають спеціалістам з кібербезпеки оцінювати потенційний ризик зламу сервісу. До даних сервісів відносять рейтинг OWASP Top 10, матриці MITTRE ATT&ACK, NIST тощо [74].

Наприклад, при сканування відкритого коду веб-додатку, DevSecOps інженер в першу чергу порівнює знайдені вразливості із рейтингом OWASP Top 10, що представлений на Рис. 1.12. З кожним роком даний список змінюється, сортується та додаються/вибувають типи вразливостей, що найчастіше використовуються зловмисниками, тому даний список є завжди актуальним, оскільки він опирається на результати досліджень світовий спільнот дослідників та зловмисників [74].

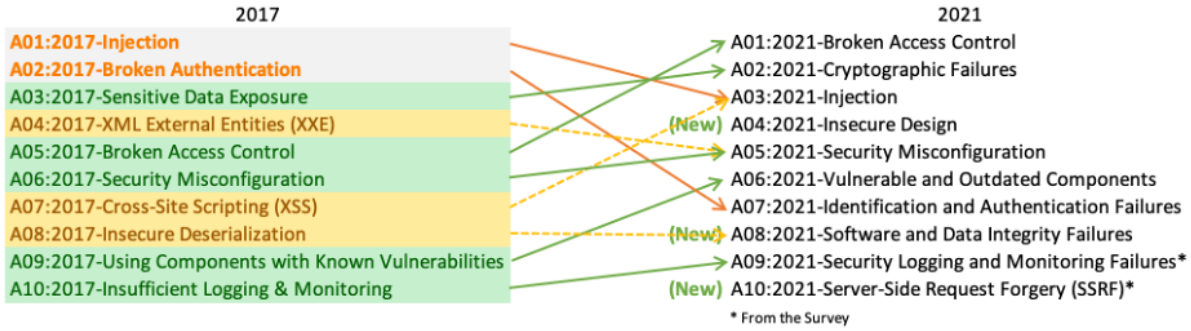


Рис. 1.12. Рейтинг найпопулярніших вразливостей за версією OWASP Top 10

Але, як би там не було і які б не були рейтинги, кожна компанія визначає пріоритетність виявлених ризиків на власний розсуд та може бути впевнена,

що визначений список вразливостей може закриватися рішеннями, що розташовані до веб-сервісів, такі як Web Application Firewall [75].

Як відомо, з мережевої архітектури існує сім рівнів моделі OSI, де кожний з них має свою назву, то в сфері кіберзахисту також використовується аналогічний підхід до визначення рішення, що дозволяє чітко визначити якого саме рішення не вистачає в інфраструктурі компанії, що покрити виявлений вектор витоку конфіденційних даних (Табл. 1.2) [75]:

Таблиця 1.2.

Покриття рішеннями з безпеки кожного вектору загроз

Рівень захищеності	**Рішення, що забезпечують безпеку**
1. Прикладний	Використання в компанії SDLC, впровадження сканерів вразливостей та сканерів вихідного коду, використання Web Application Firewall.
2. Інформаційний	Впровадження рішень для попередження витоку даних (DLP), постійний моніторинг діяльності баз даних, впровадження шифрування даних.
3. Управлінський	Визначення рівня доступу для користувачів, управління виявленими вразливостями, сканування та встановлення оновлень на впроваджені системи, перевірка встановлених конфігурацій та забезпечення постійного моніторингу розгорнутих рішень через SIEM систему.
4. Мережевий	Впровадження технологій попередження (IDS) та виявлення (IPS) вторгнень на рівні мережі, встановлення периметрових мережевих екранів, розгортання технологій протидії DDoS, забезпечення безпеки DNS та впровадження технологій MFA.
5. Довірених пристроїв	Постійний моніторинг пристроїв, що використовуються на периметрі мережі компанії (NAC)

Рівень захищеності	Рішення, що забезпечують безпеку
6. Обчислення та зберігання	Впровадження технологій попередження (IDS) та виявлення (IPS) вторгнень на рівні користувача, розгортання мережевих екранів на рівні користувача (Host Firewall), маскування та шифрування конфіденційних даних.
7. Фізичний	Забезпечення фізичної безпеки заводу, встановлення камер безпеки тощо.

Вище представлену таблицю, можна вважати деяких ідеалом для спеціалістів з інформаційної безпеки, щоб упевнитися, що компанії, в якої впроваджується кіберзахист повністю може відповідати міжнародних вимог та мати можливість успішно пройти сертифікацію міжнародного стандарту захищеності компанії – ISO 27001 [75].

1.5. Особливості застосування хмарних сервісів у державних структурах України

Говорячи про поєднання хмарних технологій та державного сектору завжди викликало хвилю емоцій у всіх представників державних установ, таких як Служби безпеки України, Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України та інших служб. Дана стурбованість була викликана тип, що дані державних структур в більшості становлять конфіденційні дані про внутрішню побудову та структуру діяльності держави та розкриття інформації про потенційні вразливі місця, в поточній інфраструктурі, що може потягти за собою експлуатацію даних місць, у випадку зламу хмарних сервісів зловмисниками [76].

До 2019 року керівництво держави Україна було проти впровадження хмарних ресурсів та їх використання для обслуговування діяльності ресурсів держави за межами країни, навіть на ресурсах локальних провайдерів зв'язку, типу «Denovo», через вище описані проблеми із витоком і викраденням даних з ресурсів хмарних сервісів [77].

Через дану затримку із прийняттям хмарних сервісів на баланс користування і впровадження в держаний сектор, в країні виникла затримка із формуванням списку об'єктів критичної інфраструктури, через що до кінця 2021 року, не було чіткого визначання, що саме в Україні вважається об'єктом критичної інфраструктури та, які об'єкти інфраструктури країни потрібно захищати в першу чергу [77].

Тільки, розпочинаючи з 2019 року, Міністерством цифрової трансформації України було запущено процес і намагання запровадити легітимність використання хмарних ресурсів, сервісів та обчислень, для перенесення на них потужностей сервісів, що розміщуються на наземних Datacenters, які вже застарілі і потребують постійної модернізації та обслуговування. Саме тому, в даному році було сформовано Пояснювальну записку до проекту Закону «Про хмарні послуги». Даним законопроекту Міністерством цифрової трансформації України запланувало офіційно врегулювати вимоги, яким повинні відповідати хмарні сервіси, що мають бути допущені до використання в Україні і мати змогу обробляти конфіденційну інформацію, що циркулює на локальних ресурсах Центрів обробки даних різних міністерств. Також, завдяки впровадженню даного закону, планувалося врегулювання питання корупції при проведенні тендерних закупівель серверного обладнання та уникнути маніпуляцій і завищенні цін локальними постачальними фізичного обладнання для держаних центрів обробки даних [78].

2020 рік був досить насиченим на події і однієї з них було зібрання саміту під назвою «Цифрова трансформація в Україні: як державному сектору прискорити перехід до моделі хмарних сервісів», що все ж дозволити державним структурам розпочати використовувати хмарні сервіси та обчислювальні потужності для уникнення величезних грошових витрат для утримання фізичних ресурсів в актуальному стані. В даному саміті взяли участь такі структури, такі як: Верховна Рада Комітету Цифрової

Трансформації, Державна Служба Спеціального Зв'язку та Захисту Інформації, Державне підприємство Дія та інші [79].

Як зазначалося на даному саміті, то хмарні сервіси є досить поширеною практикою в сучасному розвиненому економічному просторі, що допомагає покривати велику частину бізнес потреб, заощаджуючи кошти бізнес на утримання локальних обчислювальних ресурсів та місць розташування Datacenters [79].

Також, під час даного саміту було вказано, що завдяки застосуванню та урегулюванню використання хмарних обчислювальних в державному секторі допоможе на державному рівні здійснити цифрову трансформацію та зміну поглядів в розгортання веб-ресурсів, не на ресурсах локальних обчислювальних пристроях, а в повністю оформлених центрах обробки даних [79].

Завдяки такому переходу на використання хмарних ресурсів, сервіси будуть мати кращу захищеність завдяки наявності в провайдера новітніх систем захисту, постійну безперервну функціонуючу інфраструктуру, що здатна витримати не одну кібератаку, в тому числі й націлену DDoS атаку на критичну інфраструктуру держави [79].

Розпочинаючи з лютого 2022 року Міністерство цифрової трансформації України разом із Верховною радою на загальному голосуванні було прийнято законопроект від номером 2655 що має назву «Законопроект про хмарні послуги» [80].

Головним посилом Міністерства цифрової трансформації України було впровадження принципи Cloud First, для зниження корупційних схем при проведенні тендерів на закупівлях On-Premise обладнання для локальних центрів обробки даних. Як зазначається в даному законопроекті, перехід на використання хмарних обчислень дозволить Україні щорічно заощаджувати близько декількох мільярдів гривен на утримання та обслуговуванні локальних обчислювальних ресурсів в центрах обробки даних користувачів та сервісів, що опубліковані в мережі Інтернет [80].

То чому ж використання хмарних обчислень вигідніше в порівнянні з локальними обчисленнями [81]?

До переваг використання Хмарних обчислень можна віднести:

- Доступ в будь-який час і з будь-якого місця [81].
- Грошова вигода у використанні [81].
- Статична щомісячна/щорічна вартість послуг [81].
- Уникнення проблем із стабілізацією роботи обчислювальних потужностей [81].
- Високий рівень забезпечення безпеки даних [81].
- Можливість миттєвого розгортання [81].
- Уникнення витрат на живлення ЦОДів [81].

До недоліків використання Хмарних обчислень можна віднести:

- Можливість нестабільного мережевого зв’язку [81].
- Підписання на довгострокові витрати [81].
- Мінімальне втручання в доналаштування роботи орендованих сервісів [81].

Також, необхідно описати переваги використання Локальних обчислень:

- Загальна вартість володіння фізичними ресурсами та серверами [81].
- Здійснення повноцінного контролю за розгорнутою інфраструктурою [81].
- Максимальна безперервність роботи сервісів [81].

До недоліків використання Локальних обчислень, можна віднести:

- Великі початкові витрати на розгортання ЦОДів [81].
- Необхідний персонал для забезпечення технічного обслуговування [81].
- Складність при впровадженні в поточну інфраструктуру [81].

Для кращого представлення і розуміння основних переваг і недоліків використання Хмарних та Локальних обчислень, сформовано Табл. 1.3, що дозволяє об’єктивно оцінити можливості пропонованих розгортань [82]:

Таблиця 1.3.

Порівняння можливостей Хмарних та Локальних обчислень

Критерій	**Хмарні обчислення (Cloud Computing)**	**Локальні обчислення (On-Premise Computing)**
Отримання доступу з будь-якої точки земної поверхні	+	-
Збільшення кількості необхідних ресурсів за декілька хвилин	+	-
Миттєвий перерозподіл ресурсів	+	-
Забезпечення постійної відмовостійкості розгорнутих сервісів	+	+
Щорічна фіксована плата за послуги	+	-
Відсутність необхідності оплати за фізичне розміщення серверного обладнання	+	-
Відсутність мережі Інтернет	-	+
Децентралізація розміщених сервісів	+	-
Швидкість реакції на запит користувача	+	+

Критерій	**Хмарні обчислення (Cloud Computing)**	**Локальні обчислення (On-Premise Computing)**
Стабільність сервісів при ретроспективному аналізі	+	-
Забезпечення надійної захищеності розміщених сервісів	+	+
Забезпечення миттєвого відновлення сервісу, що відмовив у обслуговуванні	+	+
Миттєва реакція розробка серверного обладнання	+	-
Наявність інтегрованих засобів та сервісів для організації захищеного доступу	+	-
Кластеризація розміщення сервісів по різних точкам земної поверхні	+	-
Загальна вартість володіння всіма розгорнутими сервісами	-	+

Висновок до розділу 1

Проведено дослідження базових понять хмарних сервісів, що найбільш широко використовуються в інформаційних просторах України та світу використання яких набуло набільшого поширення саме напочатку 21 століття після 2011 року, коли компанія Amazon розпочала надавати власні послуги для компаній по розробці рішень, що були розгорнуті в хмарі.

Проведені міжнародні дослідження дали можливість визначити основні критерії оцінювання продуктивності хмарних сервісів, що використовуються постачальниками хмарних сервісів. Проте дані критерії не дозволяють повноцінно провести оцінювання кіберзахисту хмарних сервісів, оскільки вони не включають в себе достатній набір параметрів, що здатний охопити повний набір компонентів, які використовуються для забезпечення роботи хмарних сервісів.

Досліджено технологію хмарних сервісів – виділеної технології контейнеризації, що найбільш перспективно та широко використовується для розгортання хмарних сервісів за рахунок чого кількість використовуваних обчислювальних ресурсів зменшується в рази, тим самим зберігаючи свою продуктивність та відповідний рівень кіберзахисту хмарних сервісів.

Досліджено вразливості хмарних сервісів та веб-ресурсів, які незалежно від рівня діяльності компанії постійно проявляються через людську похибку при написанні програмного забезпечення чи проведенні некоректних налаштувань систем безпеки.

В процесі проведеного аналізу дійшли висновку, що існуючі хмарні сервіси мають ряд вразливостей та недоліків з точки зору кіберзахисту, які не дозволяють вирішувати задачі захищеного зберігання даних на таких сервісах. Саме тому, для вирішення даних задач прийнято рішення, щодо розробки власної унікальної системи оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

РОЗДІЛ 2. МЕТОД, МОДЕЛЬ ТА СИСТЕМА ОЦІНЮВАННЯ КІБЕРЗАХИСТУ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

2.1. Математична модель захищеного застосунку оцінювання кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури

Основною метою кожного хмарного провайдера – є забезпечення своїх клієнтів якісним сервісом та доступності власних систем, що використовуються клієнтами та компаніями для розміщення персональних бізнес сервісів чи процесів, що є ключовими для діяльності бізнесу та відіграють значну роль у життєдіяльності бізнесу. Проте, якщо постачальник хмарних сервісів недостатньо забезпечив захищеність даних чи сервісів з точки зору кіберзахисту, що останній постачає своїм клієнтам – дані клієнтів чи компаній потенційно можуть зазнати значних втрат через відсутність, наприклад, створення резервних копій, як даних так і віртуальних машин в цілому, що напряму впливає на відмовостійкість бізнес процесів та сервісів компаній, що впливають на функціональність компаній та забезпечення її безперебійної роботи [107, 97].

Саме тому, було прийнято рішення розробити «check-list», що містить більше 120 запитань із передбачуваними варіантами відповідей, що здатні забезпечити комплексну оцінку стану захищеності сервісів, віртуальних машин, консолі управління, що постачаються хмарним провайдером. Даний «check-list» створений у вигляді математичної моделі, що має за основу кортежний підхід та представляє собою комплексний опис параметрів оцінки будь-якого із існуючих хмарних сервісів [101].

Задля представлення повноцінного опису розробленої математичної моделі, розпочнемо з узагальненого представлення математичної моделі, що містить в собі перелік необхідних параметрів оцінки, представлених відповідей на параметри та рекомендації, щодо кожного із параметрів оцінки. Важливо розуміти, що від точності проведеного аудиту безпекових

налаштувань використовуваного хмарного сервісу залежить захищеність даних та точність надання рекомендацій для підвищення захищеності додатків, що функціонують в хмарі. Саме тому, для проведення якісної та комплексної оцінки стану захищеності різного роду хмарних сервісів було розроблено математичну модель, що складається з 11 параметрів кортежу, та описує ключові моменти, що містять в собі набір питань та рекомендацій, які застосовуються до таких типів хмарних сервісів, як: IaaS, CaaS, PaaS, FaaS та SaaS. Для побудови узагальненої математичної моделі було використано позначення «**CSP**», що розшифровується, як «**Cloud Service Provider**», та означає «**Постачальник хмарних сервісів**» [101, 103].

Узагальнена математична модель у вигляді кортежної моделі має наступний вигляд:

$$\boldsymbol{CSP} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{CSP}_i \right\} = \left\{ \boldsymbol{CSP}_1, \boldsymbol{CSP}_2 ..., \boldsymbol{CSP}_n \right\}, \tag{2.1}$$

де $\boldsymbol{CSP_i} \subseteq \boldsymbol{CSP}$ $(i = \overline{1,n})$ – ключовий компонент кортежної моделі характеристик, що демонструє *i*-й ідентифікатор параметра оцінки хмарних сервісів, *n* – їх кількість [108].

Наприклад, при *n* = 11, кортежна модель для узагальненої математичної моделі (2.1) буде виглядати наступним чином:

$$\boldsymbol{CSP} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{CSP}_i \right\} = \left\{ \boldsymbol{CSP}_1, \boldsymbol{CSP}_2, \boldsymbol{CSP}_3, ..., \boldsymbol{CSP}_7, ..., \boldsymbol{CSP}_{11} \right\} = \left\{ \boldsymbol{GP, N, S, SR, V, OS, CT, R, A, D, RE} \right\}, \tag{2.2}$$

де: $\boldsymbol{CSP}_1 = \boldsymbol{GP} = \text{"}\boldsymbol{General\ Points\ module}\text{"}$ – модуль, що визначає тип хмарного сервісу, його назву та перевірку діяльності з країнами-агресорами, $\boldsymbol{CSP}_2 = \boldsymbol{N} = \text{"}\boldsymbol{Network\ module}\text{"}$ – модуль, що оцінює мережеву частину хмарного сервісу на предмет захищеності та здатності протидіяти відомим загрозам, $\boldsymbol{CSP}_3 = \boldsymbol{S} = \text{"}\boldsymbol{Storage\ module}\text{"}$ – модуль, що оцінює частину, яка відповідає за зберігання конфіденційних даних компанії-замовника, $\boldsymbol{CSP}_4 = \boldsymbol{SR} = \text{"}\boldsymbol{Server\ module}\text{"}$ – модуль, що оцінює серверну або апаратну частину хмарного сервісу, що забезпечує функціонування VPS/VDS серверів,

що здійснюють обробку конфіденційних даних компанії-замовника, $CSP_5 = V =$ "***Virtualization module***" – модуль, що оцінює стан захищеності системи віртуалізації хмарного сервісу, $CSP_6 = OS =$ "***Operation System module***" – модуль, що оцінює стан захищеності операційних систем, що розгорнуті на ресурсах хмарного сервісу та обробляють конфіденційні дані компаній-замовників, $CSP_7 = CT =$ "***Container Technology module***" – модуль, оцінює стан захищеності середовища розгорнутих контейнерів, що використовуються для забезпечення працездатності сервісів компанії-замовника, $CSP_8 = R =$ "***Runtime module***" – модуль, перевіряє наявність систем логування подій, виявлення аномалій, вразливостей та перевірку працездатності всіх сервісів, використовуваних компанією-замовником, $CSP_9 = A =$ "***Application module***" – модуль, що перевіряє стан захищеності додатків, що постачаються хмарним сервісом на предмет їх оновлення та підтримки, $CSP_{10} = D =$ "***Data module***" – модуль, що оцінює методи обробки конфіденційних даних, що циркулюють на базі ресурсів хмарного сервісу та безпосередньо впливають на діяльність компанії-замовника, $CSP_{11} = RE =$ "***Requirements' module***" – модуль, що відповідає за надання рекомендацій на основі відповідей аудитора з метою направлення компанії-замовника та забезпечення підвищеної захищеності власних сервісів, що розгорнуті на базі ресурсів хмарного сервісу [108].

Перший компонент узагальненої математичної моделі **GP** – модуль, що визначає тип хмарного сервісу, його назву та перевірку діяльності з країнами-агресорами, визначається виразом:

$$\mathbf{GP} = \left\{ \bigcup_{j=1}^{m_1} \mathbf{GP_j} \right\} = \left\{ \mathbf{GP_1}, \mathbf{GP_2} \ldots, \mathbf{GP_{m_1}} \right\}, \tag{2.3}$$

де: $\mathbf{GP_j} \subseteq \mathbf{GP}$ ($j = \overline{1, m_1}$) – *j*-й параметр визначення організаційної складової оцінюваного хмарного сервісу, а m_1 – їх кількість [101].

Наприклад, при $m_1 = 3$ ($j = \overline{1,3}$) формулу (2.3) можна представити як:

$$\mathbf{GP} = \left\{ \bigcup_{j=1}^{3} \mathbf{GP_j} \right\} = \left\{ \mathbf{GP_1}, \mathbf{GP_2}, \mathbf{GP_3} \right\}, \tag{2.4}$$

де, відповідно: $\mathbf{GP_1}$ = «Виберіть тип хмарного сервісу, для якого ви бажаєте оцінити рівень захищеності:»; $\mathbf{GP_2}$ = «Назва хмарного сервісу:»; $\mathbf{GP_3}$ = «Співпраця хмарного сервісу з країнами агресорами та на окупованих територіях:» [108].

Підмножину $\mathbf{GP_j}$ визначимо як:

$$\mathbf{GP_j} = \left\{ \bigcup_{k=1}^{m_{1j}} GP_{jk} \right\} = \left\{ GP_{j1}, GP_{j2}, ..., GP_{jm_{1k}} \right\} \tag{2.5}$$

де: $GP_{jk} \subseteq \mathbf{GP_j}$ $(k = \overline{1, m_{1j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{1j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.5) із урахуванням виразу (2.3) можна представити наступним чином:

$$\mathbf{GP} = \left\{ \bigcup_{j=1}^{m_1} \mathbf{GP_j} \right\} = \left\{ \bigcup_{j=1}^{m_1} \left\{ \bigcup_{k=1}^{m_{1j}} GP_{jk} \right\} \right\} = \{ \{ GP_{11}, GP_{12}, ..., GP_{1m_{1j}} \}, \{ GP_{21}, GP_{22}, ..., GP_{2m_{1j}} \}, ..., \{ GP_{m_1 1}, GP_{m_1 2}, ..., GP_{m_1 m_{1j}} \} \}, \tag{2.6}$$

Наприклад, при $m_1 = 3$ $(j = \overline{1,3})$, $m_{11} = 5$ $(k = \overline{1,5})$, $m_{12} = 1$ $(k = \overline{1,1})$, $m_{13} = 2$ $(k = \overline{1,2})$, формула (2.6) набуде наступного вигляду:

$$\mathbf{GP} = \left\{ \bigcup_{j=1}^{3} \mathbf{GP_j} \right\} = \left\{ \bigcup_{j=1}^{3} \left\{ \bigcup_{k=1}^{m_{1j}} GP_{jk} \right\} \right\} = \{ \{ GP_{11}, GP_{12}, GP_{13}, GP_{14}, GP_{15} \}, \{ GP_{21} \}, \{ GP_{31}, GP_{32} \} \}, \tag{2.7}$$

де: GP_{11} = «IaaS (Infrastructure-as-a-Service)»; GP_{12} = «CaaS (Container-as-a-Service)»; GP_{13} = «PaaS (Platform-as-a-Service)»; GP_{14} = «FaaS (Function-as-a-Service)»; GP_{15} = «SaaS (Software-as-a-Service)»; GP_{21} = «<Вказується найменування хмарного сервісу, оцінка якого буде проводитися>»; GP_{31} = «Так»; GP_{32} = «Ні» [108].

Другий компонент узагальненої математичної моделі **N** – модуль, що оцінює мережеву частину хмарного сервісу на предмет захищеності та здатності протидіяти відомим загрозам, визначається виразом:

$$\mathbf{N} = \left\{ \bigcup_{j=1}^{m_2} \mathbf{N_j} \right\} = \left\{ \mathbf{N_1}, \mathbf{N_2} ..., \mathbf{N_{m_2}} \right\}, \tag{2.8}$$

де: $\mathbf{N_j} \subseteq \mathbf{N}$ ($j = \overline{1, m_2}$) – j-й параметр визначення організаційної складової оцінюваного хмарного сервісу, а m_2 – їх кількість [101].

Наприклад, при $m_2 = 10$ ($j = \overline{1,10}$) формулу (2.8) можна представити як:

$$\mathbf{N} = \left\{ \bigcup_{j=1}^{10} \mathbf{N_j} \right\} = \left\{ \mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3}, \mathbf{N_4}, \mathbf{N_5}, \mathbf{N_6}, \mathbf{N_7}, \mathbf{N_8}, \mathbf{N_9}, \mathbf{N_{10}} \right\}, \tag{2.9}$$

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:» [108].

Підмножину $\mathbf{N_j}$ визначимо як:

$$\mathbf{N_j} = \left\{ \bigcup_{k=1}^{m_{2j}} N_{jk} \right\} = \left\{ N_{j1}, N_{j2}, ..., N_{jm_{2j}} \right\} \tag{2.10}$$

де: $N_{jk} \subseteq \mathbf{N_j}$ $(k = \overline{1, m_{2j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{2j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.8) із урахуванням виразу (2.10) можна представити наступним чином:

$$\begin{gathered}\mathbf{N} = \left\{ \bigcup_{j=1}^{m_2} \mathbf{N_j} \right\} = \left\{ \bigcup_{j=1}^{m_2} \left\{ \bigcup_{k=1}^{m_{2j}} N_{jk} \right\} \right\} = \{ \{ N_{11}, N_{12}, ..., N_{1m_{2j}} \}, \\ \{ N_{21}, N_{22}, ..., N_{2m_{2j}} \}, ..., \{ N_{m_2 1}, N_{m_2 2}, ..., N_{m_2 m_{2j}} \} \},\end{gathered} \tag{2.11}$$

Наприклад, при $m_2 = 10$ $(j = \overline{1,10})$, $m_{21} = 6$ $(k = \overline{1,6})$, $m_{22} = 6$ $(k = \overline{1,6})$, $m_{23} = 6$ $(k = \overline{1,6})$, $m_{24} = 2$ $(k = \overline{1,2})$, $m_{25} = 2$ $(k = \overline{1,2})$, $m_{26} = 2$ $(k = \overline{1,2})$, $m_{27} = 2$ $(k = \overline{1,2})$, $m_{28} = 2$ $(k = \overline{1,2})$, $m_{29} = 2$ $(k = \overline{1,2})$, $m_{210} = 2$ $(k = \overline{1,2})$, формула (2.11) набуде наступного вигляду:

$$\begin{gathered}\mathbf{N} = \left\{ \bigcup_{j=1}^{10} \mathbf{N_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} N_{jk} \right\} \right\} = \{ \{ N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16} \}, \\ \{ N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26} \}, \{ N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36} \}, \\ \{ N_{41}, N_{42} \}, \{ N_{51}, N_{52} \}, \{ N_{61}, N_{62} \}, \{ N_{71}, N_{72} \}, \{ N_{81}, N_{82} \}, \\ \{ N_{91}, N_{92} \}, \{ N_{101}, N_{102} \} \},\end{gathered} \tag{2.12}$$

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» [108].

Враховуючи, що параметри N_{41} та N_{51} мають власні підмножини, тому дані параметри можна визначити наступним чином:

$$\mathbf{N_{jk}} = \left\{ \bigcup_{l=1}^{m_{2jk}} \mathbf{N_{jkl}} \right\} = \left\{ \mathbf{N_{jk1}}, \mathbf{N_{jk2}}, \ldots, \mathbf{N_{jkm_{2jk}}} \right\} \tag{2.13}$$

Наприклад, при $m_{241} = 11\ (l = \overline{1,11})$, $m_{252} = 1\ (l = \overline{1,1})$, формула (2.13) набуде наступного вигляду:

$$\begin{gathered}
\mathbf{N} = \left\{ \bigcup_{j=1}^{10} \mathbf{N_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} N_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} \left\{ \bigcup_{l=1}^{m_{2jk}} \mathbf{N_{jkl}} \right\} \right\} \right\} = \\
\{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\}, \\
\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\}, \\
\{\{\mathbf{N_{411}}, \mathbf{N_{412}}, \mathbf{N_{413}}, \mathbf{N_{414}}, \mathbf{N_{415}}, \mathbf{N_{416}}, \mathbf{N_{417}}, \mathbf{N_{418}}, \mathbf{N_{419}}, \mathbf{N_{4110}}, \mathbf{N_{4111}}\}, N_{42}\}, \\
\{\{\mathbf{N_{511}}\}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\}, \\
\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\},\},
\end{gathered} \tag{2.14}$$

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» [108].

Підмножину $\mathbf{N}_{\mathbf{jkl}}$ визначимо як:

$$\mathbf{N}_{\mathbf{jkl}} = \left\{ \bigcup_{p=1}^{m_{2jkl}} N_{jklp} \right\} = \left\{ N_{jkl1}, N_{jkl2}, \ldots, N_{jklm_{2jkl}} \right\} \tag{2.15}$$

де: $N_{jklp} \subseteq \mathbf{N}_{\mathbf{jkl}}$ $(p = \overline{1, m_{2jkl}})$ – p-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами l-ї підмножини, m_{2jkl} – кількість груп l-ї підмножини [108].

Відповідно вираз (2.14) із урахуванням виразу (2.15) можна представити наступним чином:

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

$$\begin{gathered}
\{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\}, \\
\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\}, \\
\{\{\{N_{4111}, N_{4112}\}, \{N_{4121}, N_{4122}, N_{4123}, N_{4124}, N_{4125}, N_{4126}, N_{4127}, N_{4128}, N_{4129}\}, \\
\{N_{4131}, N_{4132}\}, \{N_{4141}, N_{4142}\}, \{N_{4151}, N_{4152}\}, \{N_{4161}, N_{4162}\}, \{N_{4171}, N_{4172}\}, \\
\{N_{4181}, N_{4182}\}, \{N_{4191}, N_{4192}\}, \{N_{41101}, N_{41102}\}, \{N_{41111}, N_{41112}\}\}, N_{42}\}, \\
\{\{\{N_{5111}, N_{5112}\}\}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\}, \\
\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\}\},
\end{gathered} \tag{2.16}$$

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» [108].

Третій компонент узагальненої математичної моделі **S** – модуль, що оцінює системи зберігання даних хмарного сервісу, можливості відновлення даних та протидії відомим загрозам, визначається виразом:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{m_3} \mathbf{S_j} \right\} = \left\{ \mathbf{S_1}, \mathbf{S_2} \ldots, \mathbf{S_{m_3}} \right\}, \quad (2.17)$$

де: $\mathbf{S_j} \subseteq \mathbf{S}$ ($j = \overline{1, m_3}$) – j-й параметр визначення захищеності та відмовостійкості середовища зберігання даних оцінюваного хмарного сервісу, а m_3 – їх кількість [101].

Наприклад, при $m_3 = 10$ ($j = \overline{1,10}$) формулу (2.17) можна представити як:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{10} \mathbf{S_j} \right\} = \left\{ \mathbf{S_1}, \mathbf{S_2}, \mathbf{S_3}, \mathbf{S_4}, \mathbf{S_5}, \mathbf{S_6}, \mathbf{S_7}, \mathbf{S_8}, \mathbf{S_9}, \mathbf{S_{10}} \right\}, \quad (2.18)$$

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:» [108].

Підмножину $\mathbf{S_j}$ визначимо як:

$$\mathbf{S_j} = \left\{ \bigcup_{k=1}^{m_{3j}} S_{jk} \right\} = \left\{ S_{j1}, S_{j2}, \ldots, S_{jm_{3j}} \right\} \quad (2.19)$$

де: $S_{jk} \subseteq \mathbf{S_j}$ ($k = \overline{1, m_{3j}}$) – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{3j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.17) із урахуванням виразу (2.19) можна представити наступним чином:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{m_3} \mathbf{S_j} \right\} = \left\{ \bigcup_{j=1}^{m_3} \left\{ \bigcup_{k=1}^{m_{3j}} S_{jk} \right\} \right\} = \{\{S_{11}, S_{12}, \ldots, S_{1m_{3j}}\},$$
$$\{S_{21}, S_{22}, \ldots, S_{2m_{3j}}\}, \ldots, \{S_{m_3 1}, S_{m_3 2}, \ldots, S_{m_3 m_{3j}}\}\}, \quad (2.20)$$

Наприклад, при $m_3 = 10$ ($j = \overline{1,10}$), $m_{31} = 2$ ($k = \overline{1,2}$), $m_{32} = 2$ ($k = \overline{1,2}$), $m_{33} = 2$ ($k = \overline{1,2}$), $m_{34} = 2$ ($k = \overline{1,2}$), $m_{35} = 2$ ($k = \overline{1,2}$), $m_{36} = 2$ ($k = \overline{1,2}$), $m_{37} = 2$ ($k = \overline{1,2}$), $m_{38} = 2$ ($k = \overline{1,2}$), $m_{39} = 2$ ($k = \overline{1,2}$), $m_{310} = 2$ ($k = \overline{1,2}$), формула (2.20) набуде наступного вигляду:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{10} \mathbf{S_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{3j}} S_{jk} \right\} \right\} = \{\{S_{11}, S_{12}\},$$
$$\{S_{21}, S_{22}\}, \{S_{31}, S_{32}\}, \{S_{41}, S_{42}\}, \{S_{51}, S_{52}\},$$
$$\{S_{61}, S_{62}\}, \{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\},$$
$$\{S_{101}, S_{102}\}\}, \quad (2.21)$$

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» [101].

Враховуючи, що параметри S_{11} та S_{41} мають власні підмножини, тому дані параметри можна визначити наступним чином:

$$\mathbf{S_{jk}} = \left\{ \bigcup_{l=1}^{m_{3jk}} \mathbf{S_{jkl}} \right\} = \left\{ \mathbf{S_{jk1}}, \mathbf{S_{jk2}}, \ldots, \mathbf{S_{jkm_{3jk}}} \right\} \quad (2.22)$$

Наприклад, при $m_{311} = 4$ ($l = \overline{1,4}$), $m_{342} = 5$ ($l = \overline{1,5}$), формула (2.22) набуде наступного вигляду:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{10} \mathbf{S_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{3j}} S_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{3j}} \left\{ \bigcup_{l=1}^{m_{3jk}} \mathbf{S_{jkl}} \right\} \right\} \right\} =$$
$$\{\{\{\mathbf{S_{111}}, \mathbf{S_{112}}, \mathbf{S_{113}}, \mathbf{S_{114}}\}, S_{12}\}, \{S_{21}, S_{22}\}, \{S_{31}, S_{32}\},$$
$$\{\{\mathbf{S_{411}}, \mathbf{S_{412}}, \mathbf{S_{413}}, \mathbf{S_{414}}, \mathbf{S_{415}}\}, S_{42}\}, \{S_{51}, S_{52}\}, \{S_{61}, S_{62}\},$$
$$\{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\}, \{S_{101}, S_{102}\}\}, \quad (2.23)$$

де: $\mathbf{S}_{111}$ = «Рішення підтримує локальну реплікацію (Local Replication) в тому ж регіоні, що і знаходиться VPC/VPS:»; $\mathbf{S}_{112}$ = «Рішення підтримує регіональну реплікацію (Regional Replication), в мінімум ніж 2-х інших містах, окрім тих, де розташовані VPC/VPS:»; $\mathbf{S}_{113}$ = «Рішення підтримує GEO-розподілену реплікацію (Geo-Redundant Replication), в мінімум ніж 2-х інших країнах, окрім тих, де розташовані VPC/VPS:»; $\mathbf{S}_{114}$ = «Виберіть який метод реплікації підтримує хмарний сервіс:»; $\mathbf{S}_{411}$ = «Представники постачальника хмарних сервісів мають доступ до наповнення шифрованого дискового простору:»; $\mathbf{S}_{412}$ = «Вкажіть, ким забезпечується управління ключами шифрування дискового простору:»; $\mathbf{S}_{413}$ = «Рішення має готовий функціонал управління та зберігання ключів шифрування:»; $\mathbf{S}_{414}$ = «Вкажіть метод шифрування, що використовується хмарним сервісом:»; $\mathbf{S}_{415}$ = «Рішення підтримує метод симетричного шифрування не нижче ніж AES-256:» [108].

Підмножину $\mathbf{S}_{\mathbf{jkl}}$ визначимо як:

$$\mathbf{S}_{\mathbf{jkl}} = \left\{ \bigcup_{p=1}^{m_{3jkl}} S_{\ jklp} \right\} = \left\{ S_{\ jkl1}, S_{\ jkl2}, \ldots, S_{\ jklm_{3jkl}} \right\} \tag{2.24}$$

де: $S_{jklp} \subseteq \mathbf{S}_{\mathbf{jkl}}$ $(p = \overline{1, m_{3jkl}})$ – p-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами l-ї підмножини, m_{3jkl} – кількість груп l-ї підмножини [108].

Відповідно вираз (2.23) із урахуванням виразу (2.24) можна представити наступним чином:

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

$$\{\{\{\{S_{\ 1111}, S_{\ 1112}\}, \{S_{\ 1121}, S_{\ 1122}\}, \{S_{\ 1131}, S_{\ 1132}\}, \{S_{\ 1141}, S_{\ 1142}, S_{\ 1143}, S_{\ 1144}\}\}, S_{\ 12}\},$$
$$\{S_{\ 21}, S_{\ 22}\}, \{S_{\ 31}, S_{\ 32}\}, \{\{\{S_{\ 4111}, S_{\ 4112}\}, \{S_{\ 4121}, S_{\ 4122}, S_{\ 4123}\}, \{S_{\ 4131}, S_{\ 4132}\},$$
$$\{S_{\ 4141}, S_{\ 4142}, S_{\ 4143}, S_{\ 4144}\}, \{S_{\ 4151}, S_{\ 4152}\}\}, S_{\ 42}\}, \{S_{\ 51}, S_{\ 52}\}, \{S_{\ 61}, S_{\ 62}\},$$
$$\{S_{\ 71}, S_{\ 72}\}, \{S_{\ 81}, S_{\ 82}\}, \{S_{\ 91}, S_{\ 92}\}, \{S_{\ 101}, S_{\ 102}\}\}, \tag{2.25}$$

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» [108].

Четвертий компонент узагальненої математичної моделі **SR** – модуль, що оцінює рівень фізичного захисту серверного обладнання, використовуваного хмарних сервісом, визначається виразом:

$$\mathbf{SR} = \left\{ \bigcup_{j=1}^{m_4} \mathbf{SR_j} \right\} = \left\{ \mathbf{SR_1}, \mathbf{SR_2} \ldots, \mathbf{SR_{m_4}} \right\}, \tag{2.26}$$

де: $\mathbf{SR_j} \subseteq \mathbf{SR}$ ($j = \overline{1, m_4}$) – j-й параметр визначення параметра оцінки серверного обладнання постачальника хмарного сервісу, а m_4 – їх кількість [101].

Наприклад, при $m_4 = 12$ ($j = \overline{1,12}$) формулу (2.26) можна представити як:

$$\mathbf{SR} = \left\{ \bigcup_{j=1}^{12} \mathbf{SR_j} \right\} = \tag{2.27}$$

$$\left\{ \mathbf{SR_1}, \mathbf{SR_2}, \mathbf{SR_3}, \mathbf{SR_4}, \mathbf{SR_5}, \mathbf{SR_6}, \mathbf{SR_7}, \mathbf{SR_8}, \mathbf{SR_9}, \mathbf{SR_{10}}, \mathbf{SR_{11}}, \mathbf{SR_{12}} \right\},$$

де, відповідно: $\mathbf{SR_1}$ = «Виберіть рівень фізичного доступу до серверів (Hardware) хмарного сервісу:»; $\mathbf{SR_2}$ = «Фізичне обладнання хмарного сервісу знаходиться під постійним відео-наглядом:»; $\mathbf{SR_3}$ = «Доступ до приміщень центра обробки даних надається по:»; $\mathbf{SR_4}$ = «ЦОД забезпечує безперебійну подачу живлення навіть у випадках відключення світла (black out):»; $\mathbf{SR_5}$ = «ЦОД забезпечує надійну системи кондиціонування приміщень, в яких розміщуються сервера постачальника хмарного сервісу:»; $\mathbf{SR_6}$ = «Всі приміщення в ЦОДі забезпечені протипожежними системами:»; $\mathbf{SR_7}$ = «ЦОД

має в кожному приміщенні, де розміщується обладнання, контролі руху, сигналізацію та системи ідентифікації особи:»; $\mathbf{SR}_8$ = «Обладнання в ЦОДі оновлюється кожні 4 роки для забезпечення відмовостійкості та підвищення продуктивності обладнання:»; $\mathbf{SR}_9$ = «Доступ до серверів хмарного сервісу захищений мережевими екрана нового покоління (NGFW):»; $\mathbf{SR}_{10}$ = «Доступ до серверів хмарного сервісу контролюється системами виявлення та попередження вторгнень (IPS & IDS):»; $\mathbf{SR}_{11}$ = «Фізичне підключення до серверів постачальника хмарного сервісу:»; $\mathbf{SR}_{12}$ = «У випадку виходу з ладу фізичного серверу, дані:» [108].

Підмножину $\mathbf{SR}_j$ визначимо як:

$$\mathbf{SR}_j = \left\{ \bigcup_{k=1}^{m_{4j}} SR_{jk} \right\} = \left\{ SR_{j1}, SR_{j2}, \ldots, SR_{jm_{4j}} \right\} \tag{2.28}$$

де: $SR_{jk} \subseteq \mathbf{SR}_j$ $(k = \overline{1, m_{4j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{4j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.26) із урахуванням виразу (2.28) можна представити наступним чином:

$$\mathbf{SR} = \left\{ \bigcup_{j=1}^{m_4} \mathbf{SR}_j \right\} = \left\{ \bigcup_{j=1}^{m_4} \left\{ \bigcup_{k=1}^{m_{4j}} SR_{jk} \right\} \right\} = \{ \{ SR_{11}, SR_{12}, \ldots, SR_{1m_{4j}} \}, \{ SR_{21}, SR_{22}, \ldots, SR_{2m_{4j}} \}, \ldots, \{ SR_{m_4 1}, SR_{m_4 2}, \ldots, SR_{m_4 m_{4j}} \} \}, \tag{2.29}$$

Наприклад, при $m_4 = 12$ $(j = \overline{1,12})$, $m_{41} = 4$ $(k = \overline{1,4})$, $m_{42} = 2$ $(k = \overline{1,2})$, $m_{43} = 6$ $(k = \overline{1,6})$, $m_{44} = 2$ $(k = \overline{1,2})$, $m_{45} = 2$ $(k = \overline{1,2})$, $m_{46} = 2$ $(k = \overline{1,2})$, $m_{47} = 2$ $(k = \overline{1,2})$, $m_{48} = 2$ $(k = \overline{1,2})$, $m_{49} = 3$ $(k = \overline{1,3})$, $m_{410} = 4$ $(k = \overline{1,4})$, $m_{411} = 3$ $(k = \overline{1,3})$, $m_{412} = 3$ $(k = \overline{1,3})$, формула (2.29) набуде наступного вигляду:

$$\mathbf{SR} = \left\{ \bigcup_{j=1}^{12} \mathbf{SR}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{12} \left\{ \bigcup_{k=1}^{m_{4j}} SR_{jk} \right\} \right\} =$$

$$\{\{SR_{11}, SR_{12}, SR_{13}, SR_{14}\}, \{SR_{21}, SR_{22}\},$$
$$\{SR_{31}, SR_{32}, SR_{33}, SR_{34}, SR_{35}, SR_{36}\}, \{SR_{41}, SR_{42}\}, \{SR_{51}, SR_{52}\},$$
$$\{SR_{61}, SR_{62}\}, \{SR_{71}, SR_{72}\}, \{SR_{81}, SR_{82}\}, \{SR_{91}, SR_{92}, SR_{93}\},$$
$$\{SR_{101}, SR_{102}, SR_{103}, SR_{104}\}, \{SR_{111}, SR_{112}, SR_{113}\}, \{SR_{121}, SR_{122}, SR_{123}\}\}, \quad (2.30)$$

де: SR_{11} = «Обмежений лише для співробітників хмарного сервісу»; SR_{12} = «Доступ надається для співробітників хмарного сервісу та співробітників центру обробки даних»; SR_{13} = «Доступ надається для співробітників хмарного сервісу, замовників хмарного сервісу та співробітників центру обробки даних»; SR_{14} = «Доступ до серверів заборонений для всіх, окрім співробітників центру обробки даних»; SR_{21} = «Так»; SR_{22} = «Ні»; SR_{31} = «ключ-картам та фізичним ключем доступу»; SR_{32} = «ключ-картам»; SR_{33} = «шляхом передачі фізичного ключа»; SR_{34} = «по індивідуальним паперовим перепусткам»; SR_{35} = «по знайомству»; SR_{36} = «ніяк не контролюється»; SR_{41} = «Так, має автономні джерела подачі живлення (генератори, власні підстанції тощо)»; SR_{42} = «Ні»; SR_{51} = «Так»; SR_{52} = «Ні»; SR_{61} = «Так»; SR_{62} = «Ні»; SR_{71} = «Так»; SR_{72} = «Ні»; SR_{81} = «Так»; SR_{82} = «Ні»; SR_{91} = «Так»; SR_{92} = «Частково, використовуються тільки звичайні мережеві екрани (iptables, local FW etc)»; SR_{93} = «Ні»; SR_{101} = «Так»; SR_{102} = «Ні, тільки IPS»; SR_{103} = «Ні, тільки IDS»; SR_{104} = «Відсутні системи IPS/IDS»; SR_{111} = «Взагалі неможливе»; SR_{112} = «Можливе за попереднім запитом від хмарного сервісу та тримання тимчасового доступу»; SR_{113} = «Будь-хто має можливість підключитися до серверів після входу в серверну кімнату»; SR_{121} = «Автоматично відновлюються на суміжному резервному сервері та продовжують виконувати бізнес-процедури хмарного сервісу»; SR_{122} = «Вручну переносяться на суміжні сервери для відновлення працездатності бізнесу»; SR_{123} = «Не зберігаються і не відновлюються» [108].

П'ятий компонент узагальненої математичної моделі **V** – модуль, що оцінює системи віртуалізації хмарного сервісу на предмет захищеності та здатності протидіяти відомим загрозам із можливостями налаштування сповіщень, визначається виразом:

$$\mathbf{V} = \left\{ \bigcup_{j=1}^{m_5} \mathbf{V}_j \right\} = \left\{ \mathbf{V}_1, \mathbf{V}_2 \ldots, \mathbf{V}_{m_5} \right\}, \tag{2.31}$$

де: $\mathbf{V}_j \subseteq \mathbf{V}$ ($j = \overline{1, m_5}$) – j-й параметр оцінки системи віртуалізації використовуваної постачальником хмарного сервісу, а m_5 – їх кількість [101].

Наприклад, при $m_5 = 10$ ($j = \overline{1,10}$) формулу (2.31) можна представити як:

$$\mathbf{V} = \left\{ \bigcup_{j=1}^{10} \mathbf{V}_j \right\} = \left\{ \mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3, \mathbf{V}_4, \mathbf{V}_5, \mathbf{V}_6, \mathbf{V}_7, \mathbf{V}_8, \mathbf{V}_9, \mathbf{V}_{10} \right\}, \tag{2.32}$$

де, відповідно: $\mathbf{V}_1$ = «Виберіть метод віртуалізації, що використовується хмарним сервісом:»; $\mathbf{V}_2$ = «При доступі до системи віртуалізації постачальник хмарних сервісів надає можливість використання рольової моделі доступу (RBAC):»; $\mathbf{V}_3$ = «Система віртуалізації підтримує 2FA/MFA для автентифікації користувачів:»; $\mathbf{V}_4$ = «Постачальник хмарних сервісів забезпечує замовника веб-консоллю для управління встановленими віртуальними машинами:»; $\mathbf{V}_5$ = «Постачальник хмарних сервісів забезпечує замовника можливістю повноцінного управління розгорнутою віртуальною машиною із внесенням змін в безпекові налаштування:»; $\mathbf{V}_6$ = «Постачальник хмарного сервісу забезпечує можливістю підвантаження власного образу та встановлення останнього на ресурсах хмарного сервісу:»; $\mathbf{V}_7$ = «Постачальник хмарних сервісів забезпечує можливістю авторизації користувачів на розгорнутих віртуальних машинах, як з використанням логіну/паролю, так і з використанням SSH-ключів, SSL-сертифікатів тощо:»; $\mathbf{V}_8$ = «Постачальник хмарних сервісів забезпечує системою сповіщень (alerts) адміністраторів при зміні мережевих налаштувань чи налаштувань з безпеки:»; $\mathbf{V}_9$ = «Постачальник хмарних сервісів надає в реальному часі події

(events) про стан функціонування системи віртуалізації та розгорнутих віртуальних машин:»; $\mathbf{V}_{10}$ = «Постачальник хмарних сервісів надає в реальному часу аудит події (audit logs) діяльності адміністратора, авторизованого у середовище замовника:» [108].

Підмножину $\mathbf{V}_j$ визначимо як:

$$\mathbf{V}_j = \left\{ \bigcup_{k=1}^{m_{5j}} V_{jk} \right\} = \left\{ V_{j1}, V_{j2}, \ldots, V_{jm_{5j}} \right\} \tag{2.33}$$

де: $V_{jk} \subseteq \mathbf{V}_j$ $(k = \overline{1, m_{5j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{5j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.31) із урахуванням виразу (2.33) можна представити наступним чином:

$$\begin{aligned} \mathbf{V} = \left\{ \bigcup_{j=1}^{m_5} \mathbf{V}_j \right\} = \left\{ \bigcup_{j=1}^{m_5} \left\{ \bigcup_{k=1}^{m_{5j}} V_{jk} \right\} \right\} = \{ \{ V_{11}, V_{12}, \ldots, V_{1m_{5j}} \}, \\ \{ V_{21}, V_{22}, \ldots, V_{2m_{5j}} \}, \ldots, \{ V_{m_5 1}, V_{m_5 2}, \ldots, V_{m_5 m_{5j}} \} \}, \end{aligned} \tag{2.34}$$

Наприклад, при $m_5 = 10$ $(j = \overline{1,10})$, $m_{51} = 7$ $(k = \overline{1,7})$, $m_{52} = 2$ $(k = \overline{1,2})$, $m_{53} = 2$ $(k = \overline{1,2})$, $m_{54} = 2$ $(k = \overline{1,2})$, $m_{55} = 2$ $(k = \overline{1,2})$, $m_{56} = 2$ $(k = \overline{1,2})$, $m_{57} = 2$ $(k = \overline{1,2})$, $m_{58} = 2$ $(k = \overline{1,2})$, $m_{59} = 2$ $(k = \overline{1,2})$, $m_{510} = 2$ $(k = \overline{1,2})$, формула (2.34) набуде наступного вигляду:

$$\begin{aligned} \mathbf{V} = \left\{ \bigcup_{j=1}^{10} \mathbf{V}_j \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} V_{jk} \right\} \right\} = \{ \{ V_{11}, V_{12}, V_{13}, V_{14}, V_{15}, V_{16}, V_{17} \}, \\ \{ V_{21}, V_{22} \}, \{ V_{31}, V_{32} \}, \{ V_{41}, V_{42} \}, \{ V_{51}, V_{52} \}, \{ V_{61}, V_{62} \}, \\ \{ V_{71}, V_{72} \}, \{ V_{81}, V_{82} \}, \{ V_{91}, V_{92} \}, \{ V_{101}, V_{102} \} \}, \end{aligned} \tag{2.35}$$

де: V_{11} = «Vmware vCenter»; V_{12} = «Vmware vSphere»; V_{13} = «Microsoft Hyper-V»; V_{14} = «KVM»; V_{15} = «Citrix XenServer»; V_{16} = «Інше»; V_{17} = «Не використовується»; V_{21} = «Так»; V_{22} = «Ні»; V_{31} = «Так»; V_{32} = «Ні»; V_{41} = «Так»; V_{42} = «Ні»; V_{51} = «Так»; V_{52} = «Ні»; V_{61} = «Так»; V_{62} = «Ні»; V_{71} =

«Так»; V_{72} = «Ні»; V_{81} = «Так»; V_{82} = «Ні»; V_{91} = «Так»; V_{92} = «Ні»; V_{101} = «Так»; V_{102} = «Ні» [108].

Враховуючи, що параметри V_{11}, V_{12}, V_{13}, V_{14}, V_{15} та V_{16} мають власні підмножини, тому дані параметри можна визначити наступним чином:

$$\mathbf{V}_{\mathbf{jk}} = \left\{ \bigcup_{l=1}^{m_{5jk}} \mathbf{V}_{\mathbf{jkl}} \right\} = \left\{ \mathbf{V}_{\mathbf{jk1}}, \mathbf{V}_{\mathbf{jk2}}, \ldots, \mathbf{V}_{\mathbf{jkm_{5jk}}} \right\} \tag{2.36}$$

Наприклад, при $m_{511} = 3\ (l = \overline{1,3})$, $m_{512} = 3\ (l = \overline{1,3})$, $m_{513} = 3\ (l = \overline{1,3})$, $m_{514} = 3\ (l = \overline{1,3})$, $m_{515} = 3\ (l = \overline{1,3})$, $m_{516} = 3\ (l = \overline{1,3})$, формула (2.36) набуде наступного вигляду:

$$\begin{gathered}\mathbf{V} = \left\{ \bigcup_{j=1}^{10} \mathbf{V}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} V_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} \left\{ \bigcup_{l=1}^{m_{5jk}} \mathbf{V}_{\mathbf{jkl}} \right\} \right\} \right\} = \\ \{\{\{\mathbf{V}_{\mathbf{111}}, \mathbf{V}_{\mathbf{112}}, \mathbf{V}_{\mathbf{113}}\}, \{\mathbf{V}_{\mathbf{121}}, \mathbf{V}_{\mathbf{122}}, \mathbf{V}_{\mathbf{123}}\}, \{\mathbf{V}_{\mathbf{131}}, \mathbf{V}_{\mathbf{132}}, \mathbf{V}_{\mathbf{133}}\}, \\ \{\mathbf{V}_{\mathbf{141}}, \mathbf{V}_{\mathbf{142}}, \mathbf{V}_{\mathbf{143}}\}, \{\mathbf{V}_{\mathbf{151}}, \mathbf{V}_{\mathbf{152}}, \mathbf{V}_{\mathbf{153}}\}, \{\mathbf{V}_{\mathbf{161}}, \mathbf{V}_{\mathbf{162}}, \mathbf{V}_{\mathbf{163}}\}, V_{17}\}, \\ \{V_{21}, V_{22}\}, \{V_{31}, V_{32}\}, \{V_{41}, V_{42}\}, \{V_{51}, V_{52}\}, \{V_{61}, V_{62}\}, \\ \{V_{71}, V_{72}\}, \{V_{81}, V_{82}\}, \{V_{91}, V_{92}\}, \{V_{101}, V_{102}\}\},\end{gathered} \tag{2.37}$$

де: $\mathbf{V}_{\mathbf{111}}$ = «Виберіть частоту проведення аудиту з безпеки системи віртуалізації:»; $\mathbf{V}_{\mathbf{112}}$ = «Виберіть, хто має доступ до системи віртуалізації хмарного сервісу:»; $\mathbf{V}_{\mathbf{113}}$ = «Система віртуалізації знаходиться в ізольованому середовищі:»; $\mathbf{V}_{\mathbf{121}}$ = «Виберіть частоту проведення аудиту з безпеки системи віртуалізації:»; $\mathbf{V}_{\mathbf{122}}$ = «Виберіть, хто має доступ до системи віртуалізації хмарного сервісу:»; $\mathbf{V}_{\mathbf{123}}$ = «Система віртуалізації знаходиться в ізольованому середовищі:»; $\mathbf{V}_{\mathbf{131}}$ = «Виберіть частоту проведення аудиту з безпеки системи віртуалізації:»; $\mathbf{V}_{\mathbf{132}}$ = «Виберіть, хто має доступ до системи віртуалізації хмарного сервісу:»; $\mathbf{V}_{\mathbf{133}}$ = «Система віртуалізації знаходиться в ізольованому середовищі:»; $\mathbf{V}_{\mathbf{141}}$ = «Виберіть частоту проведення аудиту з безпеки системи віртуалізації:»; $\mathbf{V}_{\mathbf{142}}$ = «Виберіть, хто має доступ до системи віртуалізації хмарного сервісу:»; $\mathbf{V}_{\mathbf{143}}$ = «Система віртуалізації знаходиться в ізольованому

середовищі:»; $\mathbf{V}_{151}$ = «Виберіть частоту проведення аудиту з безпеки системи віртуалізації:»; $\mathbf{V}_{152}$ = «Виберіть, хто має доступ до системи віртуалізації хмарного сервісу:»; $\mathbf{V}_{153}$ = «Система віртуалізації знаходиться в ізольованому середовищі:»; $\mathbf{V}_{161}$ = «Виберіть частоту проведення аудиту з безпеки системи віртуалізації:»; $\mathbf{V}_{162}$ = «Виберіть, хто має доступ до системи віртуалізації хмарного сервісу:»; $\mathbf{V}_{163}$ = «Система віртуалізації знаходиться в ізольованому середовищі:» [108].

Підмножину $\mathbf{V}_{\mathbf{jkl}}$ визначимо як:

$$\mathbf{V}_{\mathbf{jkl}} = \left\{ \bigcup_{p=1}^{m_{5jkl}} V_{jklp} \right\} = \left\{ V_{jkl1}, V_{jkl2}, \ldots, V_{jklm_{5jkl}} \right\} \tag{2.38}$$

де: $V_{jklp} \subseteq \mathbf{V}_{\mathbf{jkl}}$ $(p = \overline{1, m_{5jkl}})$ – p-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами l-ї підмножини, m_{5jkl} – кількість груп l-ї підмножини [108].

Відповідно вираз (2.36) із урахуванням виразу (2.38) можна представити наступним чином:

$$\mathbf{V} = \left\{ \bigcup_{j=1}^{10} \mathbf{V}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} V_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} \left\{ \bigcup_{l=1}^{m_{5jk}} \mathbf{V}_{\mathbf{jkl}} \right\} \right\} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} \left\{ \bigcup_{l=1}^{m_{5jk}} \left\{ \bigcup_{p=1}^{m_{5jkl}} V_{jklp} \right\} \right\} \right\} \right\}$$

$$\begin{gathered}
\{\{\{\{V_{1111}, V_{1112}, V_{1113}, V_{1114}, V_{1115}, V_{1116}\}, \\
\{V_{1121}, V_{1122}, V_{1123}, V_{1124}, V_{1125}, V_{1126}, V_{1127}, V_{1128}\}, \{V_{1131}, V_{1132}\}\}, \\
\{\{V_{1211}, V_{1212}, V_{1213}, V_{1214}, V_{1215}, V_{1216}\}, \\
\{V_{1221}, V_{1222}, V_{1223}, V_{1224}, V_{1225}, V_{1226}, V_{1227}, V_{1228}\}, \{V_{1231}, V_{1232}\}\}, \\
\{\{V_{1311}, V_{1312}, V_{1313}, V_{1314}, V_{1315}, V_{1316}\}, \\
\{V_{1321}, V_{1322}, V_{1323}, V_{1324}, V_{1325}, V_{1326}, V_{1327}, V_{1328}\}, \{V_{1331}, V_{1332}\}\}, \\
\{\{V_{1411}, V_{1412}, V_{1413}, V_{1414}, V_{1415}, V_{1416}\}, \\
\{V_{1421}, V_{1422}, V_{1423}, V_{1424}, V_{1425}, V_{1426}, V_{1427}, V_{1428}\}, \{V_{1431}, V_{1432}\}\}, \\
\{\{V_{1511}, V_{1512}, V_{1513}, V_{1514}, V_{1515}, V_{1516}\}, \\
\{V_{1521}, V_{1522}, V_{1523}, V_{1524}, V_{1525}, V_{1526}, V_{1527}, V_{1528}\}, \{V_{1531}, V_{1532}\}\}, \\
\{\{V_{1611}, V_{1612}, V_{1613}, V_{1614}, V_{1615}, V_{1616}\}, \\
\{V_{1621}, V_{1622}, V_{1623}, V_{1624}, V_{1625}, V_{1626}, V_{1627}, V_{1628}\}, \{V_{1631}, V_{1632}\}\}, \\
V_{17}\}, \{V_{21}, V_{22}\}, \{V_{31}, V_{32}\}, \{V_{41}, V_{42}\}, \{V_{51}, V_{52}\}, \{V_{61}, V_{62}\}, \\
\{V_{71}, V_{72}\}, \{V_{81}, V_{82}\}, \{V_{91}, V_{92}\}, \{V_{101}, V_{102}\}\},
\end{gathered} \tag{2.39}$$

де: $V_{1111} = V_{1211} = V_{1311} = V_{1411} = V_{1511} = V_{1611}$ = «Раз на квартал»; $V_{1112} = V_{1212} = V_{1312} = V_{1412} = V_{1512} = V_{1612}$ = «Раз на пів року»; $V_{1113} = V_{1213} = V_{1313} = V_{1413} = V_{1513} = V_{1613}$ = «Раз на рік»; $V_{1114} = V_{1214} = V_{1314} = V_{1414} = V_{1514} = V_{1614}$ = «Раз на 2 роки»; $V_{1115} = V_{1215} = V_{1315} = V_{1415} = V_{1515} = V_{1615}$ = «Раз на 5 років»; $V_{1116} = V_{1216} = V_{1316} = V_{1416} = V_{1516} = V_{1616}$ = «Не проводиться»; $V_{1121} = V_{1221} = V_{1321} = V_{1421} = V_{1521} = V_{1621}$ = «Замовник»; $V_{1122} = V_{1222} = V_{1322} = V_{1422} = V_{1522} = V_{1622}$ = «Представники постачальника хмарного сервісу»; $V_{1123} = V_{1223} = V_{1323} = V_{1423} = V_{1523} = V_{1623}$ = «Представники центру обробки даних та датацентру»; $V_{1124} = V_{1224} = V_{1324} = V_{1424} = V_{1524} = V_{1624}$ = «1, 2 та 3»; $V_{1125} = V_{1225} = V_{1325} = V_{1425} = V_{1525} = V_{1625}$ = «1 та 2»; $V_{1126} = V_{1226} = V_{1326} = V_{1426} = V_{1526} = V_{1626}$ = «1 та 3»; $V_{1127} = V_{1227} = V_{1327} = V_{1427} = V_{1527} = V_{1627}$ = «2 та 3»; $V_{1128} = V_{1228} = V_{1328} = V_{1428} = V_{1528}$ = «Ніхто з вище перелічених»; $V_{1131} = V_{1231} =$

V_{1331} = V_{1431} = V_{1531} = V_{1628} = V_{1631} = «Так»; V_{1132} = V_{1232} = V_{1332} = V_{1432} = V_{1532} = V_{1632} = «Ні» [108].

Шостий компонент узагальненої математичної моделі **OS** – модуль, що оцінює стан захищеності операційної системи, що є в основі розгорнутого сервісу пропонованого хмарним сервісом та здатність системи протидіяти кіберзагрозам, визначається виразом:

$$\mathbf{OS} = \left\{ \bigcup_{j=1}^{m_6} \mathbf{OS}_j \right\} = \left\{ \mathbf{OS}_1, \mathbf{OS}_2 \ldots, \mathbf{OS}_{m_6} \right\}, \tag{2.40}$$

де: $\mathbf{OS}_j \subseteq \mathbf{OS}$ ($j = \overline{1, m_6}$) – j-й параметр оцінки операційної системи використовуваної постачальником хмарного сервісу, а m_6 – їх кількість [101].

Наприклад, при $m_6 = 11$ ($j = \overline{1,11}$) формулу (2.40) можна представити як:

$$\mathbf{OS} = \left\{ \bigcup_{j=1}^{11} \mathbf{OS}_j \right\} = \left\{ \begin{matrix} \mathbf{OS}_1, \mathbf{OS}_2, \mathbf{OS}_3, \mathbf{OS}_4, \mathbf{OS}_5, \mathbf{OS}_6, \\ \mathbf{OS}_7, \mathbf{OS}_8, \mathbf{OS}_9, \mathbf{OS}_{10}, \mathbf{OS}_{11} \end{matrix} \right\}, \tag{2.41}$$

де, відповідно: $\mathbf{OS}_1$ = «Доступ до операційної системи постачальника хмарних сервісів має:»; $\mathbf{OS}_2$ = «Постачальник хмарних сервісів забезпечує регулярне створення резервних копій операційних систем:»; $\mathbf{OS}_3$ = «Постачальник хмарних сервісів проводить регулярне встановлення оновлень компонентів операційної системи:»; $\mathbf{OS}_4$ = «Постачальник хмарних сервісів забезпечує антивірусним захистом та розслідуванням інцидентів на підтримуваних операційних системах:»; $\mathbf{OS}_5$ = «Постачальник хмарних сервісів надає можливість замовникам розгортати власне програмне забезпечення на підтримуваних операційних системах:»; $\mathbf{OS}_6$ = «Постачальник хмарних сервісів забезпечує управління мережевим екраном на підтримуваних операційних системах:»; $\mathbf{OS}_7$ = «Постачальник хмарних сервісів забезпечує доступність підтримуваної операційної системи для замовника із будь-якої точки світу:»; $\mathbf{OS}_8$ = «Постачальник забезпечує відмовостійкість для підтримуваних операційних систем:»;

$\mathbf{OS}_9$ = «Постачальник хмарних сервісів гарантує цілісність даних на підтримуваних операційних системах:»; $\mathbf{OS}_{10}$ = «Постачальник хмарних сервісів використовує технологію IAM (Identity Access Management) для доступу до підтримуваних операційних систем:»; $\mathbf{OS}_{11}$ = «Постачальник хмарних послуг вчасно знаходить та виправляє виявлені вразливості на підтримуваних операційних системах:» [108].

Підмножину $\mathbf{OS}_j$ визначимо як:

$$\mathbf{OS}_j = \left\{ \bigcup_{k=1}^{m_{6j}} OS_{jk} \right\} = \left\{ OS_{j1}, OS_{j2}, ..., OS_{jm_{6j}} \right\} \tag{2.42}$$

де: $OS_{jk} \subseteq \mathbf{OS}_j$ $(k = \overline{1, m_{6j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{6j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.40) із урахуванням виразу (2.42) можна представити наступним чином:

$$\mathbf{OS} = \left\{ \bigcup_{j=1}^{m_6} \mathbf{OS}_j \right\} = \left\{ \bigcup_{j=1}^{m_6} \left\{ \bigcup_{k=1}^{m_{6j}} OS_{jk} \right\} \right\} = \{ \{ OS_{11}, OS_{12}, ..., OS_{1m_{6j}} \}, \{ OS_{21}, OS_{22}, ..., OS_{2m_{6j}} \}, ..., \{ OS_{m_6 1}, OS_{m_6 2}, ..., OS_{m_6 m_{6j}} \} \}, \tag{2.43}$$

Наприклад, при $m_6 = 11$ $(j = \overline{1,11})$, $m_{61} = 5$ $(k = \overline{1,5})$, $m_{62} = 2$ $(k = \overline{1,2})$, $m_{63} = 2$ $(k = \overline{1,2})$, $m_{64} = 2$ $(k = \overline{1,2})$, $m_{65} = 2$ $(k = \overline{1,2})$, $m_{66} = 2$ $(k = \overline{1,2})$, $m_{67} = 2$ $(k = \overline{1,2})$, $m_{68} = 2$ $(k = \overline{1,2})$, $m_{69} = 2$ $(k = \overline{1,2})$, $m_{610} = 2$ $(k = \overline{1,2})$, $m_{611} = 2$ $(k = \overline{1,2})$, формула (43) набуде наступного вигляду:

$$\mathbf{OS} = \left\{ \bigcup_{j=1}^{11} \mathbf{OS}_j \right\} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} OS_{jk} \right\} \right\} = \{ \{ OS_{11}, OS_{12}, OS_{13}, OS_{14}, OS_{15} \}, \{ OS_{21}, OS_{22} \}, \{ OS_{31}, OS_{32} \}, \{ OS_{41}, OS_{42} \}, \{ OS_{51}, OS_{52} \}, \{ OS_{61}, OS_{62} \}, \{ OS_{71}, OS_{72} \}, \{ OS_{81}, OS_{82} \}, \{ OS_{91}, OS_{92} \}, \{ OS_{101}, OS_{102} \}, \{ OS_{111}, OS_{112} \} \}, \tag{2.44}$$

де: OS_{11} = «Замовник»; OS_{12} = «Представники постачальника хмарних послуг»; OS_{13} = «Представники центру обробки даних»; OS_{14} = «Всі з вище

переліченних»; OS_{15} = «Жоден з вище перелічених»; OS_{21} = «Так»; OS_{22} = «Ні»; OS_{31} = «Так»; OS_{32} = «Ні»; OS_{41} = «Так»; OS_{42} = «Ні»; OS_{51} = «Так»; OS_{52} = «Ні»; OS_{61} = «Так»; OS_{62} = «Ні»; OS_{71} = «Так»; OS_{72} = «Ні»; OS_{81} = «Так»; OS_{82} = «Ні»; OS_{91} = «Так»; OS_{92} = «Ні»; OS_{101} = «Так»; OS_{102} = «Ні»; OS_{111} = «Так»; OS_{112} = «Ні» [101].

Враховуючи, що параметр OS_{21} має власну підмножину, тому даний параметр можна визначити наступним чином:

$$\mathbf{OS_{jk}} = \left\{ \bigcup_{l=1}^{m_{6jk}} \mathbf{OS_{jkl}} \right\} = \left\{ \mathbf{OS_{jk1}}, \mathbf{OS_{jk2}}, \ldots, \mathbf{OS_{jkm_{6jk}}} \right\} \tag{2.45}$$

Наприклад, при $m_{621} = 1$ $(l = \overline{1,1})$, враховуючи вираз (2.45), формула (2.44) набуде наступного вигляду:

$$\begin{gathered} \mathbf{OS} = \left\{ \bigcup_{j=1}^{11} \mathbf{OS_j} \right\} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} OS_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} \left\{ \bigcup_{l=1}^{m_{6jk}} \mathbf{OS_{jkl}} \right\} \right\} \right\} = \\ \{\{OS_{11}, OS_{12}, OS_{13}, OS_{14}, OS_{15}\}, \{\{\mathbf{OS_{211}}\}, OS_{22}\}, \\ \{OS_{31}, OS_{32}\}, \{OS_{41}, OS_{42}\}, \{OS_{51}, OS_{52}\}, \{OS_{61}, OS_{62}\}, \\ \{OS_{71}, OS_{72}\}, \{OS_{81}, OS_{82}\}, \{OS_{91}, OS_{92}\}, \{OS_{101}, OS_{102}\}, \{OS_{111}, OS_{112}\}\}, \end{gathered} \tag{2.46}$$

де: $\mathbf{OS_{211}}$ = «Створена резервна копія захищена ключем шифрування:» [101].

Підмножину $\mathbf{OS_{jkl}}$ визначимо як:

$$\mathbf{OS_{jkl}} = \left\{ \bigcup_{p=1}^{m_{6jkl}} OS_{jklp} \right\} = \left\{ OS_{jkl1}, OS_{jkl2}, \ldots, OS_{jklm_{6jkl}} \right\} \tag{2.47}$$

де: $OS_{jklp} \subseteq \mathbf{OS_{jkl}}$ $(p = \overline{1, m_{6jkl}})$ – p-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами l-ї підмножини, m_{6jkl} – кількість груп l-ї підмножини [108].

Відповідно вираз (2.46) із урахуванням виразу (2.47) можна представити наступним чином:

$$\mathbf{OS} = \left\{ \bigcup_{j=1}^{11} \mathbf{OS_j} \right\} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} OS_{jk} \right\} \right\} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} \left\{ \bigcup_{l=1}^{m_{6jk}} \mathbf{OS_{jkl}} \right\} \right\} \right\} =$$

$$\left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} \left\{ \bigcup_{l=1}^{m_{6jk}} \left\{ \bigcup_{p=1}^{m_{6jkl}} OS_{jklp} \right\} \right\} \right\} \right\} = \{\{OS_{11}, OS_{12}, OS_{13}, OS_{14}, OS_{15},\}, \quad (2.48)$$

$$\{\{\{OS_{2111}, OS_{2112}\}\}, OS_{22}\}, \{OS_{31}, OS_{32}\}, \{OS_{41}, OS_{42}\},$$
$$\{OS_{51}, OS_{52}\}, \{OS_{61}, OS_{62}\}, \{OS_{71}, OS_{72}\}, \{OS_{81}, OS_{82}\},$$
$$\{OS_{91}, OS_{92}\}, \{OS_{101}, OS_{102}\}, \{OS_{111}, OS_{112}\}\},$$

де: OS_{2111} = «Так»; OS_{2112} = «Ні» [101].

Сьомий компонент узагальненої математичної моделі **СТ** – модуль, що оцінює стан захищеності середовища управління та налагодження контейнерів, визначається виразом:

$$\mathbf{CT} = \left\{ \bigcup_{j=1}^{m_7} \mathbf{CT_j} \right\} = \left\{ \mathbf{CT_1}, \mathbf{CT_2} \ldots, \mathbf{CT_{m_7}} \right\}, \quad (2.49)$$

де: $\mathbf{CT_j} \subseteq \mathbf{CT}$ ($j = \overline{1, m_7}$) – j-й параметр оцінки стану захищеності контейнерів, розгорнутих на ресурсах хмарних сервісів, а m_7 – їх кількість [101].

Наприклад, при $m_7 = 10$ ($j = \overline{1,10}$) формулу (2.49) можна представити як:

$$\mathbf{CT} = \left\{ \bigcup_{j=1}^{10} \mathbf{CT_j} \right\} = \left\{ \begin{matrix} \mathbf{CT_1}, \mathbf{CT_2}, \mathbf{CT_3}, \mathbf{CT_4}, \mathbf{CT_5}, \\ \mathbf{CT_6}, \mathbf{CT_7}, \mathbf{CT_8}, \mathbf{CT_9}, \mathbf{CT_{10}} \end{matrix} \right\}, \quad (2.50)$$

де, відповідно: $\mathbf{CT_1}$ = «Постачальних хмарних послуг надає можливість замовнику:»; $\mathbf{CT_2}$ = «Постачальних хмарних послуг регулярно проводить встановлення оновлень для системи управління та розгортання контейнерів:»; $\mathbf{CT_3}$ = «Постачальник хмарних послуг регулярно проводить сканування на предмет виявлення вразливостей встановленої системи для управління контейнерами:»; $\mathbf{CT_4}$ = «Постачальник хмарних послуг надає замовнику можливість використання технології захисту розгорнутої системи управління контейнерами та, безпосередньо, контейнерів:»; $\mathbf{CT_5}$ = «Постачальник хмарних послуг розмежовує середовища управління контейнерами між різними замовниками:»; $\mathbf{CT_6}$ = «Постачальник хмарних послуг надає

можливість замовнику налаштовувати рольову модель доступу для управління контейнерами:»; $\mathbf{CT}_7$ = «Постачальник хмарних послуг надає замовнику доступ до приватного репозиторію контейнерів для зберігання резервних копій контейнерів:»; $\mathbf{CT}_8$ = «Постачальник хмарних послуг надає детальну статистику використання контейнерів, споживання трафіку, завантаженість кожного з них та інші статистичні дані:»; $\mathbf{CT}_9$ = «Постачальник хмарних послуг забезпечує можливістю управління розгорнутими контейнерами через REST API:»; $\mathbf{CT}_{10}$ = «Постачальник хмарних послуг забезпечує функціоналом зупинки виконання контейнера при виявленій нелегальної активності та запуску нового контейнера для відновлення роботи сервісу:» [108].

Підмножину $\mathbf{CT}_\mathbf{j}$ визначимо як:

$$\mathbf{CT}_\mathbf{j} = \left\{ \bigcup_{k=1}^{m_{7j}} CT_{jk} \right\} = \left\{ CT_{j1}, CT_{j2}, \ldots, CT_{jm_{7j}} \right\} \tag{2.51}$$

де: $CT_{jk} \subseteq \mathbf{CT}_\mathbf{j}$ $(k = \overline{1, m_{7j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{7j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.49) із урахуванням виразу (2.51) можна представити наступним чином:

$$\begin{aligned} \mathbf{CT} = \left\{ \bigcup_{j=1}^{m_7} \mathbf{CT}_\mathbf{j} \right\} = \left\{ \bigcup_{j=1}^{m_7} \left\{ \bigcup_{k=1}^{m_{7j}} CT_{jk} \right\} \right\} = \{ \{ CT_{11}, CT_{12}, \ldots, CT_{1m_{7j}} \}, \\ \{ CT_{21}, CT_{22}, \ldots, CT_{2m_{7j}} \}, \ldots, \{ CT_{m_7 1}, CT_{m_7 2}, \ldots, CT_{m_7 m_{7j}} \} \}, \end{aligned} \tag{2.52}$$

Наприклад, при $m_7 = 10$ $(j = \overline{1,10})$, $m_{71} = 2$ $(k = \overline{1,2})$, $m_{72} = 2$ $(k = \overline{1,2})$, $m_{73} = 2$ $(k = \overline{1,2})$, $m_{74} = 2$ $(k = \overline{1,2})$, $m_{75} = 2$ $(k = \overline{1,2})$, $m_{76} = 2$ $(k = \overline{1,2})$, $m_{77} = 2$ $(k = \overline{1,2})$, $m_{78} = 2$ $(k = \overline{1,2})$, $m_{79} = 2$ $(k = \overline{1,2})$, $m_{710} = 2$ $(k = \overline{1,2})$, формула (2.52) набуде наступного вигляду:

$$\mathbf{CT} = \left\{ \bigcup_{j=1}^{10} \mathbf{CT_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{7j}} CT_{jk} \right\} \right\} = \{\{CT_{11}, CT_{12}\}, \{CT_{21}, CT_{22}\}, \{CT_{31}, CT_{32}\}, \{CT_{41}, CT_{42}\}, \{CT_{51}, CT_{52}\}, \{CT_{61}, CT_{62}\}, \{CT_{71}, CT_{72}\}, \{CT_{81}, CT_{82}\}, \{CT_{91}, CT_{92}\}, \{CT_{101}, CT_{102}\}\}, \quad (2.53)$$

де: CT_{11} = «Самостійно встановлювати систему для управління контейнерами»; CT_{12} = «Надає готову платформу для управління та розгортання контейнерів»; CT_{21} = «Так»; CT_{22} = «Ні»; CT_{31} = «Так»; CT_{32} = «Ні»; CT_{41} = «Так»; CT_{42} = «Ні»; CT_{51} = «Так»; CT_{52} = «Ні»; CT_{61} = «Так»; CT_{62} = «Ні»; CT_{71} = «Так»; CT_{72} = «Ні»; CT_{81} = «Так»; CT_{82} = «Ні»; CT_{91} = «Так»; CT_{92} = «Ні»; CT_{101} = «Так»; CT_{102} = «Ні» [108].

Восьмий компонент узагальненої математичної моделі **R** – модуль, що оцінює стан забезпечення безперервної роботи ресурсів постачальника хмарного сервісу, що забезпечують роботу бізнесу та бізнес процесів, визначається виразом:

$$\mathbf{R} = \left\{ \bigcup_{j=1}^{m_8} \mathbf{R_j} \right\} = \left\{ \mathbf{R_1}, \mathbf{R_2} \ldots, \mathbf{R_{m_8}} \right\}, \quad (2.54)$$

де: $\mathbf{R_j} \subseteq \mathbf{R}$ ($j = \overline{1, m_8}$) $-$ j-й параметр оцінки стану безперервної роботи хмарних сервісів, а m_8 – їх кількість [101].

Наприклад, при $m_8 = 13$ ($j = \overline{1,13}$) формулу (2.54) можна представити як:

$$\mathbf{R} = \left\{ \bigcup_{j=1}^{13} \mathbf{R_j} \right\} = \left\{ \begin{matrix} \mathbf{R_1}, \mathbf{R_2}, \mathbf{R_3}, \mathbf{R_4}, \mathbf{R_5}, \mathbf{R_6}, \mathbf{R_7}, \\ \mathbf{R_8}, \mathbf{R_9}, \mathbf{R_{10}}, \mathbf{R_{11}}, \mathbf{R_{12}}, \mathbf{R_{13}} \end{matrix} \right\}, \quad (2.55)$$

де, відповідно: $\mathbf{R_1}$ = «Постачальник хмарних сервісів забезпечує можливість логування всіх подій, що відбуваються в системі: аудит події, журнал подій, журнал змін в системі тощо:»; $\mathbf{R_2}$ = «Рішення має можливість відслідковувати зміни в функціонуванні віртуальних машин та відображати статус на панелі управління:»; $\mathbf{R_3}$ = «Рішення забезпечує синхронізацію часу для забезпечення

точно фіксування часу в подіях:»; $\mathbf{R}_4$ = «Постачальник хмарних сервісів має вбудовану систему Управління Вразливостями, що дозволяє підтримувати системи в актуальному та захищеному стані:»; $\mathbf{R}_5$ = «Постачальник хмарних сервісів має вбудовану систему виявлення аномалій в мережевому трафіку:»; $\mathbf{R}_6$ = «Постачальник хмарних сервісів проводить сегментацію для підтримуваних додатків:»; $\mathbf{R}_7$ = «Постачальник хмарних сервісів налаштовує безпечний та шифрований канал передачі даних між фізичними серверами, додатками, базами даних тощо:»; $\mathbf{R}_8$ = «Постачальник хмарних послуг має сервіс для перевірки функціонування всіх сервісів замовника:»; $\mathbf{R}_9$ = «Постачальник хмарних сервісів має вбудовану систему управління обліковими даних та впроваджену парольну політику для користувачів:»; $\mathbf{R}_{10}$ = «Постачальник хмарних послуг регулярно проводить сканування відкритого коду на предмет виявлення вразливостей у вихідному коді сервісу:»; $\mathbf{R}_{11}$ = «Рішення забезпечує можливість інтеграції із сторонніми рішеннями:»; $\mathbf{R}_{12}$ = «Рішення підтримує можливість відправки журналів подій та логів в Log Management / SIEM / SOAR систему у форматах syslog або json:»; $\mathbf{R}_{13}$ = «Рішення має вбудовану систему аналізу поведінки користувача на предмет виявлення бот активності:» [108].

Підмножину $\mathbf{R}_j$ визначимо як:

$$\mathbf{R}_j = \left\{ \bigcup_{k=1}^{m_{8j}} R_{jk} \right\} = \left\{ R_{j1}, R_{j2}, \ldots, R_{jm_{8j}} \right\} \tag{2.56}$$

де: $R_{jk} \subseteq \mathbf{R}_j$ $(k = \overline{1, m_{8j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{8j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.54) із урахуванням виразу (2.56) можна представити наступним чином:

$$\mathbf{R} = \left\{ \bigcup_{j=1}^{m_8} \mathbf{R}_j \right\} = \left\{ \bigcup_{j=1}^{m_8} \left\{ \bigcup_{k=1}^{m_{8j}} R_{jk} \right\} \right\} = \{\{R_{11}, R_{12}, \ldots, R_{1m_{8j}}\},$$
$$\{R_{21}, R_{22}, \ldots, R_{2m_{8j}}\}, \ldots, \{R_{m_8 1}, R_{m_8 2}, \ldots, R_{m_8 m_{8j}}\}\}, \quad (2.57)$$

Наприклад, при $m_8 = 13$ ($j = \overline{1,13}$), $m_{81} = 2$ ($k = \overline{1,2}$), $m_{82} = 2$ ($k = \overline{1,2}$), $m_{83} = 2$ ($k = \overline{1,2}$), $m_{84} = 2$ ($k = \overline{1,2}$), $m_{85} = 2$ ($k = \overline{1,2}$), $m_{86} = 2$ ($k = \overline{1,2}$), $m_{87} = 2$ ($k = \overline{1,2}$), $m_{88} = 2$ ($k = \overline{1,2}$), $m_{89} = 2$ ($k = \overline{1,2}$), $m_{810} = 2$ ($k = \overline{1,2}$), $m_{811} = 2$ ($k = \overline{1,2}$), $m_{812} = 2$ ($k = \overline{1,2}$), $m_{813} = 2$ ($k = \overline{1,2}$), формула (2.57) набуде наступного вигляду:

$$\mathbf{R} = \left\{ \bigcup_{j=1}^{13} \mathbf{R}_j \right\} = \left\{ \bigcup_{j=1}^{13} \left\{ \bigcup_{k=1}^{m_{8j}} R_{jk} \right\} \right\} = \{\{R_{11}, R_{12}\}, \{R_{21}, R_{22}\}, \{R_{31}, R_{32}\},$$
$$\{R_{41}, R_{42}\}, \{R_{51}, R_{52}\}, \{R_{61}, R_{62}\}, \{R_{71}, R_{72}\}, \{R_{81}, R_{82}\},$$
$$\{R_{91}, R_{92}\}, \{R_{101}, R_{102}\}, \{R_{111}, R_{112}\}, \{R_{121}, R_{122}\}, \{R_{131}, R_{132}\}\}, \quad (2.58)$$

де: R_{11} = «Так»; R_{12} = «Ні»; R_{21} = «Так»; R_{22} = «Ні»; R_{31} = «Так»; R_{32} = «Ні»; R_{41} = «Так»; R_{42} = «Ні»; R_{51} = «Так»; R_{52} = «Ні»; R_{61} = «Так»; R_{62} = «Ні»; R_{71} = «Так»; R_{72} = «Ні»; R_{81} = «Так»; R_{82} = «Ні»; R_{91} = «Так»; R_{92} = «Ні»; R_{101} = «Так»; R_{102} = «Ні» ; R_{111} = «Так»; R_{112} = «Ні» ; R_{121} = «Так»; R_{122} = «Ні» ; R_{131} = «Так»; R_{132} = «Ні» [108].

Дев'ятий компонент узагальненої математичної моделі **A** – модуль, що оцінює стан захищеності розгорнутого програмного забезпечення на ресурсах хмарного сервісу, визначається виразом:

$$\mathbf{A} = \left\{ \bigcup_{j=1}^{m_9} \mathbf{A}_j \right\} = \left\{ \mathbf{A}_1, \mathbf{A}_2 \ldots, \mathbf{A}_{m_9} \right\}, \quad (2.59)$$

де: $\mathbf{A}_j \subseteq \mathbf{A}$ ($j = \overline{1,m_9}$) – j-й параметр оцінки захищеності розгорнутого програмного забезпечення, а m_9 – їх кількість [101].

Наприклад, при $m_9 = 10$ ($j = \overline{1,10}$) формулу (2.59) можна представити як:

$$\mathbf{A} = \left\{ \bigcup_{j=1}^{10} \mathbf{A}_j \right\} = \left\{ \mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5, \mathbf{A}_6, \mathbf{A}_7, \mathbf{A}_8, \mathbf{A}_9, \mathbf{A}_{10} \right\}, \quad (2.60)$$

де, відповідно: $\mathbf{A}_1$ = «Постачальник хмарних сервісів забезпечує регулярне оновлення підтримуваних компонентів сервісу для забезпечення безперервного та безпечного функціонування всіх сервісів додатку:»; $\mathbf{A}_2$ = «Постачальник хмарних сервісів регулярно випускає оновлення власного програмного забезпечення та збільшує функціональні можливості рішення:»; $\mathbf{A}_3$ = «Постачальник хмарних сервісів для розробки програмного продукту залучає:»; $\mathbf{A}_4$ = «Постачальник хмарних сервісів встановлює тільки дозволений перелік програмного забезпечення на підтримувані системи замовника:»; $\mathbf{A}_5$ = «Рішення фіксує всіх зміни, що відбуваються на підтримуваних системах замовника:»; $\mathbf{A}_6$ = «Постачальник хмарних сервісів проводить навчання співробітників компанії та замовників щодо можливості запобігання потрапляння зловмисного програмного забезпечення в середовище компанії та мобільні пристрої:»; $\mathbf{A}_7$ = «Постачальник хмарних сервісів визначає перелік необхідного програмного забезпечення, що необхідне для роботи з сервісом:»; $\mathbf{A}_8$ = «Постачальник хмарних сервісів розробляє крос-платформенні додатки, що підтримуються на різноманітних типах пристроїв:»; $\mathbf{A}_9$ = «Постачальник хмарних сервісів регулярно проводить інвентаризацію активів для виявлення всіх легітимних та нелегітимних додатків:»; $\mathbf{A}_{10}$ = «Постачальник хмарних сервісів має вбудовану систему захисту веб-додатку замовника:» [108].

Підмножину $\mathbf{A}_j$ визначимо як:

$$\mathbf{A}_j = \left\{ \bigcup_{k=1}^{m_{9j}} A_{jk} \right\} = \left\{ A_{j1}, A_{j2}, \ldots, A_{jm_{9j}} \right\} \tag{2.61}$$

де: $A_{jk} \subseteq A_j$ $(k = \overline{1, m_{9j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{9j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.59) із урахуванням виразу (2.61) можна представити наступним чином:

$$\mathbf{A} = \left\{ \bigcup_{j=1}^{m_9} \mathbf{A_j} \right\} = \left\{ \bigcup_{j=1}^{m_9} \left\{ \bigcup_{k=1}^{m_{9j}} A_{jk} \right\} \right\} = \{\{A_{11}, A_{12}, ..., A_{1m_{9j}}\},$$
$$\{A_{21}, A_{22}, ..., A_{2m_{9j}}\}, ..., \{A_{m_9 1}, A_{m_9 2}, ..., A_{m_9 m_{9j}}\}\}, \quad (2.62)$$

Наприклад, при $m_9 = 10$ ($j = \overline{1,10}$), $m_{91} = 2$ ($k = \overline{1,2}$), $m_{92} = 2$ ($k = \overline{1,2}$), $m_{93} = 3$ ($k = \overline{1,3}$), $m_{94} = 2$ ($k = \overline{1,2}$), $m_{95} = 2$ ($k = \overline{1,2}$), $m_{96} = 2$ ($k = \overline{1,2}$), $m_{97} = 2$ ($k = \overline{1,2}$), $m_{98} = 2$ ($k = \overline{1,2}$), $m_{99} = 2$ ($k = \overline{1,2}$), $m_{910} = 2$ ($k = \overline{1,2}$), формула (2.62) набуде наступного вигляду:

$$\mathbf{A} = \left\{ \bigcup_{j=1}^{10} \mathbf{A_j} \right\} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{9j}} A_{jk} \right\} \right\} = \{\{A_{11}, A_{12}\}, \{A_{21}, A_{22}\},$$
$$\{A_{31}, A_{32}, A_{33}\}, \{A_{41}, A_{42}\}, \{A_{51}, A_{52}\}, \{A_{61}, A_{62}\},$$
$$\{A_{71}, A_{72}\}, \{A_{81}, A_{82}\}, \{A_{91}, A_{92}\}, \{A_{101}, A_{102}\}\}, \quad (2.63)$$

де: A_{11} = «Так»; A_{12} = «Ні»; A_{21} = «Так»; A_{22} = «Ні»; A_{31} = «Власний персонал»; A_{32} = «Субпідрядні організації»; A_{33} = «Нікого не залучає»; A_{41} = «Так»; A_{42} = «Ні»; A_{51} = «Так»; A_{52} = «Ні»; A_{61} = «Так»; A_{62} = «Ні»; A_{71} = «Так»; A_{72} = «Ні»; A_{81} = «Так»; A_{82} = «Ні»; A_{91} = «Так»; A_{92} = «Ні»; A_{101} = «Так»; A_{102} = «Ні» [108].

Десятий компонент узагальненої математичної моделі **D** – модуль, що оцінює стан захищеності даних компанії, що циркулюють на ресурсах постачальника хмарного сервісу, визначається виразом:

$$\mathbf{D} = \left\{ \bigcup_{j=1}^{m_{10}} \mathbf{D_j} \right\} = \left\{ \mathbf{D_1}, \mathbf{D_2} ..., \mathbf{D_{m_{10}}} \right\}, \quad (2.64)$$

де: $\mathbf{D_j} \subseteq \mathbf{D}$ ($j = \overline{1, m_{10}}$) – j-й параметр оцінки стану захищеності даних компанії, а m_{10} – їх кількість [101].

Наприклад, при $m_{10} = 12$ ($j = \overline{1,12}$) формулу (2.64) можна представити як:

$$\mathbf{D} = \left\{ \bigcup_{j=1}^{12} \mathbf{D_j} \right\} = \left\{ \begin{matrix} \mathbf{D_1}, \mathbf{D_2}, \mathbf{D_3}, \mathbf{D_4}, \mathbf{D_5}, \mathbf{D_6}, \\ \mathbf{D_7}, \mathbf{D_8}, \mathbf{D_9}, \mathbf{D_{10}}, \mathbf{D_{11}}, \mathbf{D_{12}} \end{matrix} \right\}, \quad (2.65)$$

де, відповідно: $\mathbf{D_1}$ = «Рішення проводить класифікацію даних (Data Classification), що обробляється ресурсами хмарного сервісу:»; $\mathbf{D_2}$ = «Рішення

проводить виявлення типів файлів (pdf, docx, exe etc), що передається між ресурсами хмарного сервісу:»; $\mathbf{D}_3$ = «Постачальник хмарних сервісів щоразу, перед запуском нового програмного продукту проводить тестування якості написаного коду для виявлення помилкових спрацювань:»; $\mathbf{D}_4$ = «Постачальник хмарних сервісів документує всі зміни, що проводяться в системі та надає дану інформацію замовнику:»; $\mathbf{D}_5$ = «Постачальник хмарних сервісів в межах власного програмного продукту дозволяє замовнику розмежовувати доступ до ресурсів хмарних сервісів між власними співробітниками/підрядниками:»; $\mathbf{D}_6$ = «Постачальник хмарних сервісів сповіщає замовників про початок проведення регламентних робіт у власних системах:»; $\mathbf{D}_7$ = «Постачальник хмарних сервісів надає інформацію замовнику у випадку виявлення збоїв в роботі модулів системи:»; $\mathbf{D}_8$ = «Постачальник хмарних сервісів власними силами забезпечує оновлення розробленого програмного рішення, надаючи замовнику лише посилання на вхід до консолі управління рішення:»; $\mathbf{D}_9$ = «Постачальник хмарних сервісів використовує систему попередження витоку конфіденційних даних (DLP) за межі компанії:»; $\mathbf{D}_{10}$ = «Постачальник хмарних сервісів надає замовнику доступ до порталу підтримки, для можливості створення заявок команді технічної підтримки системи:»; $\mathbf{D}_{11}$ = «Постачальник хмарних сервісів має детально описаний документ SLA:»; $\mathbf{D}_{12}$ = «Постачальник хмарних сервісів проводить на менше ніж 1 раз на рік тестування на проникнення власних систем:» [108].

Підмножину $\mathbf{D}_j$ визначимо як:

$$\mathbf{D}_j = \left\{ \bigcup_{k=1}^{m_{10j}} D_{jk} \right\} = \left\{ D_{j1}, D_{j2}, \ldots, D_{jm_{10j}} \right\} \tag{2.66}$$

де: $D_{jk} \subseteq \mathbf{D}_j$ $(k = \overline{1, m_{10j}})$ – k-а підмножина груп оцінок, що є близькими за визначеними характеристиками і оцінюваними параметрами j-ї підмножини, m_{10j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.64) із урахуванням виразу (2.66) можна представити наступним чином:

$$\mathbf{D} = \left\{ \bigcup_{j=1}^{m_{10}} \mathbf{D}_j \right\} = \left\{ \bigcup_{j=1}^{m_{10}} \left\{ \bigcup_{k=1}^{m_{10j}} D_{jk} \right\} \right\} = \{\{D_{11}, D_{12}, ..., D_{1m_{10j}}\}, \{D_{21}, D_{22}, ..., D_{2m_{10j}}\}, ..., \{D_{m_{10}1}, D_{m_{10}2}, ..., D_{m_{10}m_{10j}}\}\}, \quad (2.67)$$

Наприклад, при $m_{10} = 12$ ($j = \overline{1,12}$), $m_{101} = 2$ ($k = \overline{1,2}$), $m_{102} = 2$ ($k = \overline{1,2}$), $m_{103} = 2$ ($k = \overline{1,2}$), $m_{104} = 2$ ($k = \overline{1,2}$), $m_{105} = 2$ ($k = \overline{1,2}$), $m_{106} = 2$ ($k = \overline{1,2}$), $m_{107} = 2$ ($k = \overline{1,2}$), $m_{108} = 2$ ($k = \overline{1,2}$), $m_{109} = 2$ ($k = \overline{1,2}$), $m_{1010} = 2$ ($k = \overline{1,2}$), $m_{1011} = 2$ ($k = \overline{1,2}$), $m_{1012} = 2$ ($k = \overline{1,2}$), формула (2.67) набуде наступного вигляду:

$$\mathbf{D} = \left\{ \bigcup_{j=1}^{12} \mathbf{D}_j \right\} = \left\{ \bigcup_{j=1}^{12} \left\{ \bigcup_{k=1}^{m_{10j}} D_{jk} \right\} \right\} = \{\{D_{11}, D_{12}\}, \{D_{21}, D_{22}\}, \{D_{31}, D_{32}\}, \{D_{41}, D_{42}\}, \{D_{51}, D_{52}\}, \{D_{61}, D_{62}\}, \{D_{71}, D_{72}\}, \{D_{81}, D_{82}\}, \{D_{91}, D_{92}\}, \{D_{101}, D_{102}\}, \{D_{111}, D_{112}\}, \{D_{121}, D_{122}\}\}, \quad (2.68)$$

де: D_{11} = «Так»; D_{12} = «Ні»; D_{21} = «Так»; D_{22} = «Ні»; D_{31} = «Так»; D_{32} = «Ні»; D_{41} = «Так»; D_{42} = «Ні»; D_{51} = «Так»; D_{52} = «Ні»; D_{61} = «Так»; D_{62} = «Ні»; D_{71} = «Так»; D_{72} = «Ні»; D_{81} = «Так»; D_{82} = «Ні»; D_{91} = «Так»; D_{92} = «Ні»; D_{101} = «Так»; D_{102} = «Ні» [108].

Одинадцятий компонент узагальненої математичної моделі **RE** – модуль, що визначає набір рекомендацій, що є необхідними для прийняття фінального рішення, щодо вибору постачальника хмарного сервісу та застосовуються для всіх компонент від 2 до 10, визначається виразом:

$$\mathbf{RE} = \left\{ \bigcup_{j=1}^{m_{11}} \mathbf{RE}_j \right\} = \left\{ \mathbf{RE}_1, \mathbf{RE}_2 ..., \mathbf{RE}_{m_{11}} \right\}, \quad (2.69)$$

де: $\mathbf{RE}_j \subseteq \mathbf{RE}$ ($j = \overline{1, m_{11}}$) – j-й параметр групи рекомендацій для кожного із параметрів оцінки захищеності хмарного сервісу, а m_{11} – їх кількість [101].

Враховуючи, що на представлено 9 параметрів оцінки захищеності хмарного сервісу, то змінна m_{11} є константою і становить 9 підмножин, а саме $m_{11} = 9$ ($j = \overline{1,9}$) і формулу (2.69) можна представити як:

$$\mathbf{RE} = \left\{ \bigcup_{j=1}^{9} \mathbf{RE}_j \right\} = \left\{ \begin{matrix} \mathbf{RE}_1, \mathbf{RE}_2, \mathbf{RE}_3, \mathbf{RE}_4, \mathbf{RE}_5, \\ \mathbf{RE}_6, \mathbf{RE}_7, \mathbf{RE}_8, \mathbf{RE}_9 \end{matrix} \right\}, \tag{2.70}$$

де, відповідно: $\mathbf{RE}_1$ = «Рекомендації для компоненти N»; $\mathbf{RE}_2$ = «Рекомендації для компоненти S»; $\mathbf{RE}_3$ = «Рекомендації для компоненти SR»; $\mathbf{RE}_4$ = «Рекомендації для компоненти V»; $\mathbf{RE}_5$ = «Рекомендації для компоненти OS»; $\mathbf{RE}_6$ = «Рекомендації для компоненти CT»; $\mathbf{RE}_7$ = «Рекомендації для компоненти R»; $\mathbf{RE}_8$ = «Рекомендації для компоненти A»; $\mathbf{RE}_9$ = «Рекомендації для компоненти D» [108].

Підмножину $\mathbf{RE}_j$ визначимо як:

$$\mathbf{RE}_j = \left\{ \bigcup_{k=1}^{m_{11j}} RE_{jk} \right\} = \left\{ RE_{j1}, RE_{j2}, \ldots, RE_{jm_{11j}} \right\} \tag{2.71}$$

де: $RE_{jk} \subseteq \mathbf{RE}_j$ ($k = \overline{1, m_{11j}}$) – k-а підмножина груп рекомендацій, що визначаються індивідуально для кожного параметру оцінки і оцінюваними параметрами j-ї підмножини, m_{11j} – кількість груп j-ї підмножини [108].

Відповідно вираз (2.69) із урахуванням виразу (2.71) можна представити наступним чином:

$$\begin{aligned} \mathbf{RE} = \left\{ \bigcup_{j=1}^{m_{11}} \mathbf{RE}_j \right\} = \left\{ \bigcup_{j=1}^{m_{11}} \left\{ \bigcup_{k=1}^{m_{11j}} RE_{jk} \right\} \right\} = \{ \{ RE_{11}, RE_{12}, \ldots, RE_{1m_{11j}} \}, \\ \{ RE_{21}, RE_{22}, \ldots, RE_{2m_{11j}} \}, \ldots, \{ RE_{m_{11}1}, RE_{m_{11}2}, \ldots, RE_{m_{11}m_{11j}} \} \}, \end{aligned} \tag{2.72}$$

Наприклад, при $m_{11} = 9$ ($j = \overline{1,9}$), $m_{111} = 10$ ($k = \overline{1,10}$), $m_{112} = 10$ ($k = \overline{1,10}$), $m_{113} = 12$ ($k = \overline{1,12}$), $m_{114} = 10$ ($k = \overline{1,10}$), $m_{115} = 11$ ($k = \overline{1,11}$), $m_{116} = 10$ ($k = \overline{1,10}$), $m_{117} = 13$ ($k = \overline{1,13}$), $m_{118} = 10$ ($k = \overline{1,10}$), $m_{119} = 12$ ($k = \overline{1,12}$), формула (2.72) набуде наступного вигляду:

$$\mathbf{RE} = \left\{ \bigcup_{j=1}^{9} \mathbf{RE}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{9} \left\{ \bigcup_{k=1}^{m_{11j}} \mathbf{RE}_{\mathbf{jk}} \right\} \right\} =$$

$$\{\{\mathbf{RE}_{11}, \mathbf{RE}_{12}, \mathbf{RE}_{13}, \mathbf{RE}_{14}, \mathbf{RE}_{15}, \mathbf{RE}_{16}, \mathbf{RE}_{17}, \mathbf{RE}_{18}, \mathbf{RE}_{19}, \mathbf{RE}_{110}\},$$
$$\{\mathbf{RE}_{21}, \mathbf{RE}_{22}, \mathbf{RE}_{23}, \mathbf{RE}_{24}, \mathbf{RE}_{25}, \mathbf{RE}_{26}, \mathbf{RE}_{27}, \mathbf{RE}_{28}, \mathbf{RE}_{29}, \mathbf{RE}_{210}\},$$
$$\{\mathbf{RE}_{31}, \mathbf{RE}_{32}, \mathbf{RE}_{33}, \mathbf{RE}_{34}, \mathbf{RE}_{35}, \mathbf{RE}_{36}, \mathbf{RE}_{37}, \mathbf{RE}_{38}, \mathbf{RE}_{39}, \mathbf{RE}_{310},$$
$$\mathbf{RE}_{311}, \mathbf{RE}_{312}\},$$
$$\{\mathbf{RE}_{41}, \mathbf{RE}_{42}, \mathbf{RE}_{43}, \mathbf{RE}_{44}, \mathbf{RE}_{45}, \mathbf{RE}_{46}, \mathbf{RE}_{47}, \mathbf{RE}_{48}, \mathbf{RE}_{49}, \mathbf{RE}_{410}\}, \quad (2.73)$$
$$\{\mathbf{RE}_{51}, \mathbf{RE}_{52}, \mathbf{RE}_{53}, \mathbf{RE}_{54}, \mathbf{RE}_{55}, \mathbf{RE}_{56}, \mathbf{RE}_{57}, \mathbf{RE}_{58}, \mathbf{RE}_{59}, \mathbf{RE}_{510}, \mathbf{RE}_{511}\},$$
$$\{\mathbf{RE}_{61}, \mathbf{RE}_{62}, \mathbf{RE}_{63}, \mathbf{RE}_{64}, \mathbf{RE}_{65}, \mathbf{RE}_{66}, \mathbf{RE}_{67}, \mathbf{RE}_{68}, \mathbf{RE}_{69}, \mathbf{RE}_{610}\},$$
$$\{\mathbf{RE}_{71}, \mathbf{RE}_{72}, \mathbf{RE}_{73}, \mathbf{RE}_{74}, \mathbf{RE}_{75}, \mathbf{RE}_{76}, \mathbf{RE}_{77}, \mathbf{RE}_{78}, \mathbf{RE}_{79}, \mathbf{RE}_{710}, \mathbf{RE}_{711},$$
$$\mathbf{RE}_{712}, \mathbf{RE}_{713}\},$$
$$\{\mathbf{RE}_{81}, \mathbf{RE}_{82}, \mathbf{RE}_{83}, \mathbf{RE}_{84}, \mathbf{RE}_{85}, \mathbf{RE}_{86}, \mathbf{RE}_{87}, \mathbf{RE}_{88}, \mathbf{RE}_{89}, \mathbf{RE}_{810}\},$$
$$\{\mathbf{RE}_{91}, \mathbf{RE}_{92}, \mathbf{RE}_{93}, \mathbf{RE}_{94}, \mathbf{RE}_{95}, \mathbf{RE}_{96}, \mathbf{RE}_{97}, \mathbf{RE}_{98}, \mathbf{RE}_{99}, \mathbf{RE}_{910},$$
$$\mathbf{RE}_{911}, \mathbf{RE}_{912}\}\},$$

де: $\mathbf{RE}_{11}$ = «Питання 1»; $\mathbf{RE}_{12}$ = «Питання 2»; $\mathbf{RE}_{13}$ = «Питання 3»; $\mathbf{RE}_{14}$ = «Питання 4»; $\mathbf{RE}_{15}$ = «Питання 5»; $\mathbf{RE}_{16}$ = «Питання 6»; $\mathbf{RE}_{17}$ = «Питання 7»; $\mathbf{RE}_{18}$ = «Питання 8»; $\mathbf{RE}_{19}$ = «Питання 9»; $\mathbf{RE}_{110}$ = «Питання 10»;

$\mathbf{RE}_{21}$ = «Питання 1»; $\mathbf{RE}_{22}$ = «Питання 2»; $\mathbf{RE}_{23}$ = «Питання 3»; $\mathbf{RE}_{24}$ = «Питання 4»; $\mathbf{RE}_{25}$ = «Питання 5»; $\mathbf{RE}_{26}$ = «Питання 6»; $\mathbf{RE}_{27}$ = «Питання 7»; $\mathbf{RE}_{28}$ = «Питання 8»; $\mathbf{RE}_{29}$ = «Питання 9»; $\mathbf{RE}_{210}$ = «Питання 10»;

$\mathbf{RE}_{31}$ = «Питання 1»; $\mathbf{RE}_{32}$ = «Питання 2»; $\mathbf{RE}_{33}$ = «Питання 3»; $\mathbf{RE}_{34}$ = «Питання 4»; $\mathbf{RE}_{35}$ = «Питання 5»; $\mathbf{RE}_{36}$ = «Питання 6»; $\mathbf{RE}_{37}$ = «Питання 7»; $\mathbf{RE}_{38}$ = «Питання 8»; $\mathbf{RE}_{39}$ = «Питання 9»; $\mathbf{RE}_{310}$ = «Питання 10»; $\mathbf{RE}_{311}$ = «Питання 11»; $\mathbf{RE}_{312}$ = «Питання 12»;

$\mathbf{RE}_{41}$ = «Питання 1»; $\mathbf{RE}_{42}$ = «Питання 2»; $\mathbf{RE}_{43}$ = «Питання 3»; $\mathbf{RE}_{44}$ = «Питання 4»; $\mathbf{RE}_{45}$ = «Питання 5»; $\mathbf{RE}_{46}$ = «Питання 6»; $\mathbf{RE}_{47}$ = «Питання 7»; $\mathbf{RE}_{48}$ = «Питання 8»; $\mathbf{RE}_{49}$ = «Питання 9»; $\mathbf{RE}_{410}$ = «Питання 10»;

$\mathbf{RE}_{51}$ = «Питання 1»; $\mathbf{RE}_{52}$ = «Питання 2»; $\mathbf{RE}_{53}$ = «Питання 3»; $\mathbf{RE}_{54}$ = «Питання 4»; $\mathbf{RE}_{55}$ = «Питання 5»; $\mathbf{RE}_{56}$ = «Питання 6»; $\mathbf{RE}_{57}$ = «Питання

7»; $\mathbf{RE}_{58}$ = «Питання 8»; $\mathbf{RE}_{59}$ = «Питання 9»; $\mathbf{RE}_{510}$ = «Питання 10»; $\mathbf{RE}_{511}$ = «Питання 11»;

$\mathbf{RE}_{61}$ = «Питання 1»; $\mathbf{RE}_{62}$ = «Питання 2»; $\mathbf{RE}_{63}$ = «Питання 3»; $\mathbf{RE}_{64}$ = «Питання 4»; $\mathbf{RE}_{65}$ = «Питання 5»; $\mathbf{RE}_{66}$ = «Питання 6»; $\mathbf{RE}_{67}$ = «Питання 7»; $\mathbf{RE}_{68}$ = «Питання 8»; $\mathbf{RE}_{69}$ = «Питання 9»; $\mathbf{RE}_{610}$ = «Питання 10»;

$\mathbf{RE}_{71}$ = «Питання 1»; $\mathbf{RE}_{72}$ = «Питання 2»; $\mathbf{RE}_{73}$ = «Питання 3»; $\mathbf{RE}_{74}$ = «Питання 4»; $\mathbf{RE}_{75}$ = «Питання 5»; $\mathbf{RE}_{76}$ = «Питання 6»; $\mathbf{RE}_{77}$ = «Питання 7»; $\mathbf{RE}_{78}$ = «Питання 8»; $\mathbf{RE}_{79}$ = «Питання 9»; $\mathbf{RE}_{710}$ = «Питання 10»; $\mathbf{RE}_{711}$ = «Питання 11»; $\mathbf{RE}_{712}$ = «Питання 12»; $\mathbf{RE}_{713}$ = «Питання 13»;

$\mathbf{RE}_{81}$ = «Питання 1»; $\mathbf{RE}_{82}$ = «Питання 2»; $\mathbf{RE}_{83}$ = «Питання 3»; $\mathbf{RE}_{84}$ = «Питання 4»; $\mathbf{RE}_{85}$ = «Питання 5»; $\mathbf{RE}_{86}$ = «Питання 6»; $\mathbf{RE}_{87}$ = «Питання 7»; $\mathbf{RE}_{88}$ = «Питання 8»; $\mathbf{RE}_{89}$ = «Питання 9»; $\mathbf{RE}_{810}$ = «Питання 10»;

$\mathbf{RE}_{91}$ = «Питання 1»; $\mathbf{RE}_{92}$ = «Питання 2»; $\mathbf{RE}_{93}$ = «Питання 3»; $\mathbf{RE}_{94}$ = «Питання 4»; $\mathbf{RE}_{95}$ = «Питання 5»; $\mathbf{RE}_{96}$ = «Питання 6»; $\mathbf{RE}_{97}$ = «Питання 7»; $\mathbf{RE}_{98}$ = «Питання 8»; $\mathbf{RE}_{99}$ = «Питання 9»; $\mathbf{RE}_{910}$ = «Питання 10»; $\mathbf{RE}_{911}$ = «Питання 11»; $\mathbf{RE}_{912}$ = «Питання 12» [108].

Підмножину $\mathbf{RE}_{jk}$ визначимо як:

$$\mathbf{RE}_{jk} = \left\{ \bigcup_{l=1}^{m_{11jk}} RE_{jkl} \right\} = \left\{ RE_{jk1}, RE_{jk2}, \ldots, RE_{jkm_{11jk}} \right\} \tag{2.74}$$

де: $RE_{jkl} \subseteq \mathbf{RE}_{jk}$ $(l = \overline{1, m_{11jk}})$ – l-а підмножина груп рекомендацій для груп запитань та відповідних відповідей, що відповідають оцінюваними параметрами k-ї підмножини, що забезпечують оцінку захищеності сервісів хмарного провайдера першого порядку, m_{11jk} – кількість груп k-ї підмножини [108].

Відповідно вираз (2.72) із урахуванням виразу (2.74) можна представити наступним чином:

$$\mathbf{RE} = \left\{ \bigcup_{j=1}^{m_{11}} \mathbf{RE}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{m_{11}} \left\{ \bigcup_{k=1}^{m_{11j}} \mathbf{RE}_{\mathbf{jk}} \right\} \right\} = \left\{ \bigcup_{j=1}^{m_{11}} \left\{ \bigcup_{k=1}^{m_{11j}} \left\{ \bigcup_{l=1}^{m_{11jk}} RE_{jkl} \right\} \right\} \right\} =$$

$$\{\{\{RE_{111}, RE_{112}, \ldots, RE_{11m_{11jk}}\}, \{RE_{121}, RE_{122}, \ldots, RE_{12m_{11jk}}\}, \ldots,$$

$$\{RE_{1m_{11j}1}, RE_{1m_{11j}2}, \ldots, RE_{1m_{11j}m_{11jk}}\}\},$$

$$\{\{RE_{211}, RE_{212}, \ldots, RE_{21m_{11jk}}\}, \{RE_{221}, RE_{222}, \ldots, RE_{22m_{11jk}}\}, \ldots,$$

$$\{RE_{2m_{11j}1}, RE_{2m_{11j}2}, \ldots, RE_{2m_{11j}m_{11jk}}\}\}, \ldots,$$

$$\{\{RE_{m_{11}11}, RE_{m_{11}12}, \ldots, RE_{m_{11}1m_{11jk}}\}, \{RE_{m_{11}21}, RE_{m_{11}22}, \ldots, RE_{m_{11}2m_{11jk}}\}, \ldots,$$

$$\{RE_{m_{11}m_{11j}1}, RE_{m_{11}m_{11j}2}, \ldots, RE_{m_{11}m_{11j}m_{11jk}}\}\}\}, \quad (2.75)$$

Наприклад, для $m_{11} = 9$ ($j = \overline{1,9}$), маємо наступну кількість відповідей для кожного набору запитань:

- Оскільки $m_{111} = 10$ ($k = \overline{1,10}$), то $m_{1111} = 6$ ($k = \overline{1,6}$), $m_{1112} = 6$ ($k = \overline{1,6}$), $m_{1113} = 6$ ($k = \overline{1,6}$), $m_{1114} = 2$ ($k = \overline{1,2}$), $m_{1115} = 2$ ($k = \overline{1,2}$), $m_{1116} = 2$ ($k = \overline{1,2}$), $m_{1117} = 2$ ($k = \overline{1,2}$), $m_{1118} = 2$ ($k = \overline{1,2}$), $m_{1119} = 2$ ($k = \overline{1,2}$), $m_{11110} = 2$ ($k = \overline{1,2}$).

- Оскільки $m_{112} = 10$ ($k = \overline{1,10}$), то $m_{1121} = 2$ ($k = \overline{1,2}$), $m_{1122} = 2$ ($k = \overline{1,2}$), $m_{1123} = 2$ ($k = \overline{1,2}$), $m_{1124} = 2$ ($k = \overline{1,2}$), $m_{1125} = 2$ ($k = \overline{1,2}$), $m_{1126} = 2$ ($k = \overline{1,2}$), $m_{1127} = 2$ ($k = \overline{1,2}$), $m_{1128} = 2$ ($k = \overline{1,2}$), $m_{1129} = 2$ ($k = \overline{1,2}$), $m_{11210} = 2$ ($k = \overline{1,2}$).

- Оскільки $m_{113} = 12$ ($k = \overline{1,12}$), то $m_{1131} = 4$ ($k = \overline{1,4}$), $m_{1132} = 2$ ($k = \overline{1,2}$), $m_{1133} = 6$ ($k = \overline{1,6}$), $m_{1134} = 2$ ($k = \overline{1,2}$), $m_{1135} = 2$ ($k = \overline{1,2}$), $m_{1136} = 2$ ($k = \overline{1,2}$), $m_{1137} = 2$ ($k = \overline{1,2}$), $m_{1138} = 2$ ($k = \overline{1,2}$), $m_{1139} = 3$ ($k = \overline{1,3}$), $m_{11310} = 4$ ($k = \overline{1,4}$), $m_{11311} = 3$ ($k = \overline{1,3}$), $m_{11312} = 3$ ($k = \overline{1,3}$).

- Оскільки $m_{114} = 10$ ($k = \overline{1,10}$), то $m_{1141} = 7$ ($k = \overline{1,7}$), $m_{1142} = 2$ ($k = \overline{1,2}$), $m_{1143} = 2$ ($k = \overline{1,2}$), $m_{1144} = 2$ ($k = \overline{1,2}$), $m_{1145} = 2$ ($k = \overline{1,2}$), $m_{1146} = 2$ ($k = \overline{1,2}$), $m_{1147} = 2$ ($k = \overline{1,2}$), $m_{1148} = 2$ ($k = \overline{1,2}$), $m_{1149} = 2$ ($k = \overline{1,2}$), $m_{11410} = 2$ ($k = \overline{1,2}$).

- Оскільки $m_{115} = 11$ ($k = \overline{1,11}$), то $m_{1151} = 5$ ($k = \overline{1,5}$), $m_{1152} = 2$ ($k = \overline{1,2}$), $m_{1153} = 6$ ($k = \overline{1,6}$), $m_{1154} = 2$ ($k = \overline{1,2}$), $m_{1155} = 2$ ($k = \overline{1,2}$), $m_{1156} = 2$ ($k = \overline{1,2}$),

$m_{1157}=2\ (k=\overline{1,2})$, $m_{1158}=2\ (k=\overline{1,2})$, $m_{1159}=2\ (k=\overline{1,2})$, $m_{11510}=2\ (k=\overline{1,2})$, $m_{11511}=2\ (k=\overline{1,2})$.

- Оскільки $m_{116}=10\ (k=\overline{1,10})$, то $m_{1161}=2\ (k=\overline{1,2})$, $m_{1162}=2\ (k=\overline{1,2})$, $m_{1163}=2\ (k=\overline{1,2})$, $m_{1164}=2\ (k=\overline{1,2})$, $m_{1165}=2\ (k=\overline{1,2})$, $m_{1166}=2\ (k=\overline{1,2})$, $m_{1167}=2\ (k=\overline{1,2})$, $m_{1168}=2\ (k=\overline{1,2})$, $m_{1169}=2\ (k=\overline{1,2})$, $m_{11610}=2\ (k=\overline{1,2})$.

- Оскільки $m_{117}=13\ (k=\overline{1,13})$, то $m_{1171}=2\ (k=\overline{1,2})$, $m_{1172}=2\ (k=\overline{1,2})$, $m_{1173}=2\ (k=\overline{1,2})$, $m_{1174}=2\ (k=\overline{1,2})$, $m_{1175}=2\ (k=\overline{1,2})$, $m_{1176}=2\ (k=\overline{1,2})$, $m_{1177}=2\ (k=\overline{1,2})$, $m_{1178}=2\ (k=\overline{1,2})$, $m_{1179}=2\ (k=\overline{1,2})$, $m_{11710}=2\ (k=\overline{1,2})$, $m_{11711}=2\ (k=\overline{1,2})$, $m_{11712}=2\ (k=\overline{1,2})$, $m_{11713}=2\ (k=\overline{1,2})$.

- Оскільки $m_{118}=10\ (k=\overline{1,10})$, то $m_{1181}=2\ (k=\overline{1,2})$, $m_{1182}=2\ (k=\overline{1,2})$, $m_{1183}=3\ (k=\overline{1,3})$, $m_{1184}=2\ (k=\overline{1,2})$, $m_{1185}=2\ (k=\overline{1,2})$, $m_{1186}=2\ (k=\overline{1,2})$, $m_{1187}=2\ (k=\overline{1,2})$, $m_{1188}=2\ (k=\overline{1,2})$, $m_{1189}=2\ (k=\overline{1,2})$, $m_{11810}=2\ (k=\overline{1,2})$.

- Оскільки $m_{119}=12\ (k=\overline{1,12})$, то $m_{1191}=2\ (k=\overline{1,2})$, $m_{1192}=2\ (k=\overline{1,2})$, $m_{1193}=2\ (k=\overline{1,2})$, $m_{1194}=2\ (k=\overline{1,2})$, $m_{1195}=2\ (k=\overline{1,2})$, $m_{1196}=2\ (k=\overline{1,2})$, $m_{1197}=2\ (k=\overline{1,2})$, $m_{1198}=2\ (k=\overline{1,2})$, $m_{1199}=2\ (k=\overline{1,2})$, $m_{11910}=2\ (k=\overline{1,2})$, $m_{11911}=2\ (k=\overline{1,2})$, $m_{11912}=2\ (k=\overline{1,2})$ [108].

Враховуючи вище перераховані приклади, формула (2.75) набуде наступного вигляду:

$$\mathbf{RE} = \left\{ \bigcup_{j=1}^{9} \mathbf{RE}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{9} \left\{ \bigcup_{k=1}^{m_{11j}} \mathbf{RE}_{\mathbf{jk}} \right\} \right\} = \left\{ \bigcup_{j=1}^{9} \left\{ \bigcup_{k=1}^{m_{11j}} \left\{ \bigcup_{l=1}^{m_{11jk}} RE_{jkl} \right\} \right\} \right\} =$$

$$\{\{\{RE_{111}, RE_{112}, RE_{113}, RE_{114}, RE_{115}, RE_{116}\}, \{RE_{121}, RE_{122}, RE_{123}, RE_{124},$$
$$RE_{125}, RE_{126}\}, \{RE_{131}, RE_{132}, RE_{133}, RE_{134}, RE_{135}, RE_{136}\}, \{RE_{141}, RE_{142}\},$$
$$\{RE_{151}, RE_{152}\}, \{RE_{161}, RE_{162}\}, \{RE_{171}, RE_{172}\}, \{RE_{181}, RE_{182}\},$$
$$\{RE_{191}, RE_{192}\}, \{RE_{1101}, RE_{1102}\}\},$$
$$\{\{RE_{211}, RE_{212}\}, \{RE_{221}, RE_{222}\}, \{RE_{231}, RE_{232}\}, \{RE_{241}, RE_{242}\}, \{RE_{251}, RE_{252}\},$$
$$\{RE_{261}, RE_{262}\}, \{RE_{271}, RE_{272}\}, \{RE_{281}, RE_{282}\}, \{RE_{291}, RE_{292}\}, \{RE_{2101}, RE_{2102}\}\},$$
$$\{\{RE_{311}, RE_{312}, RE_{313}, RE_{314}\}, \{RE_{321}, RE_{322}\}, \{RE_{331}, RE_{332}, RE_{333}, RE_{334}, RE_{335},$$
$$RE_{336}\}, \{RE_{341}, RE_{342}\}, \{RE_{351}, RE_{352}\}, \{RE_{361}, RE_{362}\}, \{RE_{371}, RE_{372}\},$$
$$\{RE_{381}, RE_{382}\}, \{RE_{391}, RE_{392}, RE_{393}\}, \{RE_{3101}, RE_{3102}, RE_{3103}, RE_{3104}\},$$
$$\{RE_{3111}, RE_{3112}, RE_{3113}\}, \{RE_{3121}, RE_{3122}, RE_{3123}\}\},$$
$$\{\{RE_{411}, RE_{412}, RE_{413}, RE_{414}, RE_{415}, RE_{416}, RE_{417}\}, \{RE_{421}, RE_{422}\}, \{RE_{431}, RE_{432}\},$$
$$\{RE_{441}, RE_{442}\}, \{RE_{451}, RE_{452}\}, \{RE_{461}, RE_{462}\}, \{RE_{471}, RE_{472}\}, \{RE_{481}, RE_{482}\},$$
$$\{RE_{491}, RE_{492}\}, \{RE_{4101}, RE_{4102}\}\}, \quad (2.76)$$
$$\{\{RE_{511}, RE_{512}, RE_{513}, RE_{514}, RE_{515}\}, \{RE_{521}, RE_{522}\},$$
$$\{RE_{531}, RE_{532}\}, \{RE_{541}, RE_{542}\}, \{RE_{551}, RE_{552}\}, \{RE_{561}, RE_{562}\}, \{RE_{571}, RE_{572}\},$$
$$\{RE_{581}, RE_{582}\}, \{RE_{591}, RE_{592}\}, \{RE_{5101}, RE_{5102}\}, \{RE_{5111}, RE_{5112}\}\},$$
$$\{\{RE_{611}, RE_{612}\}, \{RE_{621}, RE_{622}\}, \{RE_{631}, RE_{632}\}, \{RE_{641}, RE_{642}\},$$
$$\{RE_{651}, RE_{652}\}, \{RE_{661}, RE_{662}\}, \{RE_{671}, RE_{672}\}, \{RE_{681}, RE_{682}\}, \{RE_{691}, RE_{692}\},$$
$$\{RE_{6101}, RE_{6102}\}\},$$
$$\{\{RE_{711}, RE_{712}\}, \{RE_{721}, RE_{722}\}, \{RE_{731}, RE_{732}\}, \{RE_{741}, RE_{742}\}, \{RE_{751}, RE_{752}\},$$
$$\{RE_{761}, RE_{762}\}, \{RE_{771}, RE_{772}\}, \{RE_{781}, RE_{782}\}, \{RE_{791}, RE_{792}\}, \{RE_{7101}, RE_{7102}\},$$
$$\{RE_{7111}, RE_{7112}\}, \{RE_{7121}, RE_{7122}\}, \{RE_{7131}, RE_{7132}\}\},$$
$$\{\{RE_{811}, RE_{812}\}, \{RE_{821}, RE_{822}\}, \{RE_{831}, RE_{832}, RE_{833}\}, \{RE_{841}, RE_{842}\},$$
$$\{RE_{851}, RE_{852}\}, \{RE_{861}, RE_{862}\}, \{RE_{871}, RE_{872}\}, \{RE_{881}, RE_{882}\}, \{RE_{891}, RE_{892}\},$$
$$\{RE_{8101}, RE_{8102}\}\},$$
$$\{\{RE_{911}, RE_{912}\}, \{RE_{921}, RE_{922}\}, \{RE_{931}, RE_{932}\}, \{RE_{941}, RE_{942}\}, \{RE_{951}, RE_{952}\},$$
$$\{RE_{961}, RE_{962}\}, \{RE_{971}, RE_{972}\}, \{RE_{981}, RE_{982}\}, \{RE_{991}, RE_{992}\},$$
$$\{RE_{9101}, RE_{9102}\}, \{RE_{9111}, RE_{9112}\}, \{RE_{9121}, RE_{9122}\}\}\},$$

де: $RE_{111} = RE_{112} = RE_{113} = RE_{114} = RE_{115} = RE_{116} =$ «Відповідно до вказаної градації рівня доступності варто враховувати, що зазначений час простою – це час, в який буде недоступний сервіс на стороні провайдера, тобто і сервіс, що розгорнутий на ресурсах хмарного провайдера. Це означає, що бізнес протягом часу простою буде недоступний для своїх клієнтів. Саме тому,

рекомендується звернути увагу на сервіси, які компанія планує розгорнути на ресурсах хмарного провайдера. Відповідно, якщо вашу компанію не задовольняє час простою хмарного сервісу на 1 рік (звісно, якщо це не максимальний рівень доступності 99.9999% з простоєм в 31.5 секунди на рік) та компанія має можливість виділити більший бюджет на закупку більш продуктивні ресурси на базі хмарних сервісах, то рекомендується розглянути хмарного провайдера, який має вищий рівень доступності та менший час простою на рік.»; $RE_{121} = RE_{122} = RE_{123} = RE_{124} = RE_{125} = RE_{126} =$ «Від кількості країн, в яких розгорнуті обчислювальні потужності хмарного сервісу, залежить час відгуку кожного із сервісів, що розгорнуті на ресурсах постачальника. Відповідно, чим більше країн, тим краща потужність і менший час затримки відповіді для клієнта, і навпаки. Також, рекомендується, використовувати найближчу точку присутності постачальника хмарного сервісу, наприклад, якщо ваші клієнти розташовуються в Україні, а найближчі точки присутності постачальника знаходяться в Польщі та Німеччині, рекомендується використовувати потужності, що розташовуються в Польщі для зменшення часу затримки між відповідями на запити клієнта. А у випадку, якщо у вас клієнти розташовуються по всьому світу, то рекомендується використовувати хмарний сервіс, що має найбільшу кількість точок присутності у країнах світу. У випадку, якщо вам достатньо зазначеної кількісті точок присутності у світі – ви можете сміло використовувати ресурси даного постачальника, проте, якщо потреби бізнесу не задовольняють країни присутності хмарного провайдера чи їх кількість та бізнес готовий виділити більший бюджет на продуктивнішого постачальника хмарних сервісів, рекомендуємо змінити постачальника.»; $RE_{131} = RE_{132} = RE_{133} = RE_{134} = RE_{135} = RE_{136} =$ «Максимальна пропускна здатність хмарного провайдера – це максимальний об'єм даних, що можуть передати мережеві канали хмарного сервісу. Варто оцінювати потреби та вимоги компанії, щодо забезпечення величини пропускного каналу, щоб забезпечити доступність всіх сервісів компанії. У випадку, якщо пропускна

здатність вибраного постачальника хмарного сервісу задовольняє потреби бізнесу +20%, то можна сміло використовувати даного хмарного провайдера. В іншому випадку, рекомендуємо вам розглянути варіант вибору іншого постачальника хмарних сервісів, для можливості задовільнити вимоги та потреби бізнесу.»; RE_{141} = «Рекомендується увімкнення модуля протидії DoS/DDoS атак для забезпечення доступності розгорнутих сервісів компанії на ресурсах провайдера.»; RE_{142} = «Відсутність захисту від DoS/DDoS атак наражає Вашу компанію на спроможність зловмисників порушити працездатність ваших сервісів, що розгорнуті на ресурсах хмарного провайдера, що означає, що під час атаки можлива часткова чи повна втрата продуктивності хмарний потужностей. Рекомендується – на ресурсах вибраного хмарного провайдера не розгортати критичні сервіси, від яких залежить функціонування бізнес процесів компанії. У випадку розгортання критичних сервісів, від яких залежить функціонування бізнес-процесів компанії рекомендується робити регулярно резервні копії сервісу та використовувати рішення для захисту від DoS/DDoS атак від іншого виробника для уникнення впливу даного типу атак на функціонування сервісів розгорнутих на ресурсах хмарного провайдера.»; RE_{151} = «Для доцільності управління DNS записами, рекомендується скористатися можливістю управління DNS записами на рівні хмарного провайдера, як Primary зоною, за для можливості реалізації всіх бізнес-потреб, що вимагаються від сервісу управління DNS записами. Або скористатися можливістю використання даного сервісу, як Secondary зони, у випадку недоступності зміни Primary зони.»; RE_{152} = «Рекомендується використання сервісу для управління DNS зона від іншого постачальника.»; RE_{161} = «Рекомендується розгорнути копію критичних бізнес сервісів компанії та за допомогою вбудованого Load-Balancing модуля налаштувати балансування між декілька копіями ваших сервісів, для забезпечення роботи відмовостійкості розгорнутого сервісу. У випадку, якщо даний сервіс (LB) тарифікується окремо – варто розрахувати

вартість та додати його до закупівлі для забезпечення відмовостійкого функціонування критичних бізнес процесів компанії.»; RE_{162} = «У зв'язку з відсутністю вбудованого модуля Load-Balancing в хмарному сервісі – варто розглянути варіант використання стороннього сервісу для забезпечення балансування навантаження між декількома розгорнутими нодами критичних бізнес сервісів компанії, або розглянути варіант зміни хмарного сервісу. У випадку невикористання балансування навантаження між декількома нодами бізнес сервісів компанії, є імовірність перевантаження однієї ноди сервісів легітимними запитами та втрати функціонування бізнесу на певний час, що може призвести до втрати репутації та прибутку компанії через відсутність своєчасної відповіді клієнту.»; RE_{171} = «Рекомендується налаштувати один із доступних варіантів доступу до VPC/VPS розгорнутих на ресурсах хмарних сервісів, для забезпечення безпечного підключення до віртуальних машин, що розгорнуті в мережі Інтернет. Також важливо налаштувати обмеження по IP-адресах, з яких буде відбуватися адміністративне підключення до віртуальних машин. Дані дії необхідно виконати для унеможливлювано нелегітимного доступу до віртуальних машин, що забезпечують функціонування критичних бізнес сервісів компанії замовника.»; RE_{172} = «У випадку відсутності можливості встановлення безпечного підключення до віртуальних машин, розгорнутих на ресурсах хмарного провайдеру – рекомендується не розгортати ЖОДНИХ сервісів, що пов'язані з працездатністю бізнес-процесів компанії замовника, оскільки доступ до сервісу буде мати будь-хто, що спричинить витік конфіденційної/комерційної інформації компанії замовника, що призведе до втрати репутації та прибутку компанії.» [96]; RE_{181} = «Рекомендується увімкнути NBAD рішення для детального аналізу трафіку, що надходить до розгорнутих сервісів на ресурсах хмарного провайдера, з можливістю виявлення аномального трафіку, бот-мереж та попередження спроби компрометації бізнес сервісів компанії замовника. У випадку, якщо даний сервіс тарифікується окремо – рекомендується закласти в бюджет

придбання даного сервісу.»; RE_{182} = «Даний сервіс не є обов'язковим, проте, у випадку, якщо ви бажаєте виявляти аномальну поведінку в трафіку, що надходить на VPC/VPS сервери та мати змогу виявляти зловмисні запити, бот мережі – рекомендується скористатися послугами компаній, що надають рішення класу NBAD/NDR.»; RE_{191} = «Рекомендується увімкнути IPS/IDS рішення для виявлення та блокування аномальної поведінки в трафіку, що надходить до бізнес сервісів, щоб забезпечити безперебійне функціонування бізнес-процесів компанії замовника. У випадку, якщо даний сервіс тарифікується окремо – рекомендується закласти в бюджет придбання даного сервісу.»; RE_{192} = «У випадку, якщо в компанії є потреба виявляти аномальну поведінку в трафіку, що надходить на VPC/VPS сервери та мати змогу виявляти зловмисні запити – рекомендується скористатися послугами компаній, що надають рішення класу IPS/IDS.»; RE_{1101} = «Рекомендується увімкнути вбудований Firewall на ресурсах постачальника хмарного сервісу для бізнес процесів компанії та визначити, для яких мереж/IP адрес буде доступний сервіс та які порти будуть доступні для підключення. Даний модуль необхідний, щоб унеможливити зловмисникам можливість підключення до інших сервісів, що функціонують на VPC/VPS та не мають бути доступними з публічної мережі Інтернет.»; RE_{1102} = «У випадку, якщо бізнес потребує обмежувати доступ по IP/URL/портам до бізнес процесів, що функціонують на ресурсах хмарного провайдера – рекомендується скористатися послугами компаній, що надають можливості рішення класу Firewall/NGFW.»;

RE_{211} = «Рекомендується увімкнути реплікацію даних між декількома вузлами мережі, тобто між розгорнутими VPC/VPS на ресурсах хмарного сервісу з метою відновлення даних та/або балансування навантаження для забезпечення відмовостійкості розгорнутого рішення та швидкого відновлення роботи сервісу.»; RE_{212} = «У випадку відсутності реплікації, компанія наражає себе на небезпеку, що не вдасться швидко відновити

працездатність сервісу та забезпечити відмовостійке функціонування сервісу компанії. У випадку розгортання критично-важливих сервісів компанії, рекомендується налаштувати власними засобами реплікацію даних між декількома VPC/VPS.»; RE_{221} = «Рекомендується з затвердженою в компанії регулярністю проводити створення резервних копій працюючих VPC/VPS, що вказана у політиці інформаційної безпеки компанії з метою оперативного відновлення працездатності критичних бізнес-сервісів та процесів компанії.»; RE_{222} = «У випадку відсутності можливості створення резервних копій VPC/VPS, компанія має шанс втрати всі даних та налаштування, що розташовуються на серверах та не буде мати можливості швидко відновити працездатність сервісу з резервної копії. Рекомендується, або замінити постачальника хмарного сервісу, або скористатися власними сервісами для створення резервних копій VPC/VPS.»; RE_{231} = «Рекомендується використовувати функціонал створення копій VPC/VPS, щоб повторно не здійснювати налаштування VPC/VPS та сервісів, що на них працюють і мають ідентичний функціонал.»; RE_{232} = «У випадку відсутності можливості створення копій VPC/VPS, компанії потрібно буде щоразу створювати нову VPC/VDS та проводити налаштування ідентичної VPC/VDS»; RE_{241} = «Рекомендується увімкнути шифрування жорсткого диску, для забезпечення конфіденційності, цілісності та доступності даних компанії, що розташовуються на ресурсах постачальника хмарних сервісів.»; RE_{242} = «У випадку відсутності шифрування дискового простору, будь-який працівник хмарного сервісу, отримавши доступ до HDD/SDD/M2 – буде мати можливість прочитати дані та передати їх третім особам, що відповідно порушує доступність, цілісність та конфіденційність даних компанії.»; RE_{251} = «У разі відповідності стандарту FIPS 140-2 – VPC/VDS хмарного провайдера мають підтверджене використання сертифікованих криптографічних модулів та алгоритмів для шифрування даних.»; RE_{252} = «У разі відсутності

відповідності стандарту FIPS 140-2 – VPC/VDS хмарного провайдера НЕ мають підтвердженого використання сертифікованих криптографічних модулів та алгоритмів для шифрування даних.»; RE_{261} = «У разі відповідності стандарту PCI-DSS – компанія має можливість проводити фінансові операції використовуючи ресурси хмарного провайдера.»; RE_{262} = «У разі відсутності відповідності стандарту PCI-DSS – компанія НЕ має можливості проводити фінансові операції використовуючи ресурси хмарного провайдера.»; RE_{271} = «У разі відповідності стандарту GDPR – компанія має можливість використовувати VPC/VDS для надання послуг клієнтам з країн ЄС.»; RE_{272} = «У разі відсутності відповідності стандарту GDPR – компанія НЕ має можливості використовувати VPC/VDS для надання послуг клієнтам з країн ЄС.»; RE_{281} = «У разі відповідності стандарту HIPAA/HITECH – компанія має можливість використовувати VPC/VDS для розгортання сервісів пов'язаних із медичним страхуванням клієнтів та обробляти їх дані.»; RE_{282} = «У разі відсутності відповідності стандарту HIPAA/HITECH – компанія НЕ має можливості використовувати VPC/VDS для розгортання сервісів пов'язаних із медичним страхуванням клієнтів та обробляти їх дані.»; RE_{291} = «У разі відповідності стандарту FedRAMP – VPC/VDS хмарного провайдера мають постійний моніторинг і постачальник має змогу оперативно реагувати на перебої функціонування власних систем.»; RE_{292} = «У разі відсутності відповідності стандарту FedRAMP – VPC/VDS хмарного провайдера НЕ мають постійний моніторинг і постачальник НЕ має змогу оперативно реагувати на перебої функціонування власних систем.»; RE_{2101} = «У разі відповідності стандарту ISO 27000 – VPC/VDS хмарного провайдера мають підтверджений рівень захисту даних, що опрацьовуються.»; RE_{2102} = «У разі відсутності відповідності стандарту ISO 27000 – VPC/VDS хмарного провайдера НЕ мають підтвердженого рівня захисту даних, що опрацьовуються.»;

$RE_{311} = RE_{312} = RE_{313} = RE_{314}$ = «Оцінка критичності здійснюється відповідно до прописаних регламентів в межах компанії.»; RE_{321} = «Дані компанії знаходяться в безпеці на рівні моніторингу фізичної доступності до серверного обладнання.»; RE_{322} = «У випадку відсутності відео-нагляду серверів хмарного провайдеру, це може призвести до несанкціонованого доступу до серверного обладнання та порушення працездатності фізичного обладнання. Варто враховувати, що в даному випадку можливе викрадення обладнання, жорстких дисків та компрометація конфіденційної інформації компанії.»; RE_{331} = «Дані компанії знаходяться в безпеці на рівні фізичної доступності.»; RE_{332} = «Дані компанії знаходяться в безпеці на рівні фізичної доступності.»; RE_{333} = «Дані компанії знаходяться в безпеці на рівні фізичної доступності, проте за умови якщо фізичний ключ видається під запис і передається лише уповноваженим особам компанії хмарного провайдера.»; RE_{334} = «Наявність лише індивідуальних паперових перепусток для отримання доступу до серверного обладнання може призвести, що паперова перепустка може бути сфальсифікована і доступ до серверного обладнання отримають особи, що не повинні мати доступ та потенційно відбудеться компрометація даних чи фізичний вплив на працездатність серверного обладнання хмарного провайдера.»; RE_{335} = «Отримання доступу до серверного обладнання лише по знайомству може призвести, що доступ до серверного обладнання отримають особи, що не повинні мати доступ та потенційно відбудеться компрометація даних чи фізичний вплив на працездатність серверного обладнання хмарного провайдера.»; RE_{336} = «Відсутність контролю доступу до серверного обладнання призведе, що доступ до серверного обладнання може отримати будь-хто, хто не повинен мати доступ та потенційно відбудеться компрометація даних чи фізичний вплив на працездатність серверного обладнання хмарного провайдера.»; RE_{341} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити безперебійне надання

послуг компанії та забезпечити працездатність бізнес процесів компанії-замовника.»; RE_{342} = «У випадку відсутності безперебійної подачі живлення у випадках вимкнення світла – провайдер хмарних сервісів не буде мати змоги забезпечити безперебійне функціонування критичних бізнес-процесів та сервісів компанії-замовника, що може призвести до фінансової втрати зі сторони клієнтів-замовників.»; RE_{351} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити безперебійне надання послуг компанії та успішне охолодження серверного обладнання.»; RE_{352} = «У випадку відсутності якісної системи кондиціонування – серверне обладнання буде перегріватися, збоїти та переставати працювати, що може вплинути на якість віддачі контенту клієнтам, що потенційно може спровокувати відтік клієнтів-замовників.»; RE_{361} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити безперебійне надання послуг компанії та дієву протидію пожежі.»; RE_{362} = «У випадку відсутності протипожежної системи в ЦОДі постачальника хмарних сервісів – є імовірність виникнення короткого замикання чи навмисного підпалу, що призведе до знищення серверного обладнання та втрати даних на локації.»; RE_{371} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити безперебійне надання послуг компанії та виявлення/попередження несанкціонованого доступу до серверного обладнання.»; RE_{372} = «У випадку відсутності системи охорони – відсутня можливість контролю осіб, що входять в ЦОД хмарного постачальника, що може призвести до несанкціонованого доступу до серверного обладнання та навмисного псування обладнання, а також викрадення конфіденційної інформації, що циркулює на серверах, що використовуються компаніями-замовниками.»; RE_{381} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити безперебійне надання послуг компанії.»; RE_{382} = «У випадку відсутності оновлення обладнання кожних 4 роки – клієнти можуть стикнутися з проблемою зависання VPC/VDS,

некоректної роботи обладнання, погіршення продуктивності тощо, що буде впливати на якість контенту, що надається компаніями і потенційних відтік клієнтів-замовників.»; RE_{391} = «При наявності мережевого екрану нового покоління (NGFW), компанії та постачальник будуть мати змогу обмежити доступ до сервісів на мережевому рівні, блокувати доступ до портів, виявляти атаки, виявляти нелегітимні URL адреси тощо.»; RE_{392} = «При наявності стандартних засобів контрою доступу на мережевому рівні, компанії та постачальник будуть мати змогу обмежити доступ до сервісів на мережевому рівні та блокувати доступ до портів, але буде неможливо виявляти атаки та нелегітимні URL адреси.»; RE_{393} = «У випадку відсутності мережевих екранів, постачальник хмарних сервісів та компанія замовник не має змоги обмежити доступ до сервісів на мережевому рівні, блокувати доступ до портів, виявляти атаки, виявляти нелегітимні URL адреси. Відсутність мережевих екранів означає, що сервіси компаній замовників доступі для всього світу і будь-хто буде мати можливість отримати до них доступ, навіть шляхом перебору паролю.»; RE_{3101} = «У даному випадку, VPC/VDS сервери компанії замовника будуть захищені, оскільки буде присутня можливість, як виявлення атак на мережевому рівні, так і їх блокування. Блокування атак буде можливе, як для атак по сигнатурній базі даних, так і підозрілих запитів.»; RE_{3102} = «У даному випадку, компанія замовник буде мати можливість попереджувати лише відомі сигнатури, але не виявляти нові атаки, підозрілі запити, тощо.»; RE_{3103} = «У даному випадку, компанія замовник буде мати можливість лише виявляти сигнатури атак, зловмисні запити, проте не блокувати їх.»; RE_{3104} = «Сигнатурний аналіз буде відсутній для VPC/VDS серверів, тому рекомендується скористатися власними засобами виявлення атак на мережевому рівні задля виявлення та блокування атак на рівні сигнатур (наприклад, можна скористатися рішенням Snort або Suricata).»; RE_{3111} = «У даному випадку, ніхто не зможе отримати доступ до серверної частини

провайдера хмарних послуг та отримати фізичний доступ до жорстких дисків, на яких зберігаються дані компанії.»; RE_{3112} = «У даному випадку, існує імовірність компрометації даних компанії та фальсифікація пропуску для отримання та компрометації даних компанії, що розташовуються на ресурсах хмарних сервісів.»; RE_{3113} = «У даному випадку, будь-хто може отримати доступ до серверної частини постачальника хмарних послуг, щоб виконати будь-які протиправні дії, що вплинуть на функціонування серверного обладнання постачальника та порушити функціонування бізнес-процесів компанії замовника.»; RE_{3121} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити безперебійне надання послуг компанії.»; RE_{3122} = «В даному випадку постачальник хмарних сервісів має змогу забезпечити відновлення функціонування бізнес-процесів компанії з певною затримкою (затримка залежить від часу ручного відновлення налаштувань VPC/VDS фахівцями постачальника).»; RE_{3123} = «Постачальник не забезпечує відновлення функціонування бізнес-процесів компанії, що означає, що фахівцям компанії замовника необхідно буде самостійно займатися повторним налаштуванням власних бізнес-процесів, через порушення функціонування серверного обладнання постачальника. В даному випадку, бізнес-процеси компанії замовника будуть мати простій та не зможуть надавати послуги клієнтам, що призведе до втрати прибутку компанії. Якщо даний варіант не є припустимим, рекомендується скористатися послугами іншого постачальника хмарних послуг.»;

$RE_{411} = RE_{412} = RE_{413} = RE_{414} = RE_{415} = RE_{416}$ = «Вибір системи віртуалізації залежить від архітектури хмарного провайдера.»; RE_{417} = «У разі НЕвикористання систем віртуалізації компанія буде вимушена використовувати VDS сервери хмарного провайдера, що не надають змоги розгорнути ISO образи готових ОС, що містять повноцінно налаштовану систему або системи, що постачаються виключно у вигляді готового ISO

образу. У разі, якщо компанія має необхідність використання готових ISO образів, рекомендується розглянути хмарного провайдера, надає можливість використання систем віртуалізації.»; RE_{421} = «У даному випадку, компанія має можливість розмежувати права доступу між адміністраторами, аналітиками та аудиторами, що забезпечує принцип інформаційної безпеки, щодо мінімізації привілеїв доступу.»; RE_{422} = «У випадку відсутності рольової моделі доступу – всі користувачі, що отримують доступ до платформи будуть мати адміністративний рівень доступу, що суперечить принципах інформаційної безпеки, щодо мінімізації привілеїв доступу. Рекомендується надавати доступ до системи віртуалізації лише відповідальним адміністраторам.»; RE_{431} = «При наявності 2FA/MFA в системі віртуалізації – перевірте, чи налаштована вона та увімкнена для всіх користувачів. Якщо не увімкнена – сплануйте підключення 2FA/MA для всіх користувачів та адміністраторів, що мають доступ до системи віртуалізації для запобігання витоку облікових даних та несанкціонованого доступу до даних та VPS/VDS серверів компанії.»; RE_{432} = «У випадку відсутності підтримки 2FA/MFA в системі віртуалізації – присутня можливість компрометації логіну/паролю користувача чи адміністратора, чи передача облікових даних стороннім осіб, що потенційно можуть нашкодити діяльності компанії чи порушити бізнес процеси. За можливості, намагайтеся не розгортати на ресурсах даного хмарного сервісу критичні бізнес процеси, щоб запобігти впливу на діяльність бізнес процесів та компанії.»; RE_{441} = «Рекомендується в межах компанії визначити перелік осіб, яким необхідний доступ до консолі управління VPS/VDS з метою належного забезпечення та обслуговування працездатності розгорнутих VPS/VDS серверів.»; RE_{442} = «У випадку відсутності доступу до управління розгорнутими віртуальними машинами – компанія наражає себе на небезпеку, що у випадку непрацездатності сервіси – збитки від простою бізнес критичних сервісів будуть збільшуватися до тих пір, доки постачальник чи розробник хмарних сервісів – не виявить бажання відповідно до SLA допомогти з

підняттям встановлених VPS/VDS. Рекомендується на ресурсах даного хмарного сервісу не розгортати бізнес-критичні додатки чи сервіси, управління яким буде недоступне і буде забезпечуватися виключно через провайдера.»; RE_{451} = «Рекомендується застосувати всі необхідні зміни в безпекових налаштування, що компанія має затверджені для власної наземної інфраструктури або у відповідністю з розробленою політикою безпеки компанії.»; RE_{452} = «В даному випадку, замовник немає можливості вносити зміни в безпекові налаштування, що може поставити під сумнів безпечне функціонування розгорнутих VPS/VDS. Рекомендується в даному випадку, або співпрацювати з хмарним сервісом для внесення змін в безпекові налаштування, або розглянути варіант отримання прав для редагування безпекових налаштувань розгорнутих VPS/VDS серверів.»; RE_{461} = «Рекомендується скористатися даною можливістю.»; RE_{462} = «Відсутня можливість розгортання власних сервісів та рішень, що постачаються у вигляді ISO файлу. У випадку наявності в компанії даного типу рішень – рекомендується розглянути варіант використання іншого хмарного сервісу чи вступити в співпрацю з постачальником хмарного сервісу з метою підвантаження унікального образу для вашої компанії.»; RE_{471} = «Рекомендується налаштувати доступ до VPS/VDS серверів для всіх користувачів по SSL сертифікатам, для забезпечення безпечного підключення та відсутності можливості компрометації облікових даних користувачів/адміністраторів.»; RE_{472} = «У випадку відсутності можливості використання SSL сертифікатів для авторизації користувачів на VPS/VDS – існує імовірність компрометації облікових даних, що має доступ до серверів, що розгорнуті на ресурси хмарних сервісів. Рекомендується не розгортати на ресурсах даного хмарного сервісу критичних бізнес процесів компанії.»; RE_{481} = «Рекомендується налаштувати систему оповіщення адміністраторів систем при внесенні змін в мережеві налаштування VPS/VDS серверів з метою

забезпечення прозорої видимості щодо всіх змін, що вносять адміністраторами VPS/VDS серверів.»; RE_{482} = «У випадку відсутності системи сповіщення – адміністратор не буде мати змоги вчасно бути сповіщеним, що в функціонування VPS/VDS серверів було внесено зміни, що потенційно може спровокувати втрату працездатності бізнес сервісу, що може призвести до зупинки діяльності бізнесу, втрати репутації, прибутку тощо.»; RE_{491} = «Рекомендується налаштувати легування працездатності всіх VPS/VDS серверів, для повної видимості функціонування та статусу відпрацювання VPS/VDS серверів, що оброблять критичні бізнес процеси компанії.»; RE_{492} = «У випадку відсутності логування подій в реальному часі – адміністратор не буде мати змоги вчасно бути сповіщеним, щодо функціонування VPS/VDS серверів та зміни, які було внесено чи статус відпрацювання кожного сервісу. Рекомендується розпочати співпрацю з хмарним сервісом, щодо можливості отримання подій в реальному часі щодо функціонування VPS/VDS серверів.»; RE_{4101} = «Рекомендується час від часу проводити аудит подій, що стосуються діяльності адміністраторів хмарного сервісу та, за можливості, налаштувати вивантаження подій в SIEM систему для створення необхідних фільтрів та виявлення несанкціонованих дій щодо діяльності при налаштуваннях VPS/VDS серверів компанії.»; RE_{4102} = «У випадку відсутності фіксації дій адміністратора у вигляді audit logs – компанія не зможе фіксувати діяльність адміністраторів системи та перевірити, які дії відбувалися в системі перед тим, як бізнес-сервіс перестав функціонувати. Рекомендується, або використовувати спеціалізовані системи для доступу до хмарного сервісу, по типу PAM систем, або скористатися послугами іншого хмарного провайдера для розгортання критичних бізнес додатків та сервісів компанії.»;

RE_{511} = «Рекомендується використання даного хмарного провайдера.»; RE_{512} = «У випадку, якщо доступ будуть мати виключно представники хмарного сервісу, то компанія не буде мати змогу оперативно вносити зміни і

потрібно буде постійно робити запити на представників хмарного сервісу, що занадто сповільнює випуск оновлень чи нових версій програмного забезпечення. Рекомендується розглянути варіанти із самостійним управлінням операційною системою.»; RE_{513} = «У випадку, якщо доступ будуть мати виключно представники ЦОД , то компанія не буде мати змогу оперативно вносити зміни і потрібно буде постійно постійно робити запити на представників ЦОДу, що занадто сповільнює випуск оновлень чи нових версій програмного забезпечення. Рекомендується розглянути варіанти із самостійним управлінням операційною системою.»; RE_{514} = «Якщо доступ будуть мати всі, то це буде порушавати норми безпеки та конфіденційності даних, що містяться на даних VPS/VDS серверах, тому на ресурсах даного хмарного провайдера небезпечно розміщати дані, тому рекомендується звернутися до іншого хмарного провайдера або використовувати даного провайдера виключно для тестового середовища.»; RE_{515} = «НЕ рекомендується використання даного хмарного провайдера.»; RE_{521} = «Рекомендується налаштувати систему створення регулярних резервних копій ОС, що знаходяться в продуктивному середовищі та забезпечують виконання бізнес-процесів компанії.»; RE_{522} = «У випадку відсутності створення регулярних копій ОС чи snapshots – компанії потрібно буде з обережністю вносити зміни в продуктивне середовище, оскільки при найменшому збою – потрібно буде підіймати систему з нуля. Рекомендується в даному випадку, налагодити стороннє рішення, що буде створювати регулярну копії ОС.»; RE_{531} = «Рекомендується регулярно проводити оновлення ОС, з метою закриття відомих вразливостей та забезпечити безпечне функціонування ОС, що забезпечує працездатність сервісів компанії замовника.»; RE_{532} = «Відсутність можливості регулярного встановлення оновлень на ОС – провокує можливість появи експлуатацій, що можуть вплинути на працездатність бізнес-сервісів компанії та вплинути на безпеку діяльності

сервісу, оскільки при вірному підході – зловмисники зможуть викрасти конфіденційні дані компанії та скористатися ними, що спровокує втрату репутації та прибутку компанії.»; RE_{541} = «Рекомендується скористатися послугами хмарного провайдера, щодо антивірусного захисту VPS/VDS серверів, проте за можливості, використовуйте власне програмне забезпечення для антивірусного захисту та розслідування інцидентів.»; RE_{542} = «Рекомендується самостійно придбати антивірусне забезпечення та встановити його на VPS/VDS сервера, що були придбані у хмарного провайдера з метою захисту ОС та сервісів компанії від зловмисного програмного забезпечення, шифрувальників, безфайлових атак тощо.»; RE_{551} = «Рекомендується використання даного хмарного провайдера.»; RE_{552} = «У випадку неможливості встановлення власного програмного забезпечення – компанія не буде мати змогу розгортати власні сервіси на базі VPS/VDS серверів хмарного провайдера. Якщо розгортання власних бізнес сервісів є необхідним – варто тісно співпрацювати з постачальником хмарних сервісів або скористатися послугами іншого хмарного провайдера.»; RE_{561} = «Рекомендується обмежити доступ тільки до тих ресурсів, що виконуються на базі ОС, а для інших закрити мережевий доступ.»; RE_{562} = «У випадку неможливості управління міжмережевим екраном на базі ОС – адміністратори не будуть мати змогу управляти операційними системи, якщо останні будуть мати нестандартні порти. Рекомендується в даному випадку, тісно співпрацювати з постачальником хмарного сервісу з метою внесення змін у функціонування мережевого екрану на базі ОС.»; RE_{571} = «Рекомендується налаштувати технології CDN для вашого веб-додатку чи сервісу.»; RE_{572} = «В даному випадку, якщо технологія CDN буде відсутньою в хмарного провайдера – користувачам необхідно буде звертатися напряму до сервісів компанії, що знаходиться в єдиному місці, що спровокує час затримки щодо обробки запитів та відповіді користувачам. Рекомендується для таких

випадків використовувати CDN рішення іншого провайдера, для забезпечення швидкої взаємодії клієнта із сервісом компанії.»; RE_{581} = «Рекомендується налаштування відмовостійкості для всіх бізнес критичних сервісів та веб-додатків компанії-замовника.»; RE_{582} = «У випадку відсутності забезпечення відмовостійкості – компанія має потенційну небезпеку, якщо один із сервісів компанія перестане працювати, то частина бізнес-критичної інфраструктури перестане працювати. Рекомендується використовувати власні рішення та забезпечення відмовостійкості.»; RE_{591} = «Рекомендується використання даного хмарного провайдера.»; RE_{592} = «НЕ рекомендується використання даного хмарного провайдера.»; RE_{5101} = «Рекомендується налаштувати IAM рішення для відслідковування дій користувачів, для гранульованого надання доступу до сервісів тощо.»; RE_{5102} = «В даному випадку, хмарний провайдер не має змоги відсліковувати, які дії були несені користувачем, відсутні можливість гранульованого надання доступу до сервісів тощо. Рекомендується скористатися власним рішення (за наявності рішення IAM в межах компанії) для забезпечення повної видимості доступів та дій, що виконують адміністратори та користувачі операційної системи.»; RE_{5111} = «Рекомендується на основі отриманих звітів – вносити зміни в налаштування ОС для забезпечення безпечного функціонування ОС та бізнес-сервісів компанії.»; RE_{5112} = «У випадку відсутності регулярного сканування на вразливості хмарним провайдером – провайдер не буде володіти цілісною картиною вразливостей та проблем, що присутні в мережі хмарного провайдера. Рекомендується запросити у постачальника хмарних сервісів документ, згідно якого проводиться регулярне сканування на вразливості або скористатися послугами іншого хмарного провайдера або скористатися власним рішенням компанії для проведення сканування та виявлення вразливості на ресурсах VPS/VDS.»;

RE_{611} = «Рекомендується слідкувати за оновленнями системи контейнеризації та версії систем у використовуваних контейнерах для мінімізації потенційної компрометації даних компанії та втручання у виконання бізнес процесів компанії.»; RE_{612} = «У випадку, якщо компанія не має можливості управляти середовищем для розгортання контейнерів, то може існувати проблема, що система управління контейнерами буде мати незакриті вразливості, що можуть спровокувати компрометації даних в контейнерах і доступ до розгорнутих контейнерів буде не тільки в компанії, але і в постачальника хмарних послуг. Якщо вище перераховане не передбачене політикою безпеки компанії і є дозволено в межах компанії, тоді використання даного середовища є припустимим, проте в іншому випадку, рекомендується розглянути іншого постачальника хмарних сервісів.»; RE_{621} = «Рекомендується отримати від постачальника хмарних сервісів план щодо встановлення оновлень для системи управління контейнерами, з метою підтримки системи в актуальному стані.»; RE_{622} = «Рекомендується отримати від постачальника хмарних сервісів план щодо встановлення оновлень для системи управління контейнерами, з метою підтримки системи в актуальному стані. У випадку відсутності оновлень – необхідно запросити у постачальника проведення робіт щодо оновлення системи управління контейнерами або змінити постачальника хмарних сервісів.»; RE_{631} = «Рекомендується оперативно в найкорошті терміни після виявлення вразливостей – приймати міри, щодо усунення виявлених вразливостей, щоб мати захищену систему та стійку до кібератак.»; RE_{632} = «У випадку відсутності регламенту проведення сканування на вразливості систем управління контейнерами, постачальник хмарних сервісів не є обізнаним в наявних вразливостях, що присутні в системах провайдера. Рекомендується, або самостійно проводити сканування на вразливості системи управління контейнерами і безпосередньо контейнерів, або розглянути іншого постачальника хмарних сервісів, що буде мати системи виявлення

вразливостей і буде оперативного реагувати на їх закриття.»; RE_{641} = «Рекомендується скористатися готовими технологіями захисту систем управління контейнерами та за можливості використати і власні сервіси, щоб підвищити рівень захищеності використовуваних контейнерів та бізнес процесів компанії.»; RE_{642} = «У випадку, якщо постачальник не надає готовий набір захисту для розгорнутої системи управління контейнерами, рекомендується використати власні системи для захисту розгорнутих контейнерів з метою забезпечення безпечного функціонування сервісів компанії.»; RE_{651} = «Рекомендується слідкувати за правами доступу, що мають відповідальні співробітники, для унеможливлювано факту компрометації виконуваного контейнера.»; RE_{652} = «У випадку, якщо постачальник хмарних сервісів не розмежовує середовища між різними замовниками, то це означає, що всі користувачі даного хмарного провайдера будуть мати доступ до інших контейнерів інших замовників, що є протиріччю заходам в організації інформаційної безпеки. Рекомендується не використовувати засоби управління контейнерами на ресурсах даного хмарного провайдера та розгорнути власну систему управління контейнерами.»; RE_{661} = «Рекомендується налаштувати власні ролі та надати права доступу для адміністраторів системи таким чином, як це прописано відповідно до їх посадових обов'язків.»; RE_{662} = «У випадку, якщо постачальник хмарних сервісів не має можливості надавати налаштування власних користувачів та рівнів доступу, то постачальник повинен мати готовий набір користувачів із відповідними ролями доступу, що будуть мати змогу управляти лише розгорнутими контейнерами в середовищі компанії.»; RE_{671} = «Рекомендується підключитися до приватного репозиторію постачальника та мати власний репозиторій, щоб мати можливість забезпечувати безперервне функціонування бізнес-процесів компанії.»; RE_{672} = «Рекомендується мати власний репозиторій контейнерів для можливості оперативного розгортання

сформованого пакету бізнес сервісів та оперативного забезпечення діяльності бізнесу.»; RE_{681} = «Рекомендується налаштувати системи алертування при досягненні ліміту, щодо використовуваних ресурсів та піднятих контейнерів, з метою уникнути перевищення ліміту використання обчислювальних середовищ постачальника та попередити можливість виходу за бюджет компанії.»; RE_{682} = «У випадку відсутності статистики, компанія не буде мати уявлення та можливість оцінити власні витрати об'єктивно. Рекомендується наприкінці кожного місяця запитувати у постачальника хмарних сервісів статистику, щодо використаних ресурсів або вибрати тип оплати – передплата.»; RE_{691} = «Рекомендується скористатися готовим REST API та налаштувати автоматичне оновлення чи розгортання контейнерів для оперативного запуску бізнес процесів компанії з забезпеченням мінімальних затримок.»; RE_{692} = «У даному випадку, компанія не буде мати змогу автоматизовано вносити зміни та застосовувати нові налаштування/запускати нові контейнери без входу на консоль управління. Рекомендується сумісно з постачальником розробити API для автоматизованого управління розгорнутими контейнерами та їх розгортання.»; RE_{6101} = «Рекомендується реагувати на всі звіти від постачальника, щодо виявлення аномальної активності, для оперативного реагування на потенційні загрози та уникнення блокування діяльності бізнес процесів компанії.»; RE_{6102} = «У випадку відсутності даного функціоналу, компанія може не спостерігати аномальну активність власними засобами захисту і потенційно може підпасти під санкції чи штрафи, щодо проведення нелегальної активності, по прикладу входу в C&C мережу, що спровокує блокування компанії на певній частині пристроїв мережі Інтернет. Рекомендується мати власні сервіси, щодо виявлення та реагування на аномальні активності в середовищі використовуваних контейнерів.»;

RE_{711} = «Рекомендується з визначеною регулярністю переглядати події та зміни, що відбуваються в системі, для відслідковування та виявлення аномальної поведінки користувача. Також, рекомендується налаштувати інтеграцію з вашою SIEM системою, для можливості кореляції подій та виставлення сповіщень про виявлення аномальної поведінки на ресурсах хмарного сервісу.»; RE_{712} = «У випадку, якщо не буде здійснюватися логування подій в системі, адміністратор не буде бачити, що виконують користувачі та не зможе відслідкувати зміни, що було внесено в налаштування системи. Рекомендується, направляти події з ресурсів хмарного сервісу на вашу власну SIEM систему та проводити аналіз даних подій із використанням сповіщень про виявлення несанкціонованих дій.»; RE_{721} = «Рекомендується час від часу переглядати історію змін на VPS/VDS серверах, щоб мати змогу виявляти несанкціоновані зміни та користувача, який застосував дані зміни. Також, рекомендується налаштувати інтеграцію з вашою SIEM системою, щоб збирати події зі всіх VPS/VDS, що обслуговують бізнес процеси компанії.»; RE_{722} = «У випадку, якщо постачальник хмарних сервісів не має систему версійності по змінам на віртуальних машинах, це означає, що адміністратору, щоб перевірити історію змін необхідно буде авторизуватися на кожну VPS/VDS та дивитися події локально. Рекомендується в даному випадку, робити вивантаження подій, що відбуваються на VPS/VDS в вашу SIEM систему, щоб мати повну видимість дій, що виконуються на VPS/VDS серверах, що обслуговують бізнес процеси компанії.»; RE_{731} = «Рекомендується налаштувати синхронізацію часу між всіма компонентами мережі, як хмарної, так і наземної для можливості точного встановлення виникнення потенційної проблеми чи атаки, чи збою в бізнес-сервісах компанії.»; RE_{732} = «Відсутність синхронізації часу може призвести до того, що неможливо буде точно визначити час виникнення інциденту, оскільки в різних системах буде представлений різний час. Рекомендується на всіх VPS/VDS серверах використовувати NTP такий же, що використовується в

межах компанії.»; RE_{741} = «Рекомендується з певною періодичністю та використовуючи власну систему Управління вразливостями та/або використовуючи систему Управління вразливостями від постачальника хмарних послуг, відповідно до внутрішніх процедур компанії проводити аналіз та виявлення вразливостей на всіх розгорнутих VPS/VDS серверах, що використовує компанія на базі хмарного провайдеру, що забезпечують функціонування бізнес сервісів компанії.»; RE_{742} = «Рекомендується з певною періодичністю та використовуючи власну систему Управління вразливостями, відповідно до внутрішніх процедур компанії проводити аналіз та виявлення вразливостей на всіх розгорнутих VPS/VDS серверах, що використовує компанія на базі хмарного провайдеру, що забезпечують функціонування бізнес сервісів компанії.»; RE_{751} = «Рекомендується налаштувати або підключити функцію виявлення аномального трафіку в мережі, в якій виконуються VPS/VDS сервера, що обслуговують бізнес сервіси компанії, з метою уникнення можливості потрапляння зловмисного пакету даних чи шкідливого ПЗ на ресурси серверів.»; RE_{752} = «У випадку відсутності системи виявлення аномалій в мережевому трафіку, що надходить до VPS/VDS серверів, рекомендується використовувати власну систему IDS/IPS, для можливості виявлення та блокування зловмисного трафіку в мережі, в якій функціонує VPS/VDS серверах компанії.»; RE_{761} = «Рекомендується використання даного хмарного провайдера.»; RE_{762} = «НЕ рекомендується використання даного хмарного провайдера.»; RE_{771} = «Рекомендується увімкнути модуль шифрування каналу передачі даних між VPS/VDS серверами та ключ шифрування зберігати у надійному сховищі в межах компанії.»; RE_{772} = «Відсутність шифрування може завдати шкоди сервісам та бізнес-процес, від яких залежить функціонування бізнесу. Рекомендується власноруч налаштувати шифроване з'єднання між сервісами, що розгорнуті на VPS/VDS серверах з метою закриття каналу від сторонніх осіб.»; RE_{781} =

«Рекомендується використовувати, як сервіс провайдера, так і власний сервіс, щоб отримувати сповіщення про перебої в роботі VPS/VDS серверів, щоб уникати простою виконання бізнес сервісів та негативного впливу на діяльність бізнесу.»; RE_{782} = «У випадку відсутності сервісу, що перевіряє функціонування всіх VPS/VDS серверів замовника, постачальник не буде мати уявлення про стан власної мережі та працездатність певного регіону, що може завдати шкоди репутації, як замовника, так і постачальника, через непрацюючий сервіс. Рекомендується використовувати власні засоби для відслідковування працездатності бізнес-додатків, сервісів, що оперативно реагувати на всі ситуації, що впливають на працездатність VPS/VDS серверів, для уникнення втрати репутації та втрати прибутку компанії.»; RE_{791} = «Рекомендується час від часу проводити актуалізацію облікових записів на ресурсах хмарного провайдера для видалення неактуальних облікових даних чи оновлення доступу. Також варто налаштувати парольну політику до такої, що використовується в вашій компанії та затверджена політикою ІБ.»; RE_{792} = «У випадку відсутності єдиної системи управління обліковими даними та відсутності парольної політики може відбутися таке, що обліковий запис користувача скомпрометують і отримають несанкціонований доступ до сервісів, що мав доступ користувач. Аналогічно з парольною політикою – тому, рекомендується використовувати технології ZTNA та/або PAM для контрою доступу до бізнес-додатків, від яких залежить працездатність бізнесу та функціонування сервісів компанії.»; RE_{7101} = «Рекомендується використання даного хмарного провайдера.»; RE_{7102} = «НЕ рекомендується використання даного хмарного провайдера.»; RE_{7111} = «Рекомендується використовувати готові інтеграції для можливості побудови комплексних складних рішень.»; RE_{7112} = «Рекомендується, для необхідності проведення інтеграції використовувати REST API від хмарного постачальника, щоб мати можливість оперативно виконувати передачу подій між різними системи та

будувати комплексні рішення на базі ресурсів хмарних сервісів, в тому числі й по безпекових рішеннях.»; RE_{7121} = «Рекомендується налаштувати інтеграцію з системою логування, щоб регулярно отримувати відомості про стан кожної VPS/VDS та аналізувати всі зміни, що вносяться адміністраторами на панелі управління.»; RE_{7122} = «У випадку, коли хмарний сервіс немає можливості передавати події в систему логування, виникає така проблема, що зникає видимість про адміністраторів, що взаємодіють з адміністративною панеллю та станом VPS/VDS серверів. Рекомендується використовувати системи логування, що мають агенти, що можуть розгортатися на VPS/VDS серверах та збирати інформацію про стан кожного серверу, що дозволить якісно та точно визначати працездатність кожного сервісу, проте в даному випадку видимості по адміністративній панелі управління не буде.»; RE_{7131} = «Рекомендується увімкнути поведінковий аналіз користувачів з метою виявлення та блокування бот активності на ресурсах компанії чи орендованих ресурсах хмарного провайдера для зменшення імовірності впливу на працездатність бізнес сервісів компанії.»; RE_{7132} = «Рекомендується використовувати системи логування для виявлення часу внесення та застосування змін, щоб виявити аномальну поведінку користувача та ідентифікувати C&C чи бот активність на адміністративній панелі управління чи VPS/VDS серверах, які забезпечують функціонування бізнес сервісів компанії замовника.»;

RE_{811} = «В даному випадку, рекомендується використання даного хмарного сервісу, оскільки постачальник хмарного сервісу регулярно проводить оновлення підтримуваних сервісів та має останні оновлення систем, що закривають виявлені вразливості в застарілому програмному забезпеченні.»; RE_{812} = «У випадку, якщо постачальник хмарних сервісів не проводить регулярне оновлення підтримуваного програмного забезпечення, це означає, що постачальник використовує застаріле програмне забезпечення, що має безліч відомих враливостей, що потенційно небезпечно використовувати з

точки зору кібербезпеки. Тому, рекомендується запросити оновлення підтримуваного програмного забезпечення постачальником, або скористатися послугами іншого постачальника хмарних сервісів.»; RE_{821} = «В даному випадку, рекомендується використання даного хмарного сервісу, оскільки постачальник хмарного сервісу регулярно проводить оновлення сервісів власного виробництва, має останні оновлення систем, що закривають виявлені вразливості в застарілому програмному забезпеченні та постійно доповнює функціонал новими функціями.»; RE_{822} = «У випадку, якщо постачальник хмарних сервісів не проводить регулярне власного програмного забезпечення, це означає, що постачальник використовує застаріле програмне забезпечення, що має безліч відомих враливостей, що потенційно небезпечно використовувати з точки зору кібербезпеки та має недостатній функціонал, що не відповідає потреб ринку Тому, рекомендується запросити оновлення розроблюваного власними силами постачальника програмного забезпечення, або скористатися послугами іншого постачальника хмарних сервісів.»; RE_{831} = «При використанні власного персоналу для розробки програмного забезпечення, постачальник хмарних сервісів має повну видимість в програмному забезпеченні та можливість оперативно вносити зміни чи доповнювати функціонал, що підтримують розробники постачальника. В даному випадку, рекомендується розгортання бізнес сервісів компанії для забезпечення діяльності бізнесу та надання послуг клієнтам компанії.»; RE_{832} = «При використанні персоналу субпідрядної компанії для розробки програмного забезпечення, постачальник хмарних сервісів має часткову видимість в програмному продукту та оперативність внесення змін чи впровадження нового функціоналу буде суттєво нижчою, ніж при наявності власного відділу розробок. В даному випадку, рекомендується розгортання бізнес сервісів компанії для забезпечення діяльності бізнесу та надання послуг клієнтам компанії.»; RE_{833} = «При відсутності власних розробок (власними силами чи силами субпідрядних організації) – постачальник хмарних сервісів

наражає себе на небезпеку тим, що він використовує програмне забезпечення, функціонально невідоме для IT фахівців постачальника і немає можливості впливати на внесення функціональних змін в використовуваний програмний продукт. В даному випадку, використання постачальника хмарних сервісів рекомендується лише за умови, що постачальник регулярно проводить оновлення програмного забезпечення та виконує п.9.1»; RE_{841} = «Це означає, що VPS/VDS сервери мають тільки зазначений перелік програмного забезпечення на підтримуваних системах. Рекомендується використання даного постачальника хмарних сервісів та розгортання на їх основі бізнес процесів компанії для забезпечення діяльності бізнес.»; RE_{842} = «В даному випадку, існує імовірність, що постачальник хмарних сервісів встановить програмне забезпечення без відома замовника. Рекомендувати використання даного постачальника хмарних сервісів можливо, лише за умови попередньо узгодження з замовник встановлення програмного забезпечення, що не входить в перелік дозволеного ПЗ.»; RE_{851} = «При наявності логування всіх дій, що вносяться постачальником у функціонування хмарних сервісів, компанія замовник має можливість виявляти дана зміни та оцінювати, що було змінено та що, потенційно може вплину на функціонування бізнес сервісів. Рекомендується налаштувати вивантаження подій з хмарної системи у власну SIEM систему для можливості швидкого реагування на внесені зміни в функціонування хмарних сервісів, що обслуговують бізнес процеси та сервіси компанії замовника.»; RE_{852} = «У випадку відсутності логування, компанія замовник не буде бачити змін, що були внесені фахівцями постачальника хмарного сервісу, тобто, у випадку зупинки діяльності бізнес процесів і сервісів, компанія замовник не буде мати змоги виявити причину відмови роботи сервісу. Рекомендується провести перемови з постачальником хмарного сервісу та забезпечити налаштування вивантаження логів з хмарного сервісу, що стосуються саме орендованих VPS/VDS серверів замовником.»; RE_{861} = «Рекомендується проходити навчання від постачальника хмарних

сервісів задля підвищення рівня обізнаності в кіберзахищеності хмарних сервісів.»; RE_{862} = «У випадку відсутності навчання зі сторони постачальника хмарних сервісів – компанія замовник може не мати необхідно рівня знань, щодо зловмисного програмного забезпечення, що може потрапити на VPS/VDS сервера компанії. Рекомендується в межах компанії проводити регулярне навчання для протидії зловмисному програмному забезпеченню та підвищенню рівня обізнаності фахівців компанії замовника з точки зору кібербезпеки.»; RE_{871} = «При наявному переліку – компанія замовник буде мати можливість використовувати мінімально можливий набір відразу на старті ознайомлення з хмарним сервісом.»; RE_{872} = «При відсутності визначеного переліку необхідного програмного забезпечення – компанія замовник, не етапі ознайомлення роботи із сервісом має витратити час своїх фахівців для пошуку необхідного програмного забезпечення для взаємодії з системами постачальника хмарних сервісів.»; RE_{881} = «Рекомендується використання сервісів даного постачальника хмарних сервісів, оскільки компанія замовник буде мати можливість управляти власними придбаними сервісами, з використанням різноманітних типів пристроїв (ПК, мобільний пристрій тощо).»; RE_{882} = «У випадку відсутності підтримки крос-платформних додатків, компанія замовник для управління придбаними сервісами має використовувати лише чітко визначений тип пристрою чи програмного забезпечення для взаємодії з сервісами постачальника, що ускладнює процес налаштування власних сервісів та не надає можливості оперативного внесення змін в працездатність сервісів.»; RE_{891} = «В даному випадку, постачальник має уявлення про встановлене програмне забезпечення та швидке реагування на несанкціоноване програмне забезпечення з метою забезпечення безпечного функціонування бізнес сервісів замовника. Рекомендується використання ресурсів даного постачальника хмарних сервісів.»; RE_{892} = «У випадку відсутності інвентаризації встановлених

додатків, постачальник хмарних сервісів не буде мати змоги оперативно виявляти встановлення нелегітимного програмного забезпечення, що може призвести до компрометації даних компанії замовника. Рекомендується з певною частотою проводити аудит встановленого програмного забезпечення на використовуваних VPS/VDS хмарного провайдера для забезпечення конфіденційної обробки комерційних даних компанії.»; RE_{8101} = «Рекомендується увімкнути систему захисту веб-додатків від постачальника хмарних сервісів та отримати можливість переглядати встановлені налаштування з метою внесення змін саме під функціональні можливості підтримуваних веб-додатків та бізнес сервісів.»; RE_{8102} = «У випадку відсутності системи веб-захисту від постачальника хмарних сервісів – рекомендується придбати та встановити власну систему захисту, по типу WAF/WAAP/Anti-DDoS тощо, з метою уникнення потенційного впливу на працездатність веб-додатків чи бізнес сервісів компанії замовника зі сторони зловмисників.» [100];

RE_{911} = «Рекомендується увімкнути систему Data Classification з метою виявлення типів даних, що надходять на ресурси хмарних сервісів та співставлення з дозволеними типами даним, що передбачені для визначеного типу веб-додатку чи сервісу, та попередження несанкціонованої обробки іншого, недозволеного типу даних чи його витоку за межі компанії.»; RE_{912} = «В даному випадку, це не є критичною необхідністю, проте, рекомендується використання власного рішення Data Classification з метою виявлення типів даних, що надходять на ресурси хмарного сервісіу та співставлення з дозволеними типами даним, що передбачені для визначеного типу веб-додатку чи сервісу, та попередження несанкціонованої обробки іншого, недозволеного типу даних чи його витоку за межі компанії.»; RE_{921} = «Рекомендується увімкнути модуль, що дозволяє виявляти типи файлів, що передаються, щоб мати можливість виявляти та аналізувати файли, і виявляти у файлах конфіденційну інформацію, з метою попередження витоку даних за межі

компанії, так і компрометацію даних, що зберігаються локально на сервері хмарного провайдера.»; RE_{922} = «В даному випадку, це не є критичною необхідністю, проте, рекомендується використання власного рішення, що дозволяє виявляти типи файлів, що передаються, щоб мати можливість виявляти та аналізувати файли, і виявляти у файлах конфіденційну інформацію, з метою попередження витоку даних за межі компанії, так і компрометацію даних, що зберігаються локально на сервері хмарного провайдера.»; RE_{931} = «Рекомендується використання даного хмарного провайдера.»; RE_{932} = «У випадку, якщо постачальник хмарних сервісів не проводить перевірку написаного коду рішенням класу SAST, це означає, що програмний код, потенційно може бути вразливим та містити велику кількість загроз, що негативно вплинуть на працездатність сервісів замовника. Рекомендується використовувати власні програмні засоби для закриття знайдених вразливостей на ресурсах, що використовуються компанією замовником.»; RE_{941} = «За наявності інформації про всі зміни, що було внесено в функціонування хмарного сервісу – замовник може оцінити, як це негативно може вплинути на функціонування розгорнутого сервісу, щоб застосувати перелік дії з метою НЕпорушення працездатності використовуваного сервісу.»; RE_{942} = «У випадку відсутності інформації про внесені зміни – компанія замовник не буде мати інформацію про зміни, які були внесені в систему, що потенційно може вплинути на функціонування бізнес сервісу компанії. Рекомендується завчасно домовитися з постачальником хмарних сервісів, що всі зміни будуть задокументовані на направлені на замовника.»; RE_{951} = «Рекомендується використання даного хмарного провайдера.»; RE_{952} = «У випадку відсутності можливості розмежування прав доступу в межах власного додатку – компанія замовник буде вимушена надавати доступ для субпідрядної компанії чи власним співробітникам права доступу з адміністративними можливостями, що негативно може вплинути на

функціонування бізнес сервісів. Рекомендується, або не надавати доступ стороннім особам, або проводити з ними регулярні зустрічі, або впровадити PAM систему або розглянути варіант використання іншого постачальника хмарних сервісів.»; RE_{961} = «Рекомендується використання даного хмарного провайдера.»; RE_{962} = «У випадку відсутності сповіщення про початок проведення регламентних робіт – компанія замовник може тимчасово втратити доступ до розгорнутих в хмарні бізнес сервісів, та лише здогадуватися, коли та в який час сервіс відновить свою роботу. Рекомендується домовитися з постачальником хмарних сервісів про сповіщення компанії замовника, щодо проведення робіт, задля уникнення можливості впливу регламентних робіт на функціонування бізнес сервісів замовника.»; RE_{971} = «Рекомендується використання даного хмарного провайдера.»; RE_{972} = «У випадку відсутності сповіщення про виявлення збоїв – компанія замовник може тимчасово втратити доступ до розгорнутих в хмарні бізнес сервісів, та лише здогадуватися, що за збій стався на ресурсах хмарного провайдера. Рекомендується домовитися з постачальником хмарних сервісів про сповіщення компанії замовника, щодо виявлення збоїв в роботі сервісу, задля розуміння, що деякий час бізнес сервісів замовника може бути недоступний, проте до цього моменту, за можливості, рекомендується зробити повну копію системи.»; RE_{981} = «Рекомендується використання даного хмарного провайдера.»; RE_{982} = «В даному випадку, рекомендується сумісно з постачальником запланувати сесію-дзвінок, щоб домовитися про необхідні зміни, що необхідно застосовувати до ресурсів хмарних сервісів, задля мінімізації впливу оновлень на працездатну систему замовника.»; RE_{991} = «Рекомендується увімкнути модуль, що підключає DLP рішення задля автоматизованого виявлення витоку конфіденційних даних за межі компанії та потенційного отримання збитку компанією замовником.»; RE_{992} = «У випадку відсутності даного рішення, рекомендується використати власне DLP

рішення задля автоматизованого виявлення витоку конфіденційних даних за межі компанії та потенційного отримання збитку компанією замовником.»; RE_{9101} = «Рекомендується використання даного хмарного провайдера.»; RE_{9102} = «У випадку відсутності порталу підтримки та відсутності можливості відкриття заявок в підтримку, рекомендується домовитися з постачальником хмарних сервісів, щодо виділення контактів окремого фахівця, що буде реагувати на всі запити, що стосуються роботи хмарного сервісу.»; RE_{9111} = «Рекомендується використання даного хмарного провайдера.»; RE_{9112} = «У випадку відсутності прописаного SLA документу, постачальник може собі дозволити не реагувати на запити від замовника, тому рекомендується на етапі підписання контракту – підписати індивідуальний SLA документ, що буде регламентувати постачальника хмарного сервісу реагувати на запити від замовника у визначений час.»; RE_{9121} = «Рекомендується використання даного хмарного провайдера.»; RE_{9122} = «У випадку, якщо постачальник хмарних сервісів не проводить тестування власних сервісів на проникнення, то існує імовірність, що ресурси хмарних сервісів мають незакриті вразливості та можуть стати причиною витоку даних компанії. Рекомендується, або самостійно проводити тестування на проникнення використовуваних сервісів, або скористатися послугами іншого хмарного провайдера.».

Підмножину $\mathbf{RE}_{\mathbf{jkl}}$ визначимо як:

$$\mathbf{RE}_{\mathbf{jkl}} = \left\{ \bigcup_{p=1}^{m_{11jkl}} \mathbf{RE}_{\mathbf{jklp}} \right\} = \left\{ \mathbf{RE}_{\mathbf{jkl1}}, \mathbf{RE}_{\mathbf{jkl2}}, \ldots, \mathbf{RE}_{\mathbf{jklm_{11jkl}}} \right\} \quad (2.77)$$

де: $\mathbf{RE}_{\mathbf{jklp}} \subseteq \mathbf{RE}_{\mathbf{jkl}}$ $(p = \overline{1, m_{11jkl}})$ – p-а підмножина груп другого рівня запитань, що визначаються встановленими відповідями та відповідають оцінюваними параметрами l-ї підмножини, що забезпечують оцінку захищеності сервісів хмарного провайдера першого порядку, m_{11jkl} – кількість груп l-ї підмножини.

Відповідно вираз (2.75) із урахуванням виразу (2.77) можна представити наступним чином:

$$\mathbf{RE} = \left\{\bigcup_{j=1}^{m_{11}} \mathbf{RE}_{\mathbf{j}}\right\} = \left\{\bigcup_{j=1}^{m_{11}}\left\{\bigcup_{k=1}^{m_{11j}} \mathbf{RE}_{\mathbf{jk}}\right\}\right\} = \left\{\bigcup_{j=1}^{m_{11}}\left\{\bigcup_{k=1}^{m_{11j}}\left\{\bigcup_{l=1}^{m_{11jk}} RE_{\ jkl}\right\}\right\}\right\} =$$

$$\left\{\bigcup_{j=1}^{m_{11}}\left\{\bigcup_{k=1}^{m_{11j}}\left\{\bigcup_{l=1}^{m_{11jk}}\left\{\bigcup_{p=1}^{m_{11jkl}} \mathbf{RE}_{\mathbf{jklp}}\right\}\right\}\right\}\right\} =$$

$$\{\{\{\{\mathbf{RE}_{1111}, \mathbf{RE}_{1112}, \ldots, \mathbf{RE}_{111\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{1121}, \mathbf{RE}_{1122}, \ldots, \mathbf{RE}_{112\mathbf{m}_{11jkl}}\}, \ldots,$$

$$\{\mathbf{RE}_{11\mathbf{m}_{11jk}1}, \mathbf{RE}_{11\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{11\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\},$$

$$\{\{\mathbf{RE}_{1211}, \mathbf{RE}_{1212}, \ldots, \mathbf{RE}_{121\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{1221}, \mathbf{RE}_{1222}, \ldots, \mathbf{RE}_{122\mathbf{m}_{11jkl}}\}, \ldots,$$

$$\{\mathbf{RE}_{12\mathbf{m}_{11jk}1}, \mathbf{RE}_{12\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{12\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\}, \ldots,$$

$$\{\{\mathbf{RE}_{1\mathbf{m}_{11j}11}, \mathbf{RE}_{1\mathbf{m}_{11j}12}, \ldots, \mathbf{RE}_{1\mathbf{m}_{11j}1\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{1\mathbf{m}_{11j}21}, \mathbf{RE}_{1\mathbf{m}_{11j}22}, \ldots, \mathbf{RE}_{1\mathbf{m}_{11j}2\mathbf{m}_{11jkl}}\}, \ldots,$$

$$\{\mathbf{RE}_{1\mathbf{m}_{11j}\mathbf{m}_{11jk}1}, \mathbf{RE}_{1\mathbf{m}_{11j}\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{1\mathbf{m}_{11j}\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\}\},$$

$$\{\{\{\mathbf{RE}_{2111}, \mathbf{RE}_{2112}, \ldots, \mathbf{RE}_{211\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{2121}, \mathbf{RE}_{2122}, \ldots, \mathbf{RE}_{212\mathbf{m}_{11jkl}}\}, \ldots, \qquad (2.78)$$

$$\{\mathbf{RE}_{21\mathbf{m}_{11jk}1}, \mathbf{RE}_{21\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{21\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\},$$

$$\{\{\mathbf{RE}_{2211}, \mathbf{RE}_{2212}, \ldots, \mathbf{RE}_{221\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{2221}, \mathbf{RE}_{2222}, \ldots, \mathbf{RE}_{222\mathbf{m}_{11jkl}}\}, \ldots,$$

$$\{\mathbf{RE}_{22\mathbf{m}_{11jk}1}, \mathbf{RE}_{22\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{22\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\}, \ldots, \{\{\mathbf{RE}_{2\mathbf{m}_{11j}11}, \mathbf{RE}_{2\mathbf{m}_{11j}12}, \ldots,$$

$$\mathbf{RE}_{2\mathbf{m}_{11j}1\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{2\mathbf{m}_{11j}21}, \mathbf{RE}_{2\mathbf{m}_{11j}22}, \ldots, \mathbf{RE}_{2\mathbf{m}_{11j}2\mathbf{m}_{11jkl}}\}, \ldots,$$

$$\{\mathbf{RE}_{2\mathbf{m}_{11j}\mathbf{m}_{11jk}1}, \mathbf{RE}_{2\mathbf{m}_{11j}\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{2\mathbf{m}_{11j}\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\}\}, \ldots,$$

$$\{\{\{\mathbf{RE}_{\mathbf{m}_{11}111}, \mathbf{RE}_{\mathbf{m}_{11}112}, \ldots, \mathbf{RE}_{\mathbf{m}_{11}11\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{\mathbf{m}_{11}121}, \mathbf{RE}_{\mathbf{m}_{11}122}, \ldots,$$

$$\mathbf{RE}_{\mathbf{m}_{11}12\mathbf{m}_{11jkl}}\}, \ldots, \{\mathbf{RE}_{\mathbf{m}_{11}1\mathbf{m}_{11jk}1}, \mathbf{RE}_{\mathbf{m}_{11}1\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{\mathbf{m}_{11}1\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\},$$

$$\{\{\mathbf{RE}_{\mathbf{m}_{11}211}, \mathbf{RE}_{\mathbf{m}_{11}212}, \ldots, \mathbf{RE}_{\mathbf{m}_{11}21\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{\mathbf{m}_{11}221}, \mathbf{RE}_{\mathbf{m}_{11}222}, \ldots,$$

$$\mathbf{RE}_{\mathbf{m}_{11}22\mathbf{m}_{11jkl}}\}, \ldots, \{\mathbf{RE}_{\mathbf{m}_{11}2\mathbf{m}_{11jk}1}, \mathbf{RE}_{\mathbf{m}_{11}2\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{\mathbf{m}_{11}2\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\}, \ldots,$$

$$\{\{\mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}11}, \mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}12}, \ldots, \mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}1\mathbf{m}_{11jkl}}\}, \{\mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}21}, \mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}22}, \ldots,$$

$$\mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}2\mathbf{m}_{11jkl}}\}, \ldots, \{\mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}\mathbf{m}_{11jk}1}, \mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}\mathbf{m}_{11jk}2}, \ldots, \mathbf{RE}_{\mathbf{m}_{11}\mathbf{m}_{11j}\mathbf{m}_{11jk}\mathbf{m}_{11jkl}}\}\}\}\},$$

Наприклад, для $m_{11} = 9\ (j = \overline{1,9})$, $m_{11141} = 11\ (p = \overline{1,11})$, $m_{11151} = 1\ (p = \overline{1,1})$, $m_{11211} = 4\ (p = \overline{1,4})$, $m_{11241} = 5\ (p = \overline{1,5})$, $m_{11411} = m_{11412} = m_{11413} = m_{11414} = m_{11415} = m_{11416} = 3\ (p = \overline{1,3})$, $m_{11521} = 1\ (p = \overline{1,1})$, формула (2.78) набуде наступного вигляду:

$$\mathbf{RE} = \left\{ \bigcup_{j=1}^{9} \mathbf{RE}_{\mathbf{j}} \right\} = \left\{ \bigcup_{j=1}^{9} \left\{ \bigcup_{k=1}^{m_{11j}} \mathbf{RE}_{\mathbf{jk}} \right\} \right\} = \left\{ \bigcup_{j=1}^{9} \left\{ \bigcup_{k=1}^{m_{11j}} \left\{ \bigcup_{l=1}^{m_{11jk}} RE_{jkl} \right\} \right\} \right\} =$$

$$\left\{ \bigcup_{j=1}^{9} \left\{ \bigcup_{k=1}^{m_{11j}} \left\{ \bigcup_{l=1}^{m_{11jk}} \left\{ \bigcup_{p=1}^{m_{11jkl}} \mathbf{RE}_{\mathbf{jklp}} \right\} \right\} \right\} \right\} =$$

$$\{\{\{RE_{111}, RE_{112}, RE_{113}, RE_{114}, RE_{115}, RE_{116}\}, \{RE_{121}, RE_{122}, RE_{123}, RE_{124},$$
$$RE_{125}, RE_{126}\}, \{RE_{131}, RE_{132}, RE_{133}, RE_{134}, RE_{135}, RE_{136}\},$$
$$\{\{\mathbf{RE}_{\mathbf{1411}}, \mathbf{RE}_{\mathbf{1412}}, \mathbf{RE}_{\mathbf{1413}}, \mathbf{RE}_{\mathbf{1414}}, \mathbf{RE}_{\mathbf{1415}}, \mathbf{RE}_{\mathbf{1416}}, \mathbf{RE}_{\mathbf{1417}}, \mathbf{RE}_{\mathbf{1418}}, \mathbf{RE}_{\mathbf{1419}},$$
$$\mathbf{RE}_{\mathbf{14110}}, \mathbf{RE}_{\mathbf{14111}}\}, RE_{142}\}, \{\{\mathbf{RE}_{\mathbf{1511}}\}, RE_{152}\}, \{RE_{161}, RE_{162}\},$$
$$\{RE_{171}, RE_{172}\}, \{RE_{181}, RE_{182}\}, \{RE_{191}, RE_{192}\}, \{RE_{1101}, RE_{1102}\}\},$$
$$\{\{\{\mathbf{RE}_{\mathbf{2111}}, \mathbf{RE}_{\mathbf{2112}}, \mathbf{RE}_{\mathbf{2113}}, \mathbf{RE}_{\mathbf{2114}}\}, RE_{212}\}, \{RE_{221}, RE_{222}\}, \{RE_{231}, RE_{232}\},$$
$$\{\mathbf{RE}_{\mathbf{2411}}, \mathbf{RE}_{\mathbf{2412}}, \mathbf{RE}_{\mathbf{2413}}, \mathbf{RE}_{\mathbf{2414}}, \mathbf{RE}_{\mathbf{2415}}\}, RE_{242}\}, \{RE_{251}, RE_{252}\},$$
$$\{RE_{261}, RE_{262}\}, \{RE_{271}, RE_{272}\}, \{RE_{281}, RE_{282}\}, \{RE_{291}, RE_{292}\}, \{RE_{2101}, RE_{2102}\}\},$$
$$\{\{RE_{311}, RE_{312}, RE_{313}, RE_{314}\}, \{RE_{321}, RE_{322}\}, \{RE_{331}, RE_{332}, RE_{333}, RE_{334}, RE_{335},$$
$$RE_{336}\}, \{RE_{341}, RE_{342}\}, \{RE_{351}, RE_{352}\}, \{RE_{361}, RE_{362}\}, \{RE_{371}, RE_{372}\},$$
$$\{RE_{381}, RE_{382}\}, \{RE_{391}, RE_{392}, RE_{393}\}, \{RE_{3101}, RE_{3102}, RE_{3103}, RE_{3104}\},$$
$$\{RE_{3111}, RE_{3112}, RE_{3113}\}, \{RE_{3121}, RE_{3122}, RE_{3123}\}\},$$
$$\{\{\{\mathbf{RE}_{\mathbf{4111}}, \mathbf{RE}_{\mathbf{4112}}, \mathbf{RE}_{\mathbf{4113}}\}, \{\mathbf{RE}_{\mathbf{4121}}, \mathbf{RE}_{\mathbf{4122}}, \mathbf{RE}_{\mathbf{4123}}\}, \{\mathbf{RE}_{\mathbf{4131}}, \mathbf{RE}_{\mathbf{4132}}, \mathbf{RE}_{\mathbf{4133}}\},$$
$$\{\mathbf{RE}_{\mathbf{4141}}, \mathbf{RE}_{\mathbf{4142}}, \mathbf{RE}_{\mathbf{4143}}\}, \{\mathbf{RE}_{\mathbf{4151}}, \mathbf{RE}_{\mathbf{4152}}, \mathbf{RE}_{\mathbf{4153}}\}, \{\mathbf{RE}_{\mathbf{4161}}, \mathbf{RE}_{\mathbf{4162}}, \mathbf{RE}_{\mathbf{4163}}\},$$
$$RE_{417}\}, \{RE_{421}, RE_{422}\}, \{RE_{431}, RE_{432}\}, \{RE_{441}, RE_{442}\}, \{RE_{451}, RE_{452}\},$$
$$\{RE_{461}, RE_{462}\}, \{RE_{471}, RE_{472}\}, \{RE_{481}, RE_{482}\}, \{RE_{491}, RE_{492}\}, \{RE_{4101}, RE_{4102}\}\},$$
$$\{\{RE_{511}, RE_{512}, RE_{513}, RE_{514}, RE_{515}\}, \{\{\mathbf{RE}_{\mathbf{5211}}\}, RE_{522}\},$$
$$\{RE_{531}, RE_{532}\}, \{RE_{541}, RE_{542}\}, \{RE_{551}, RE_{552}\}, \{RE_{561}, RE_{562}\}, \{RE_{571}, RE_{572}\},$$
$$\{RE_{581}, RE_{582}\}, \{RE_{591}, RE_{592}\}, \{RE_{5101}, RE_{5102}\}, \{RE_{5111}, RE_{5112}\}\},$$
$$\{\{RE_{611}, RE_{612}\}, \{RE_{621}, RE_{622}\}, \{RE_{631}, RE_{632}\}, \{RE_{641}, RE_{642}\},$$
$$\{RE_{651}, RE_{652}\}, \{RE_{661}, RE_{662}\}, \{RE_{671}, RE_{672}\}, \{RE_{681}, RE_{682}\}, \{RE_{691}, RE_{692}\},$$
$$\{RE_{6101}, RE_{6102}\}\}, \quad (2.79)$$

$$\{\{RE_{711},RE_{712}\},\{RE_{721},RE_{722}\},\{RE_{731},RE_{732}\},\{RE_{741},RE_{742}\},\{RE_{751},RE_{752}\},$$
$$\{RE_{761},RE_{762}\},\{RE_{771},RE_{772}\},\{RE_{781},RE_{782}\},\{RE_{791},RE_{792}\},\{RE_{7101},RE_{7102}\},$$
$$\{RE_{7111},RE_{7112}\},\{RE_{7121},RE_{7122}\},\{RE_{7131},RE_{7132}\}\},$$
$$\{\{RE_{811},RE_{812}\},\{RE_{821},RE_{822}\},\{RE_{831},RE_{832},RE_{833}\},\{RE_{841},RE_{842}\},$$
$$\{RE_{851},RE_{852}\},\{RE_{861},RE_{862}\},\{RE_{871},RE_{872}\},\{RE_{881},RE_{882}\},\{RE_{891},RE_{892}\}, \quad (2.79)$$
$$\{RE_{8101},RE_{8102}\}\},$$
$$\{\{RE_{911},RE_{912}\},\{RE_{921},RE_{922}\},\{RE_{931},RE_{932}\},\{RE_{941},RE_{942}\},\{RE_{951},RE_{952}\},$$
$$\{RE_{961},RE_{962}\},\{RE_{971},RE_{972}\},\{RE_{981},RE_{982}\},\{RE_{991},RE_{992}\},$$
$$\{RE_{9101},RE_{9102}\},\{RE_{9111},RE_{9112}\},\{RE_{9121},RE_{9122}\}\}\},$$

де: $\mathbf{RE}_{1411}$ = «Питання 1»; $\mathbf{RE}_{1412}$ = «Питання 2»; $\mathbf{RE}_{1413}$ = «Питання 3»; $\mathbf{RE}_{1414}$ = «Питання 4»; $\mathbf{RE}_{1415}$ = «Питання 5»; $\mathbf{RE}_{1416}$ = «Питання 6»; $\mathbf{RE}_{1417}$ = «Питання 7»; $\mathbf{RE}_{1418}$ = «Питання 8»; $\mathbf{RE}_{1419}$ = «Питання 9»; $\mathbf{RE}_{14110}$ = «Питання 10»; $\mathbf{RE}_{14111}$ = «Питання 11»; $\mathbf{RE}_{1511}$ = «Питання 1»; $\mathbf{RE}_{2111}$ = «Питання 1»; $\mathbf{RE}_{2112}$ = «Питання 2»; $\mathbf{RE}_{2113}$ = «Питання 3»; $\mathbf{RE}_{2114}$ = «Питання 4»; $\mathbf{RE}_{2411}$ = «Питання 1»; $\mathbf{RE}_{2412}$ = «Питання 2»; $\mathbf{RE}_{2413}$ = «Питання 3»; $\mathbf{RE}_{2414}$ = «Питання 4»; $\mathbf{RE}_{2415}$ = «Питання 5»; $\mathbf{RE}_{4111} = \mathbf{RE}_{4121} = \mathbf{RE}_{4131} = \mathbf{RE}_{4141} = \mathbf{RE}_{4151} = \mathbf{RE}_{4161}$ = «Питання 1»; $\mathbf{RE}_{4112} = \mathbf{RE}_{4122} = \mathbf{RE}_{4132} = \mathbf{RE}_{4142} = \mathbf{RE}_{4152} = \mathbf{RE}_{4162}$ = «Питання 2»; $\mathbf{RE}_{4113} = \mathbf{RE}_{4123} = \mathbf{RE}_{4133} = \mathbf{RE}_{4143} = \mathbf{RE}_{4153} = \mathbf{RE}_{4163}$ = «Питання 3»; $\mathbf{RE}_{5211}$ = «Питання 1».

Підмножину $\mathbf{RE}_{\mathbf{jklp}}$ визначимо як:

$$\mathbf{RE}_{\mathbf{jklp}} = \left\{ \bigcup_{s=1}^{m_{11jklp}} RE_{jklps} \right\} = \left\{ RE_{jklp1}, RE_{jklp2}, \ldots, RE_{jklpm_{11jklp}} \right\} \quad (2.80)$$

де: $RE_{jklps} \subseteq \mathbf{RE}_{\mathbf{jklp}}$ $(s = \overline{1, m_{11jklp}})$ – s-а підмножина груп рекомендацій другого рівня, що надають рекомендації щодо покращення роботи сервісів на ресурсах хмарного сервісу та відповідають оцінюваними параметрами p-ї підмножини, що забезпечують оцінку захищеності сервісів хмарного провайдера першого порядку, m_{11jklp} – кількість груп p-ї підмножини.

Наприклад, для $m_{11}=9\ (j=\overline{1,9})$, $m_{111411}=2\ (p=\overline{1,2})$, $m_{111412}=8\ (p=\overline{1,8})$, $m_{111413}=2\ (p=\overline{1,2})$, $m_{111414}=2\ (p=\overline{1,2})$, $m_{111415}=2\ (p=\overline{1,2})$, $m_{111416}=2\ (p=\overline{1,2})$, $m_{111417}=2\ (p=\overline{1,2})$, $m_{111418}=2\ (p=\overline{1,2})$, $m_{111419}=2\ (p=\overline{1,2})$, $m_{1114110}=2\ (p=\overline{1,2})$, $m_{1114111}=2\ (p=\overline{1,2})$, $m_{111511}=2\ (p=\overline{1,2})$, $m_{112111}=2\ (p=\overline{1,2})$, $m_{112112}=2\ (p=\overline{1,2})$, $m_{112113}=2\ (p=\overline{1,2})$, $m_{112114}=4\ (p=\overline{1,4})$, $m_{112411}=2\ (p=\overline{1,2})$, $m_{112412}=3\ (p=\overline{1,3})$, $m_{112413}=2\ (p=\overline{1,2})$, $m_{112414}=3\ (p=\overline{1,3})$, $m_{112415}=2\ (p=\overline{1,2})$,

$m_{114111}=6\ (p=\overline{1,6})$, $m_{114112}=8\ (p=\overline{1,8})$, $m_{114113}=2\ (p=\overline{1,2})$, $m_{114121}=6\ (p=\overline{1,6})$, $m_{114122}=8\ (p=\overline{1,8})$, $m_{114123}=2\ (p=\overline{1,2})$, $m_{114131}=6\ (p=\overline{1,6})$, $m_{114132}=8\ (p=\overline{1,8})$, $m_{114133}=2\ (p=\overline{1,2})$, $m_{114141}=6\ (p=\overline{1,6})$, $m_{114142}=8\ (p=\overline{1,8})$, $m_{114143}=2\ (p=\overline{1,2})$, $m_{114151}=6\ (p=\overline{1,6})$, $m_{114152}=8\ (p=\overline{1,8})$, $m_{114153}=2\ (p=\overline{1,2})$, $m_{114161}=6\ (p=\overline{1,6})$, $m_{114162}=8\ (p=\overline{1,8})$, $m_{114163}=2\ (p=\overline{1,2})$, $m_{115211}=2\ (p=\overline{1,2})$, формула (79) із урахуванням виразу (80) набуде наступного вигляду:

$$\mathbf{RE}=\left\{\bigcup_{j=1}^{9}\mathbf{RE}_{\mathbf{j}}\right\}=\left\{\bigcup_{j=1}^{9}\left\{\bigcup_{k=1}^{m_{11j}}\mathbf{RE}_{\mathbf{jk}}\right\}\right\}=\left\{\bigcup_{j=1}^{9}\left\{\bigcup_{k=1}^{m_{11j}}\left\{\bigcup_{l=1}^{m_{11jk}}RE_{jkl}\right\}\right\}\right\}=$$

$$\left\{\bigcup_{j=1}^{9}\left\{\bigcup_{k=1}^{m_{11j}}\left\{\bigcup_{l=1}^{m_{11jk}}\left\{\bigcup_{p=1}^{m_{11jkl}}\mathbf{RE}_{\mathbf{jklp}}\right\}\right\}\right\}\right\}=\left\{\bigcup_{j=1}^{9}\left\{\bigcup_{k=1}^{m_{11j}}\left\{\bigcup_{l=1}^{m_{11jk}}\left\{\bigcup_{p=1}^{m_{11jkl}}\left\{\bigcup_{s=1}^{m_{11jklp}}RE_{jklps}\right\}\right\}\right\}\right\}\right\}=$$

$$\{\{\{RE_{111},RE_{112},RE_{113},RE_{114},RE_{115},RE_{116}\},\{RE_{121},RE_{122},RE_{123},RE_{124},$$
$$RE_{125},RE_{126}\},\{RE_{131},RE_{132},RE_{133},RE_{134},RE_{135},RE_{136}\},$$
$$\{\{\{RE_{14111},RE_{14112}\},\{RE_{14121},RE_{14122},RE_{14123},RE_{14124},RE_{14125},RE_{14126},$$
$$RE_{14127},RE_{14128}\},\{RE_{14131},RE_{14132}\},\{RE_{14141},RE_{14142}\},\{RE_{14151},RE_{14152}\},$$
$$\{RE_{14161},RE_{14162}\},\{RE_{14171},RE_{14172}\},\{RE_{14181},RE_{14182}\},\{RE_{14191},RE_{14192}\},$$
$$\{RE_{141101},RE_{141102}\},\{RE_{141111},RE_{141112}\}\},RE_{142}\},\{\{\{RE_{15111},RE_{15112}\}\},RE_{152}\},$$
$$\{RE_{161},RE_{162}\},\{RE_{171},RE_{172}\},\{RE_{181},RE_{182}\},\{RE_{191},RE_{192}\},\{RE_{1101},RE_{1102}\}\},$$
$$\{\{\{\{RE_{21111},RE_{21112}\},\{RE_{21121},RE_{21122}\},\{RE_{21131},RE_{21132}\},\{RE_{21141},RE_{21142},$$
$$RE_{21143},RE_{21144}\}\},RE_{212}\},\{RE_{221},RE_{222}\},\{RE_{231},RE_{232}\},$$
$$\{\{\{RE_{24111},RE_{24112}\},\{RE_{24121},RE_{24122},RE_{24123}\},\{RE_{24131},RE_{24132}\},$$
$$\{RE_{24141},RE_{24142},RE_{24143}\},\{RE_{24151},RE_{24152}\}\},RE_{242}\},\{RE_{251},RE_{252}\},$$
$$\{RE_{261},RE_{262}\},\{RE_{271},RE_{272}\},\{RE_{281},RE_{282}\},\{RE_{291},RE_{292}\},\{RE_{2101},RE_{2102}\}\},$$

(2.8

$$\{\{RE_{311},RE_{312},RE_{313},RE_{314}\},\{RE_{321},RE_{322}\},\{RE_{331},RE_{332},RE_{333},RE_{334},RE_{335},$$
$$RE_{336}\},\{RE_{341},RE_{342}\},\{RE_{351},RE_{352}\},\{RE_{361},RE_{362}\},\{RE_{371},RE_{372}\},$$
$$\{RE_{381},RE_{382}\},\{RE_{391},RE_{392},RE_{393}\},\{RE_{3101},RE_{3102},RE_{3103},RE_{3104}\},$$
$$\{RE_{3111},RE_{3112},RE_{3113}\},\{RE_{3121},RE_{3122},RE_{3123}\}\},$$
$$\{\{\{\{RE_{41111},RE_{41112},RE_{41113},RE_{41114},RE_{41115},RE_{41116}\},$$
$$\{RE_{41121},RE_{41122},RE_{41123},RE_{41124},RE_{41125},RE_{41126},RE_{41127},RE_{41128}\},\{RE_{41131},RE_{41132}\}\},$$
$$\{\{RE_{41211},RE_{41212},RE_{41213},RE_{41214},RE_{41215},RE_{41216}\},$$
$$\{RE_{41221},RE_{41222},RE_{41223},RE_{41224},RE_{41225},RE_{41226},RE_{41227},RE_{41228}\},\{RE_{41231},RE_{41232}\}\},$$
$$\{\{RE_{41311},RE_{41312},RE_{41313},RE_{41314},RE_{41315},RE_{41316}\},$$
$$\{RE_{41321},RE_{41322},RE_{41323},RE_{41324},RE_{41325},RE_{41326},RE_{41327},RE_{41328}\},\{RE_{41331},RE_{41332}\}\},$$
$$\{\{RE_{41411},RE_{41412},RE_{41413},RE_{41414},RE_{41415},RE_{41416}\},$$
$$\{RE_{41421},RE_{41422},RE_{41423},RE_{41424},RE_{41425},RE_{41426},RE_{41427},RE_{41428}\},\{RE_{41431},RE_{41432}\}\},$$
$$\{\{RE_{41511},RE_{41512},RE_{41513},RE_{41514},RE_{41515},RE_{41516}\},$$
$$\{RE_{41521},RE_{41522},RE_{41523},RE_{41524},RE_{41525},RE_{41526},RE_{41527},RE_{41528}\},\{RE_{41531},RE_{41532}\}\},$$
$$\{\{RE_{41611},RE_{41612},RE_{41613},RE_{41614},RE_{41615},RE_{41616}\},$$
$$\{RE_{41621},RE_{41622},RE_{41623},RE_{41624},RE_{41625},RE_{41626},RE_{41627},RE_{41628}\},\{RE_{41631},RE_{41632}\}\}, \quad (2.81)$$
$$RE_{417}\},\{RE_{421},RE_{422}\},\{RE_{431},RE_{432}\},\{RE_{441},RE_{442}\},\{RE_{451},RE_{452}\},$$
$$\{RE_{461},RE_{462}\},\{RE_{471},RE_{472}\},\{RE_{481},RE_{482}\},\{RE_{491},RE_{492}\},\{RE_{4101},RE_{4102}\}\},$$
$$\{\{RE_{511},RE_{512},RE_{513},RE_{514},RE_{515}\},\{\{\{RE_{52111},RE_{52112}\}\},RE_{522}\},$$
$$\{RE_{531},RE_{532}\},\{RE_{541},RE_{542}\},\{RE_{551},RE_{552}\},\{RE_{561},RE_{562}\},\{RE_{571},RE_{572}\},$$
$$\{RE_{581},RE_{582}\},\{RE_{591},RE_{592}\},\{RE_{5101},RE_{5102}\},\{RE_{5111},RE_{5112}\}\},$$
$$\{\{RE_{611},RE_{612}\},\{RE_{621},RE_{622}\},\{RE_{631},RE_{632}\},\{RE_{641},RE_{642}\},$$
$$\{RE_{651},RE_{652}\},\{RE_{661},RE_{662}\},\{RE_{671},RE_{672}\},\{RE_{681},RE_{682}\},\{RE_{691},RE_{692}\},$$
$$\{RE_{6101},RE_{6102}\}\},\{\{RE_{711},RE_{712}\},\{RE_{721},RE_{722}\},\{RE_{731},RE_{732}\},\{RE_{741},RE_{742}\},$$
$$\{RE_{751},RE_{752}\},\{RE_{761},RE_{762}\},\{RE_{771},RE_{772}\},\{RE_{781},RE_{782}\},\{RE_{791},RE_{792}\},$$
$$\{RE_{7101},RE_{7102}\},\{RE_{7111},RE_{7112}\},\{RE_{7121},RE_{7122}\},\{RE_{7131},RE_{7132}\}\},$$
$$\{\{RE_{811},RE_{812}\},\{RE_{821},RE_{822}\},\{RE_{831},RE_{832},RE_{833}\},\{RE_{841},RE_{842}\},$$
$$\{RE_{851},RE_{852}\},\{RE_{861},RE_{862}\},\{RE_{871},RE_{872}\},\{RE_{881},RE_{882}\},\{RE_{891},RE_{892}\},$$
$$\{RE_{8101},RE_{8102}\}\},\{\{RE_{911},RE_{912}\},\{RE_{921},RE_{922}\},\{RE_{931},RE_{932}\},\{RE_{941},RE_{942}\},$$
$$\{RE_{951},RE_{952}\},\{RE_{961},RE_{962}\},\{RE_{971},RE_{972}\},\{RE_{981},RE_{982}\},\{RE_{991},RE_{992}\},$$
$$\{RE_{9101},RE_{9102}\},\{RE_{9111},RE_{9112}\},\{RE_{9121},RE_{9122}\}\}\},$$

де: RE_{14111} = «У випадку, коли рішення для захисту від DoS/DDoS атак постачається в комплекті – воно або не має готових налаштувань для вашої інфраструктури, або має загальні налаштування, які в більшості випадків налаштовані в режимі моніторингу. Рекомендується надати можливість інженеру, що буде налаштовувати захист на всіх хмарних сервісів, розібратися в технології захисту від DoS/DDoS атак, шляхом вивчення документації та проходження навчання від постачальника хмарного сервісу, для отримання навичок роботи з рішенням.»; RE_{14112} = «У випадку, коли рішення для захисту від DoS/DDoS атак постачається як окремий платний модуль – варто передбачити виділення бюджету для даного модуля, оскільки від нього залежить доступність розгорнутих хмарних сервісів та працездатність бізнес-процесів, оскільки в іншому випадку, сервіси, розгорнуті на ресурсах хмарного провайдеру, можуть бути уражені атакою DoS/DDoS та бізнес процеси компанії можуть відмовити в обслуговуванні. Також, варто враховувати, окремий платний модуль або може не мати готових налаштувань для вашої інфраструктури, або має загальні налаштування, які в більшості випадків налаштовані в режимі моніторингу. Рекомендується надати можливість інженеру, що буде налаштовувати захист на всіх хмарних сервісів, розібратися в технології захисту від DoS/DDoS атак, шляхом вивчення документації та проходження навчання від постачальника, для отримання навичок роботи з рішенням.»; RE_{14121} = «Оскільки рішення для захисту від DoS/DDoS атак працює на таких рівнях моделі OSI як: Layer 3, Layer 4 та Layer 7, - то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист від: GET Floods, Slow POST, Slowloris тощо (L7); DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4); UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Оскільки даний модуль захисту від DoS/DDoS атак має повноцінний набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність

широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14122} = «Оскільки рішення для захисту від DoS/DDoS атак працює лише на таких рівнях моделі OSI як: Layer 3 та Layer 4, - то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист від: DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4); UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Проте варто враховувати, що хмарні сервіси не будуть захищені на Layer 7 від таких типів атак, як: GET Floods, Slow POST, Slowloris тощо. Так як, даний модуль захисту від DoS/DDoS атак лише частковий набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14123} = «Оскільки рішення для захисту від DoS/DDoS атак працює лише на таких рівнях моделі OSI як: Layer 3 та Layer 7, - то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист від: GET Floods, Slow POST, Slowloris тощо (L7); UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Проте варто враховувати, що хмарні сервіси не будуть захищені на Layer 4 від таких типів атак, як: DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо. Так як, даний модуль захисту від DoS/DDoS атак лише частковий набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14124} = «Оскільки рішення для захисту від DoS/DDoS атак працює лише на таких рівнях моделі OSI як: Layer 4 та Layer 7, - то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист від: GET Floods, Slow POST, Slowloris тощо (L7); DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4). Проте варто враховувати, що хмарні сервіси не будуть захищені на Layer 3 від

таких типів атак, як: UDP flood, ICMP flood, ACK flood, Ping flood тощо. Так як, даний модуль захисту від DoS/DDoS атак лише частковий набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14125} = «Оскільки рішення для захисту від DoS/DDoS атак працює лише на Layer 3 моделі OSI, то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист лише від: UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Проте варто враховувати, що хмарні сервіси не будуть захищені на Layer 7 та Layer 4 від таких типів атак, як: GET Floods, Slow POST, Slowloris тощо (L7); DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4). Так як, даний модуль захисту від DoS/DDoS атак лише частковий набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14126} = «Оскільки рішення для захисту від DoS/DDoS атак працює лише на Layer 4 моделі OSI, то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист лише від: DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4). Проте варто враховувати, що хмарні сервіси не будуть захищені на Layer 7 та Layer 3 від таких типів атак, як: GET Floods, Slow POST, Slowloris тощо (L7); UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Так як, даний модуль захисту від DoS/DDoS атак лише частковий набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14127} = «Оскільки рішення для захисту від DoS/DDoS атак працює лише на Layer 7 моделі OSI,

то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист лише від: GET Floods, Slow POST, Slowloris тощо (L7). Проте варто враховувати, що хмарні сервіси не будуть захищені на Layer 4 та Layer 3 від таких типів атак, як: DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4); UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Так як, даний модуль захисту від DoS/DDoS атак лише частковий набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.»; RE_{14128} = «У зв'язку з тим, що провайдер хмарних сервісів не підтримує захист на жодному з рівнів моделі OSI таких, як: Layer 3, Layer 4 та Layer 7, - це ставить під сумнів працездатність вбудованого модуля захист від DoS/DDoS атак. Рекомендується, або змінити хмарного провайдера, або використати стороннє рішення іншого розробника, що спеціалізується на захисті від DoS/DDoS атак.»; RE_{14131} = «В даному випадку, варто з певною періодичністю проводити тести на проникнення з метою перевірки коректності встановлених налаштувань розробником. Також, рекомендується скористатися стороннім рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{14132} = «Перед початком встановлення налаштувань, рекомендується надати час інженеру, що буде займатися налаштуванням захисту сервісів, розгорнутих на ресурсах хмарних сервісів, дослідити функціонал рішення із залученням інтегратора чи розробника. Додатково, рекомендується забезпечити навчання інженеру по роботі із даним рішенням, щоб навчити співробітника роботі із даним модулем захисту від DoS/DDoS атак.»; RE_{14141} = «У випадку, якщо попередньо-налаштовані правила – це лише шаблон, який можна змінювати, то варто внести зміни під функціональні можливості бізнес процесів, що функціонують на ресурсах

хмарних сервісів, оскільки попередньо-налаштовані правила не у всіх випадках працює коректно і можуть провокувати false-positive спрацювання.»; RE_{14142} = «В даному випадку, рекомендується розглянути варіант із впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{14151} = «Рекомендується, перед створенням індивідуальних правил захисту від DoS/DDoS атак, скористатися дослідженням можливостей бізнес процесів, що розгорнуті на ресурсах хмарних сервісів для можливості побудови коректних правил захисту та зменшення false-positive спрацювань.»; RE_{14152} = «В даному випадку, рекомендується розглянути варіант із впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{14161} = «В даному випадку, у випадку недостатньої видимості попередньо налаштованої аналітикою на стороні хмарного провайдера, рекомендується побудувати власні інформаційні панелі, або направити події на вашу SIEM систему, або скористатися рішенням, наприклад, Grafana, для можливості побудови індивідуальних інформаційних панелей для забезпечення кращої видимості подій та трафіку.»; RE_{14162} = «Рекомендується направити події з хмарного провайдера на вашу SIEM систему, або скористатися рішенням, наприклад, Grafana, для можливості побудови індивідуальних інформаційних панелей для забезпечення кращої видимості подій та трафіку.»; RE_{14171} = «Рекомендується, перед створенням індивідуальних rate-контролів захисту від DoS/DDoS атак, скористатися дослідженням можливостей бізнес процесів, що розгорнуті на ресурсах хмарних сервісів для можливості побудови коректних rate-контролів захисту та зменшення false-positive спрацювань та попередження блокування легітимних запитів користувачів сервісів.»; RE_{14172} = «В даному випадку, рекомендується розглянути варіант із

впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{14181} = «Рекомендується увімкнути модуль захисту від UDP Flood атак.»; RE_{14182} = «У випадку критичності відсутності модуля захисту від UDP Flood атак, рекомендується розглянути варіант із впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{14191} = «Рекомендується увімкнути модуль захисту від TCP SYN Flood атак.»; RE_{14192} = «У випадку критичності відсутності модуля захисту від TCP SYN Flood атак, рекомендується розглянути варіант із впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{141101} = «Рекомендується увімкнути модуль захисту від DNS query flood атак.»; RE_{141102} = «У випадку критичності відсутності модуля захисту від DNS query flood атак, рекомендується розглянути варіант із впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{141111} = «Рекомендується увімкнути модуль захисту від HTTP flood атак.»; RE_{141112} = «У випадку критичності відсутності модуля захисту від HTTP flood атак, рекомендується розглянути варіант із впровадженням стороннього рішенням, що спеціалізується на захисті від DoS/DDoS атак, для підвищення рівні захищеності сервісів, розгорнутих на ресурсах хмарного провайдера.»; RE_{15111} = «Незалежно від налаштувань DNS (як Primary чи Seocndary), рекомендується налаштувати захист DNSSEC для можливості захисту запитів на рівні DNS та перевірки цілісності та легітимності запитів, що передаються.»; RE_{15112} = «У випадку відсутності налаштувань DNSSEC, компанія не має змогу перевіряти легітимність та цілісність запитів, що

надсилаються на DNS сервер. Рекомендується скористатися іншим сервісом для організації захисту DNSSEC та забезпечити захист на рівні DNS запитів.»; RE_{21111} = «Рекомендується увімкнути реплікацію для забезпечення можливості відновлення даних в межах одного регіону.»; RE_{21112} = «У випадку відсутності локальної реплікації, компанія не буде мати можливість в межах одного регіону робити реплікацію між декількома VPC/VPS. У випадку необхідності, варто розглянути використання, або іншого хмарного провайдера, або власні засоби для проведення реплікації даних між декількома VPC/VPS в межах одного регіону.»; RE_{21121} = «Рекомендується увімкнути реплікацію для забезпечення можливості відновлення даних в межах декількох виділених регіонів.»; RE_{21122} = «У випадку відсутності регіональної реплікації, компанія не буде мати можливість в межах декількох виділених регіонів робити реплікацію між декількома VPC/VPS. У випадку необхідності, варто розглянути використання, або іншого хмарного провайдера, або власні засоби для проведення реплікації даних між декількома VPC/VPS в межах декількох виділених регіонах.»; RE_{21131} = «Рекомендується увімкнути реплікацію для забезпечення можливості відновлення даних в межах виділених GEO-розподілених регіонів»; RE_{21132} = «У випадку відсутності GEO-розподіленої реплікації, компанія не буде мати можливість в межах декількох виділених регіонів робити реплікацію між декількома VPC/VPS. У випадку необхідності, варто розглянути використання, або іншого хмарного провайдера, або власні засоби для проведення реплікації даних між декількома VPC/VPS в межах декількох виділених регіонах.»; RE_{21141} = «Рекомендується застосувати даний метод реплікації.»; RE_{21142} = «Рекомендується застосувати даний метод реплікації.»; RE_{21143} = «Використовуючи бізнес-потреби компанії забезпечити використання, як синхронної, так і асинхронної

реплікації даних між декількома VPC/VPS, що забезпечують функціонування бізнес-критичних сервісів компанії.»; RE_{21144} = «У випадку, якщо постачальник хмарних сервісів не буде мати можливість робити реплікацію, як синхронну, так і асинхронну, компанія не буде спроможна оперативно оновлювати інформацію на декількох VPC/VPS серверах, що необхідні для реплікації даних. В такому випадку, необхідно скористатися власними засобами, для забезпечення перевірки актуальності даних на реплікаційних VPC/VPS.»; RE_{24111} = «Дані компанії знаходяться в безпеці і не будуть передані третім особам.»; RE_{24112} = «У даному випадку, ключі, що використовуються для шифрування дискового простору знаходяться, як в компанії, так і в постачальника, що ставить під сумнів конфіденційність даних компанії, що зберігаються на ресурсах хмарних сервісів.»; RE_{24121} = «У даному випадку, ключі, що використовуються для шифрування дискового простору знаходяться в постачальника, що ставить під сумнів конфіденційність даних компанії, що зберігаються на ресурсах хмарних сервісів.»; RE_{24122} = «Дані компанії знаходяться в безпеці і не будуть передані третім особам.»; RE_{24123} = «У даному випадку, ключі, що використовуються для шифрування дискового простору знаходяться, як в компанії, так і в постачальника, що ставить під сумнів конфіденційність даних компанії, що зберігаються на ресурсах хмарних сервісів.»; RE_{24131} = «Рекомендується використання даного хмарного провайдера.»; RE_{24132} = «НЕ рекомендується використання даного хмарного провайдера.»; RE_{24141} = «-»; RE_{24142} = «-»; RE_{24143} = «-»; RE_{24151} = «Рекомендується використання даного хмарного провайдера.»; RE_{24152} = «У випадку використання симетричного шифрування нижче ніж AES-256, компанія ставить під сумнів криптостійкість даних, що зберігаються на ресурсах хмарних сервісів, оскільки симетричні методи

шифрування нижче ніж AES-256 мають публічні вразливості та методи їх експлуатації.»;

$RE_{41111} = RE_{41211} = RE_{41311} = RE_{41411} = RE_{41511} = RE_{41611} =$ «При аудиті безпекових налаштувань системи віртуалізації кожного квартал та застосування виправлень – можна рекомендувати розгортання критичних бізнес сервісів на ресурсах даного хмарного провайдера.»;

$RE_{41112} = RE_{41212} = RE_{41312} = RE_{41412} = RE_{41512} = RE_{41612} =$ «При аудиті безпекових налаштувань системи віртуалізації кожні пів року та застосування виправлень – можна рекомендувати розгортання критичних бізнес сервісів на ресурсах даного хмарного провайдера.»;

$RE_{41113} = RE_{41213} = RE_{41313} = RE_{41413} = RE_{41513} = RE_{41613} =$ «При аудиті безпекових налаштувань системи віртуалізації кожного року та застосування виправлень – можна рекомендувати розгортання критичних бізнес сервісів на ресурсах даного хмарного провайдера.»;

$RE_{41114} = RE_{41214} = RE_{41314} = RE_{41414} = RE_{41514} = RE_{41614} =$ «При аудиті безпекових налаштувань системи віртуалізації кожні два роки та застосування виправлень – необхідно з обережністю відноситися до розгортання критичних бізнес сервісів компанії.»;

$RE_{41115} = RE_{41215} = RE_{41315} = RE_{41415} = RE_{41515} = RE_{41615} =$ «При аудиті безпекових налаштувань системи віртуалізації кожні п'ять років та застосування виправлень – не можна рекомендувати розгортання критичних бізнес сервісів компанії, тому рекомендується розгортання критичних бізнес сервісів на ресурсах іншого хмарного провайдера, проте ресурси даного хмарного провайдера можна використовувати в якості тестового полігону.»;

$RE_{41116} = RE_{41216} = RE_{41316} = RE_{41416} = RE_{41516} = RE_{41616} =$ «У разі відсутності аудиту безпеки системи віртуалізації хмарного провайдера – існує імовірність, що хмарний провайдер використовує застарілу версію системи віртуалізації,

що має безліч вразливостей чи некоректних налаштувань, що ставить під сумнів безпечне використання та розгортання критичних сервісів компанії на ресурсах даного хмарного провайдера. Якщо планується розгортання критичних бізнес сервісів – рекомендується скористатися послугами іншого хмарного провайдера.»;

$RE_{41121} = RE_{41221} = RE_{41321} = RE_{41421} = RE_{41521} = RE_{41621} =$ «Рекомендація непередбачена.»;

$RE_{41122} = RE_{41222} = RE_{41322} = RE_{41422} = RE_{41522} = RE_{41622} =$ «Рекомендація непередбачена.»;

$RE_{41123} = RE_{41223} = RE_{41323} = RE_{41423} = RE_{41523} = RE_{41623} =$ «Рекомендація непередбачена.»;

$RE_{41124} = RE_{41224} = RE_{41324} = RE_{41424} = RE_{41524} = RE_{41624} =$ «Рекомендація непередбачена.»;

$RE_{41125} = RE_{41225} = RE_{41325} = RE_{41425} = RE_{41525} = RE_{41625} =$ «Рекомендація непередбачена.»;

$RE_{41126} = RE_{41226} = RE_{41326} = RE_{41426} = RE_{41526} = RE_{41626} =$ «Рекомендація непередбачена.»;

$RE_{41127} = RE_{41227} = RE_{41327} = RE_{41427} = RE_{41527} = RE_{41627} =$ «Рекомендація непередбачена.»;

$RE_{41128} = RE_{41228} = RE_{41328} = RE_{41428} = RE_{41528} = RE_{41628} =$ «Рекомендація не передбачена.»;

$RE_{41131} = RE_{41231} = RE_{41331} = RE_{41431} = RE_{41531} = RE_{41631} =$ «Використання даного хмарного провайдера рекомендується, як для критичних так і некритичних бізнес сервісів компанії»;

$RE_{41132} = RE_{41232} = RE_{41332} = RE_{41432} = RE_{41532} = RE_{41632} =$ «У випадку, якщо система віртуалізації знаходиться не в ізольованому середовищі – є імовірність, що доступ до системи віртуалізації можливий з мережі інтернет, що ставить під сумнів безпечне використання та розгортання критичних бізнес

сервісів, що можуть бути скомпрометованими. Рекомендується на ресурсах даного хмарного провайдера не розгортати критичні бізнес сервіси компанії, та використовувати іншого хмарного провайдера для розгортання критичних бізнес сервісів компанії.»;

RE_{52111} = «Рекомендується налаштувати шифрування резервних копій з метою уникнення можливості компрометації конфіденційних даних компанії.»; RE_{52112} = «Відсутність захисту резервної копії ключем шифрування означає, що будь-хто може скористатися копією та розгорнути її на власних ресурсах із даними, що були збережені в певний момент часу, що спровокує витік конфіденційних даних компанії. Рекомендується надавати доступ до створення та управління резервними копіями лише відповідальних осіб.» [108].

Для представлення узагальненого вигляду розробленої моделі, що був розроблений із урахуванням різноманітних типів хмарних сервісів, що є представленими на ринку, із перевіркою використання необхідних компонентів, для забезпечення безпечного розгортання бізнес сервісів компанії та забезпеченням наявності рекомендацій для кожного питання, рекомендується поглянути на Рис. 2.1, що надає можливість оцінити структуру розробленого математичної моделі у вигляді узагальненої схеми, що буде містити всі можливі рівні та включатиме параметри оцінки хмарних сервісів [108, 103]:

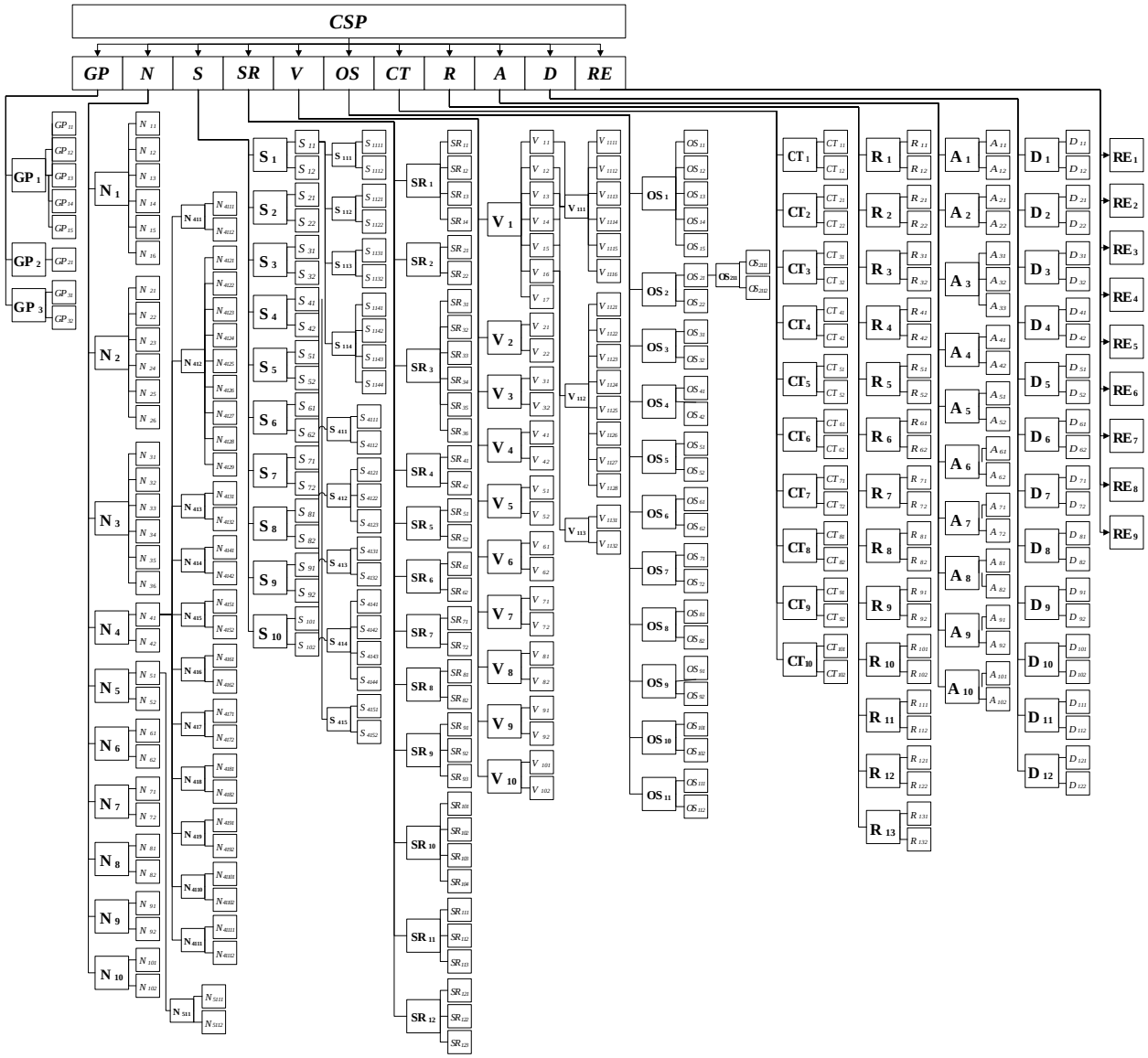


Рис. 2.1. Узагальнена схема математичної моделі оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури

2.2. Математичний метод захищеного застосунку оцінювання кіберзахищеності хмарних сервісів від витоку конфіденційних даних компаній

Для обчислення рівня захищеності хмарного сервісу (**ЗХС**) від витоку конфіденційних даних компаній, для кожного із описаних вище одинадцяти пунктів затверджено сталу оцінку, в залежності від суми яких постачальник хмарних сервісів отримає задоволення щодо рекомендації чи не рекомендації у використанні оцінюваного постачальника для розміщення на ресурсах останнього критичних бізнес процесів та сервісів компанії. В залежності від

наданих відповідей аудитором – по кожному з оцінюваних пунктів буде надано рекомендацію щодо використання певного функціоналу чи усунення прогалини в забезпеченні безпеки розгорнутих сервісів компанії [107].

Всі затверджені сталі оцінки було виставлено з використанням балів в діапазоні від 0 до 5, де 0 – це найнижчий бал оцінювання, а 5 – це найвищий бал оцінювання [106, 95].

Для одинадцяти компонентів кортежу, описаних в розділі 2 пункту 1, пропонується метод для визначення ЗХС [106].

Зважаючи на детально описані компоненти кортежу визначено десять основних етапів визначення ЗХС:

- отримання загальної інформації про оцінюваний хмарний сервіс та роботу з країнами-агресорами;
- визначення рівня захищеності мережевого модуля хмарного сервісу;
- визначення рівня захищеності модуля зберігання даних хмарного сервісу;
- визначення рівня захищеності серверного модуля хмарного сервісу;
- визначення рівня захищеності модуля віртуалізації хмарного сервісу;
- визначення рівня захищеності модуля операційної системи хмарного сервісу;
- визначення рівня захищеності модуля управління контейнеризацією хмарного сервісу;
- визначення рівня захищеності модуля забезпечення безперервної роботи хмарного сервісу;
- визначення рівня захищеності модуля управління додатками хмарного сервісу;
- визначення рівня захищеності модуля обробки та управління даними хмарного сервісу [106].

Варто врахувати, що в оцінці будуть брати участь різноманітні типи хмарних сервісів, що маркуються, як:

- IaaS (Infrastructure-as-a-Service).

- CaaS (Container-as-a-Service).
- PaaS (Platform-as-a-Service).
- FaaS (Function-as-a-Service).
- SaaS (Software-as-a-Service).

Оскільки для кожного типу хмарного сервісу доступна в опрацювання лише частина модулів, то відповідно і оцінки ЗХС має відбуватися по визначеному наборі етапів. В Табл. 2.1, що зображена нижче, представлено залежність кожного із типів хмарних сервісів та модулів, що застосовуються до них [106].

Таблиця 2.1.

Параметри залежності модулів і типів хмарних сервісів

№	Параметр	IaaS	CaaS	PaaS	FaaS	SaaS
1	$CSP_1 = GP =$ "***General Points module***"	+	+	+	+	+
2	$CSP_2 = N =$ "***Network module***"	+	+	+	+	+
3	$CSP_3 = S =$ "***Storage module***"	+	+	+	+	+
4	$CSP_4 = SR =$ "***Server module***"	+	+	+	+	+
5	$CSP_5 = V =$ "***Virtualization module***"	+	+	+	+	+
6	$CSP_6 = OS =$ "***Operation System module***"	-	+	+	+	+
7	$CSP_7 = CT =$ "***Container Technology module***"	-	+	+	+	+
8	$CSP_8 = R =$ "***Runtime module***"	-	-	+	+	+
9	$CSP_9 = A =$ "***Application module***"	-	-	-	+	+
10	$CSP_{10} = D =$ "***Data module***"	-	-	-	-	+
11	$CSP_{11} = RE =$ "***Recommendation's module***"	+	+	+	+	+

Нижче описано кожний етап ЗХС, що базується на продемонстрованих у Розділі 2.1 компонентах кортежу та затвердженої оцінки для кожного визначеного питання-відповіді [106].

Отримання загальної інформації про оцінюваний хмарний сервіс та роботу з країнами-агресорами (ЗІ)

Етап 1 – визначення загальної інформації про оцінюваний хмарний сервіс. Для формування значення параметру **GP**, аудитору необхідно визначити тип оцінюваного хмарного сервісу, його назви та співпраці з країнами-агресорами [106].

Наприклад, якщо компанія планує оцінити PaaS сервіс, що має назву «Enco Industries» та не співпрацює з країнами-агресорами, то даний компонент, враховуючи формулу (2.7), буде виглядати наступним чином [106]:

$$\mathbf{CSP}_1 = \mathbf{GP} = \{PaaS, "Enco\ Industries", Hi\}, \quad (2.82)$$

Варто врахувати, що на першому етапі не застосовуються оцінки по причині того, що даний компонент несе в собі виключно інформаційних характер про оцінюваного постачальника хмарного сервісу [106].

Визначення рівня захищеності мережевого модуля хмарного сервісу (ЗММ)

Етап 2 – визначення рівня захищеності мережевого модуля хмарного сервісу. Задля уникнення повторного визначення формул, розпочинаючи з даного компоненту і до десятого – буде взято за основу лише останню виведену формулу для якої і буде застосовано затверджену кількість балів, що відповідає кожному із варіантів відповідей [106].

Для даного етапу, шляхом перетворення формули (2.12), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP}_2 = \mathbf{N} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{2j}} N_{jk}\right\}\right\} = \{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\},$$
$$\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\},$$
$$\{N_{41}, N_{42}\}, \{N_{51}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\},$$
$$\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\}\} = \quad (2.83)$$
$$\{\{"5","4","3","2","1","0"\},$$
$$\{"5","4","3","2","1","0"\}, \{"5","4","3","2","1","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}\},$$

де: N_{11} = «99.9999% (простій в рік 31,5 секунд)» = "*5*" (балів); N_{12} = «99.999% (простій в рік 5,26 хвилин)» = "*4*" (бали); N_{13} = «99.99% (простій в рік 52,56 хвилин)» = "*3*" (бали); N_{14} = «99.9% (простій в рік 8,76 годин)» = "*2*" (бали); N_{15} = «99% (простій в рік 3,65 днів)» = "*1*" (бал); N_{16} = «90% і менше (простій в рік 36,5 днів)» = "*0*" (балів); N_{21} = «більше 30» = "*5*" (балів); N_{22} = «21-30» = "*4*" (бали); N_{23} = «11-20» = "*3*" (бали); N_{24} = «6-10» = "*2*" (бали); N_{25} = «2-5» = "*1*" (бал); N_{26} = «1» = "*0*" (балів); N_{31} = «301-400 і більше» = "*5*" (балів); N_{32} = «201-300» = "*4*" (бали); N_{33} = «101-200» = "*3*" (бали); N_{34} = «51-100» = "*2*" (бали); N_{35} = «2-50» = "*1*" (бал); N_{36} = «1 і менше» = "0" (балів); N_{41} = «Так» = "*5*" (балів); N_{42} = «Ні» = "*0*" (балів); N_{51} = «Так» = "*5*" (балів); N_{52} = «Ні» = "*0*" (балів); N_{61} = «Так» = "*5*" (балів); N_{62} = «Ні» = "*0*" (балів); N_{71} = «Так» = "*5*" (балів); N_{72} = «Ні» = "*0*" (балів); N_{81} = «Так» = "*5*" (балів); N_{82} = «Ні» = "*0*" (балів); N_{91} = «Так» = "*5*" (балів); N_{92} = «Ні» = "*0*" (балів); N_{101} = «Так» = "*5*" (балів); N_{102} = «Ні» = "*0*" (балів) [106].

Аналогічно, перетворивши формулу (2.16), ми отримаємо наступний вигляд другого рівня компоненту [106]:

$$\mathbf{CSP}_2 = \mathbf{N} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{2j}} \left\{ \bigcup_{l=1}^{m_{2jk}} \left\{ \bigcup_{p=1}^{m_{2jkl}} N_{jklp} \right\} \right\} \right\} \right\}$$

$$\begin{gathered}
\{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{16}\}, \\
\{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}, N_{26}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}, N_{36}\}, \\
\{\{\{N_{4111}, N_{4112}\}, \{N_{4121}, N_{4122}, N_{4123}, N_{4124}, N_{4125}, N_{4126}, N_{4127}, N_{4128}\}, \\
\{N_{4131}, N_{4132}\}, \{N_{4141}, N_{4142}\}, \{N_{4151}, N_{4152}\}, \{N_{4161}, N_{4162}\}, \{N_{4171}, N_{4172}\}, \\
\{N_{4181}, N_{4182}\}, \{N_{4191}, N_{4192}\}, \{N_{41101}, N_{41102}\}, \{N_{41111}, N_{41112}\}\}, N_{42}\}, \\
\{\{\{N_{5111}, N_{5112}\}\}, N_{52}\}, \{N_{61}, N_{62}\}, \{N_{71}, N_{72}\}, \{N_{81}, N_{82}\}, \\
\{N_{91}, N_{92}\}, \{N_{101}, N_{102}\}\} = \\
\{\{"5","4","3","2","1","0"\}, \\
\{"5","4","3","2","1","0"\}, \{"5","4","3","2","1","0"\}, \\
\{\{\{"5","3"\}, \{"5","3","3","3","1","1","1","0"\}, \{"5","5"\}, \{"5","0"\}, \{"5","0"\}, \\
\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\}, "0"\}, \\
\{\{\{"5","0"\}\}, "0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\
\{"5","0"\}, \{"5","0"\}\},
\end{gathered} \tag{2.84}$$

де: N_{4111} = «Постачається в комплекті» = "*5*" (балів); N_{4112} = «Постачається як окремий платний модуль» = "*3*" (бали); N_{4121} = «Layer 3, 4, 7» = "*5*" (балів); N_{4122} = «Layer 3, 4» = "*3*" (бали); N_{4123} = «Layer 3, 7» = "*3*" (бали); N_{4124} = «Layer 4, 7» = "*3*" (бали); N_{4125} = «Тільки Layer 3» = "*1*" (бал); N_{4126} = «Тільки Layer 4» = "*1*" (бал); N_{4127} = «Тільки Layer 7» = "*1*" (бал); N_{4128} = «На жодному з вище перелічених» = "*0*" (балів); N_{4131} = «Виробником» = "*5*" (балів); N_{4132} = «Замовником» = "*5*" (балів); N_{4141} = «Так» = "*5*" (балів); N_{4142} = «Ні» = "*0*" (балів); N_{4151} = «Так» = "*5*" (балів); N_{4152} = «Ні» = "*0*" (балів); N_{4161} = «Так» = "*5*" (балів); N_{4162} = «Ні» = "*0*" (балів); N_{4171} = «Так» = "*5*" (балів); N_{4172} = «Ні» = "*0*" (балів); N_{4181} = «Так» = "*5*" (балів); N_{4182} = «Ні» = "*0*" (балів); N_{4191} = «Так» = "*5*" (балів); N_{4192} = «Ні» = "*0*" (балів); N_{41101} = «Так» = "*5*" (балів); N_{41102} = «Ні» = "*0*" (балів); N_{41111} = «Так» = "*5*" (балів); N_{41112} = «Ні» = "*0*" (балів); N_{5111} = «Так» = "*5*" (балів); N_{5112} = «Ні» = "*0*" (балів) [106].

Визначення рівня захищеності модуля зберігання даних хмарного сервісу (ЗМЗД)

Етап 3 – визначення рівня захищеності модуля, що відповідає за зберігання даних для віх орендованих сервісів хмарного провайдера [106].

Для даного етапу, шляхом перетворення формули (2.21), отримаємо наступний вигляд компоненту [106]:

$$\begin{gathered}\mathbf{CSP}_3 = \mathbf{S} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{3j}} S_{jk}\right\}\right\} = \{\{S_{11}, S_{12}\}, \\ \{S_{21}, S_{22}\}, \{S_{31}, S_{32}\}, \{S_{41}, S_{42}\}, \{S_{51}, S_{52}\}, \\ \{S_{61}, S_{62}\}, \{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\}, \\ \{S_{101}, S_{102}\}\} = \\ \{\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\ \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\ \{"5","0"\}, \{"5","0"\}\},\end{gathered} \tag{2.85}$$

де: S_{11} = «Так» = “*5*” (балів); S_{12} = «Ні» = “*0*” (балів); S_{21} = «Так» = “*5*” (балів); S_{22} = «Ні» = “*0*” (балів); S_{31} = «Так» = “*5*” (балів); S_{32} = «Ні» = “*0*” (балів); S_{41} = «Так» = “*5*” (балів); S_{42} = «Ні» = “*0*” (балів); S_{51} = «Так» = “*5*” (балів); S_{52} = «Ні» = “*0*” (балів); S_{61} = «Так» = “*5*” (балів); S_{62} = «Ні» = “*0*” (балів); S_{71} = «Так» = “*5*” (балів); S_{72} = «Ні» = “*0*” (балів); S_{81} = «Так» = “*5*” (балів); S_{82} = «Ні» = “*0*” (балів); S_{91} = «Так» = “*5*” (балів); S_{92} = «Ні» = “*0*” (балів); S_{101} = «Так» = “*5*” (балів); S_{102} = «Ні» = “*0*” (балів) [106].

Аналогічно, перетворивши формулу (2.25), ми отримаємо наступний вигляд другого рівня компоненту [106]:

$$\mathbf{CSP}_3 = \mathbf{S} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{3j}} \left\{ \bigcup_{l=1}^{m_{3jk}} \left\{ \bigcup_{p=1}^{m_{3jkl}} S_{jklp} \right\} \right\} \right\} \right\} =$$

$$\{\{\{\{S_{1111}, S_{1112}\}, \{S_{1121}, S_{1122}\}, \{S_{1131}, S_{1132}\}, \{S_{1141}, S_{1142}, S_{1143}, S_{1144}\}\}, S_{12}\},$$
$$\{S_{21}, S_{22}\}, \{S_{31}, S_{32}\}, \{\{\{S_{4111}, S_{4112}\}, \{S_{4121}, S_{4122}, S_{4123}\}, \{S_{4131}, S_{4132}\},$$
$$\{S_{4141}, S_{4142}, S_{4143}, S_{4144}\}, \{S_{4151}, S_{4152}\}\}, S_{42}\}, \{S_{51}, S_{52}\}, \{S_{61}, S_{62}\}, \quad (2.86)$$
$$\{S_{71}, S_{72}\}, \{S_{81}, S_{82}\}, \{S_{91}, S_{92}\}, \{S_{101}, S_{102}\}\} =$$
$$\{\{\{\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"3","3","5","0"\}\}, "0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{\{\{"0","5"\}, \{"0","5","0"\}, \{"5","0"\},$$
$$\{"3","4","5"\}, \{"5","0"\}\}, "0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\},$$

де: S_{1111} = «Так» = “*5*” (балів); S_{1112} = «Ні» = “*0*” (балів); S_{1121} = «Так = “*5*” (балів)»; S_{1122} = «Ні» = “*0*” (балів); S_{1131} = «Так» = “*5*” (балів); S_{1132} = «Ні» = “*0*” (балів); S_{1141} = «Synchronous Replication» = “*3*” (бали); S_{1142} = «Asynchronous Replication» = “*3*” (бали); S_{1143} = «Всі вище перелічені» = “*5*” (балів); S_{1144} = «Жодного зі вище перелічених» = “*0*” (балів); S_{4111} = «Так» = “*0*” (балів); S_{4112} = «Ні» = “*5*” (балів); S_{4121} = «Постачальником» = “*0*” (балів); S_{4122} = «Замовником» = “*5*” (балів); S_{4123} = «Постачальником і замовником» = “*0*” (балів); S_{4131} = «Так» = “*5*” (балів); S_{4132} = «Ні» = “*0*” (балів); S_{4141} = «Симетричне шифрування» = “*3*” (бали); S_{4142} = «Асиметричне шифрування» = “*4*” (бали); S_{4143} = «Симетричне та асиметричне шифрування» = “*5*” (балів); S_{4151} = «Так» = “*5*” (балів); S_{4152} = «Ні» = “*0*” (балів) [106, 102].

Визначення рівня захищеності серверного модуля хмарного сервісу (ЗСМ)

Етап 4 – визначення рівня захищеності серверної частини хмарного сервісу, що відповідає за обчислювальні потужності постачальника [106].

Для даного етапу, шляхом перетворення формули (2.30), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP}_4 = \mathbf{SR} = \left\{ \bigcup_{j=1}^{12} \left\{ \bigcup_{k=1}^{m_{4j}} SR_{jk} \right\} \right\} =$$

$$\{\{SR_{11}, SR_{12}, SR_{13}, SR_{14}\}, \{SR_{21}, SR_{22}\},$$
$$\{SR_{31}, SR_{32}, SR_{33}, SR_{34}, SR_{35}, SR_{36}\}, \{SR_{41}, SR_{42}\}, \{SR_{51}, SR_{52}\},$$
$$\{SR_{61}, SR_{62}\}, \{SR_{71}, SR_{72}\}, \{SR_{81}, SR_{82}\}, \{SR_{91}, SR_{92}, SR_{93}\},$$
$$\{SR_{101}, SR_{102}, SR_{103}, SR_{104}\}, \{SR_{111}, SR_{112}, SR_{113}\}, \{SR_{121}, SR_{122}, SR_{123}\}\} =$$
$$\{\{"4","3","2","5"\}, \{"5","0"\},$$
$$\{"5","4","3","2","0","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","2","0"\},$$
$$\{"5","3","3","0"\}, \{"5","3","0"\}, \{"5","2","0"\}\}, \quad (2.87)$$

де: SR_{11} = «Обмежений лише для співробітників хмарного сервісу» = "*4*" (бали); SR_{12} = «Доступ надається для співробітників хмарного сервісу та співробітників центру обробки даних» = "*3*" (бали); SR_{13} = «Доступ надається для співробітників хмарного сервісу, замовників хмарного сервісу та співробітників центру обробки даних» = "*2*" (бали); SR_{14} = «Доступ до серверів заборонений для всіх, окрім співробітників центру обробки даних» » = "*5*" (балів); SR_{21} = «Так» = "*5*" (балів); SR_{22} = «Ні» = "*0*" (балів); SR_{31} = «ключ-картам та фізичним ключем доступу» = "*5*" (балів); SR_{32} = «ключ-картам» = "*4*" (бали); SR_{33} = «шляхом передачі фізичного ключа» = "*3*" (бали); SR_{34} = «по індивідуальним паперовим перепусткам» = "*2*" (бали); SR_{35} = «по знайомству» = "*0*" (балів); SR_{36} = «ніяк не контролюється» = "*0*" (балів); SR_{41} = «Так, має автономні джерела подачі живлення (генератори, власні підстанції тощо)» = "*5*" (балів); SR_{42} = «Ні» = "*0*" (балів); SR_{51} = «Так» = "*5*" (балів); SR_{52} = «Ні» = "*0*" (балів); SR_{61} = «Так» = "*5*" (балів); SR_{62} = «Ні» = "*0*" (балів); SR_{71} = «Так» = "*5*" (балів); SR_{72} = «Ні» = "*5*" (балів); SR_{81} = «Так» = "*5*" (балів); SR_{82} = «Ні» = "*5*" (балів); SR_{91} = «Так» = "*5*" (балів); SR_{92} = «Частково, використовуються тільки звичайні мережеві екрани (iptables, local FW etc)» = "*2*" (бали); SR_{93} = «Ні» = "*0*" (балів); SR_{101} = «Так» = "*5*" (балів);

SR_{102} = «Ні, тільки IPS» = "*3*" (бали); SR_{103} = «Ні, тільки IDS» = "*3*" (бали); SR_{104} = «Відсутні системи IPS/IDS» = "*0*" (балів); SR_{111} = «Взагалі неможливе» = "*5*" (балів); SR_{112} = «Можливе за попереднім запитом від хмарного сервісу та тримання тимчасового доступу» = "*3*" (бали); SR_{113} = «Будь-хто має можливість підключитися до серверів після входу в серверну кімнату» = "*0*" (балів); SR_{121} = «Автоматично відновлюються на суміжному резервному сервері та продовжують виконувати бізнес-процедури хмарного сервісу» = "*5*" (балів); SR_{122} = «Вручну переносяться на суміжні сервери для відновлення працездатності бізнесу» = "*2*" (бали); SR_{123} = «Не зберігаються і не відновлюються» = "*0*" (балів) [106, 102].

Визначення рівня захищеності модуля віртуалізації хмарного сервісу (ЗМВ)

Етап 5 – визначення рівня захищеності модуля віртуалізації, що відповідає за функціонування всіх VPC/VDS серверів, що надає постачальник хмарних сервісів [106].

Для даного етапу, шляхом перетворення формули (2.35), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP}_5 = \mathbf{V} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} V_{jk} \right\} \right\} =$$

$$\begin{gathered} \{\{V_{11}, V_{12}, V_{13}, V_{14}, V_{15}, V_{16}, V_{17}\}, \\ \{V_{21}, V_{22}\}, \{V_{31}, V_{32}\}, \{V_{41}, V_{42}\}, \{V_{51}, V_{52}\}, \{V_{61}, V_{62}\}, \\ \{V_{71}, V_{72}\}, \{V_{81}, V_{82}\}, \{V_{91}, V_{92}\}, \{V_{101}, V_{102}\}\} = \\ \{\{"5","5","5","3","3","2","0"\}, \\ \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\ \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\}, \end{gathered} \tag{2.88}$$

де: V_{11} = «Vmware vCenter» = "*5*" (балів); V_{12} = «Vmware vSphere» = "*5*" (балів); V_{13} = «Microsoft Hyper-V» = "*5*" (балів); V_{14} = «KVM» = "*3*" (бали); V_{15} = «Citrix XenServer» = "*3*" (бали); V_{16} = «Інше» = "*2*" (бали); V_{17} = «Не

використовується» = “*0*” (балів); V_{21} = «Так» = “*5*” (балів); V_{22} = «Ні» = “*0*” (балів); V_{31} = «Так» = “*5*” (балів); V_{32} = «Ні» = “*0*” (балів); V_{41} = «Так» = “*5*” (балів); V_{42} = «Ні» = “*0*” (балів); V_{51} = «Так» = “*5*” (балів); V_{52} = «Ні» = “*0*” (балів); V_{61} = «Так» = “*5*” (балів); V_{62} = «Ні» = “*0*” (балів); V_{71} = «Так» = “*5*” (балів); V_{72} = «Ні» = “*0*” (балів); V_{81} = «Так» = “*5*” (балів); V_{82} = «Ні» = “*0*” (балів); V_{91} = «Так» = “*5*” (балів); V_{92} = «Ні» = “*0*” (балів); V_{101} = «Так» = “*5*” (балів); V_{102} = «Ні» = “*0*” (балів) [106].

Аналогічно, перетворивши формулу (2.39), ми отримаємо наступний вигляд другого рівня компоненту [106]:

$$\mathbf{CSP}_5 = \mathbf{V} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{5j}} \left\{ \bigcup_{l=1}^{m_{5jk}} \left\{ \bigcup_{p=1}^{m_{5jkl}} V_{jklp} \right\} \right\} \right\} \right\}$$

$$\begin{gathered}
\{\{\{\{V_{1111},V_{1112},V_{1113},V_{1114},V_{1115},V_{1116}\},\\
\{V_{1121},V_{1122},V_{1123},V_{1124},V_{1125},V_{1126},V_{1127},V_{1128}\},\{V_{1131},V_{1132}\}\},\\
\{\{V_{1211},V_{1212},V_{1213},V_{1214},V_{1215},V_{1216}\},\\
\{V_{1221},V_{1222},V_{1223},V_{1224},V_{1225},V_{1226},V_{1227},V_{1228}\},\{V_{1231},V_{1232}\}\},\\
\{\{V_{1311},V_{1312},V_{1313},V_{1314},V_{1315},V_{1316}\},\\
\{V_{1321},V_{1322},V_{1323},V_{1324},V_{1325},V_{1326},V_{1327},V_{1328}\},\{V_{1331},V_{1332}\}\},\\
\{\{V_{1411},V_{1412},V_{1413},V_{1414},V_{1415},V_{1416}\},\\
\{V_{1421},V_{1422},V_{1423},V_{1424},V_{1425},V_{1426},V_{1427},V_{1428}\},\{V_{1431},V_{1432}\}\},\\
\{\{V_{1511},V_{1512},V_{1513},V_{1514},V_{1515},V_{1516}\},\\
\{V_{1521},V_{1522},V_{1523},V_{1524},V_{1525},V_{1526},V_{1527},V_{1528}\},\{V_{1531},V_{1532}\}\},\\
\{\{V_{1611},V_{1612},V_{1613},V_{1614},V_{1615},V_{1616}\},\\
\{V_{1621},V_{1622},V_{1623},V_{1624},V_{1625},V_{1626},V_{1627},V_{1628}\},\{V_{1631},V_{1632}\}\},\\
V_{17}\},\{V_{21},V_{22}\},\{V_{31},V_{32}\},\{V_{41},V_{42}\},\{V_{51},V_{52}\},\{V_{61},V_{62}\},\\
\{V_{71},V_{72}\},\{V_{81},V_{82}\},\{V_{91},V_{92}\},\{V_{101},V_{102}\}\} =\\
\{\{\{\text{"5","4","3","2","1","0"}\},\{\text{"3","4","5","1","2","3","4","0"}\},\{\text{"5","0"}\}\},\\
\{\{\text{"5","4","3","2","1","0"}\},\{\text{"3","4","5","1","2","3","4","0"}\},\{\text{"5","0"}\}\},\\
\{\{\text{"5","4","3","2","1","0"}\},\{\text{"3","4","5","1","2","3","4","0"}\},\{\text{"5","0"}\}\},\\
\{\{\text{"5","4","3","2","1","0"}\},\{\text{"3","4","5","1","2","3","4","0"}\},\{\text{"5","0"}\}\},\\
\{\{\text{"5","4","3","2","1","0"}\},\{\text{"3","4","5","1","2","3","4","0"}\},\{\text{"5","0"}\}\},\\
\{\{\text{"5","4","3","2","1","0"}\},\{\text{"3","4","5","1","2","3","4","0"}\},\{\text{"5","0"}\}\},\\
\text{"0"}\},\{\text{"5","0"}\},\{\text{"5","0"}\},\{\text{"5","0"}\},\{\text{"5","0"}\},\{\text{"5","0"}\},\\
\{\text{"5","0"}\},\{\text{"5","0"}\},\{\text{"5","0"}\},\{\text{"5","0"}\}\},
\end{gathered} \tag{2.89}$$

де: $V_{1111} = V_{1211} = V_{1311} = V_{1411} = V_{1511} = V_{1611}$ = «Раз на квартал» = “*5*” (балів); $V_{1112} = V_{1212} = V_{1312} = V_{1412} = V_{1512} = V_{1612}$ = «Раз на пів року» = “*4*” (бали); $V_{1113} = V_{1213} = V_{1313} = V_{1413} = V_{1513} = V_{1613}$ = «Раз на рік» = “*3*” (бали); $V_{1114} = V_{1214} = V_{1314} = V_{1414} = V_{1514} = V_{1614}$ = «Раз на 2 роки» = “*2*” (бали); $V_{1115} = V_{1215} = V_{1315} = V_{1415} = V_{1515} = V_{1615}$ = «Раз на 5 років» = “*1*” (бал); $V_{1116} = V_{1216} = V_{1316} = V_{1416} = V_{1516} = V_{1616}$ = «Не проводиться» = “*0*” (балів); $V_{1121} = V_{1221} = V_{1321} = V_{1421} = V_{1521} = V_{1621}$ = «Замовник» = “*3*” (бали); $V_{1122} = V_{1222} = V_{1322} = V_{1422} = V_{1522} = V_{1622}$ = «Представники постачальника хмарного сервісу» = “*4*” (бали); $V_{1123} = V_{1223} = V_{1323} = V_{1423} = V_{1523} = V_{1623}$ = «Представники центру обробки даних та датацентру» = “*5*” (балів); $V_{1124} = V_{1224} = V_{1324} = V_{1424} = V_{1524} = V_{1624}$ = «1, 2 та 3» = “*1*” (бал); $V_{1125} = V_{1225} = V_{1325} = V_{1425} = V_{1525} = V_{1625}$ = «1 та 2» = “*2*” (бали); $V_{1126} = V_{1226} = V_{1326} = V_{1426} = V_{1526} = V_{1626}$ = «1 та 3» = “*3*” (бали); $V_{1127} = V_{1227} = V_{1327} = V_{1427} = V_{1527} = V_{1627}$ = «2 та 3» = “*4*” (бали); $V_{1128} = V_{1228} = V_{1328} = V_{1428} = V_{1528}$ = «Ніхто з вище перелічених» = “*5*” (балів); $V_{1131} = V_{1231} = V_{1331} = V_{1431} = V_{1531} = V_{1628} = V_{1631}$ = «Так»; $V_{1132} = V_{1232} = V_{1332} = V_{1432} = V_{1532} = V_{1632}$ = «Ні» = “*0*” (балів) [106].

Визначення рівня захищеності модуля операційної системи хмарного сервісу (ЗМОС)

Етап 6 – визначення рівня захищеності операційної система, що є основою системи віртуалізації та VPC/VDS серверів, що використовуються компаніями-замовниками [106].

Для даного етапу, шляхом перетворення формули (2.44), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP}_6 = \mathbf{OS} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} OS_{jk} \right\} \right\} =$$

$$\begin{gathered} \{\{OS_{11}, OS_{12}, OS_{13}, OS_{14}, OS_{15}\}, \{OS_{21}, OS_{22}\}, \{OS_{31}, OS_{32}\}, \\ \{OS_{41}, OS_{42}\}, \{OS_{51}, OS_{52}\}, \{OS_{61}, OS_{62}\}, \{OS_{71}, OS_{72}\}, \\ \{OS_{81}, OS_{82}\}, \{OS_{91}, OS_{92}\}, \{OS_{101}, OS_{102}\}, \{OS_{111}, OS_{112}\}\} = \\ \{\{"5","3","2","1","0"\}, \{"5","0"\}, \{"5","0"\}, \\ \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\ \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\}, \end{gathered} \tag{2.90}$$

де: OS_{11} = «Замовник» = "*5*" (балів); OS_{12} = «Представники постачальника хмарних послуг» = "*3*" (бали); OS_{13} = «Представники центру обробки даних» = "*2*" (бали); OS_{14} = «Всі з вище перелічених» = "*1*" (бал); OS_{15} = «Жоден з вище перелічених» = "*0*" (балів); OS_{21} = «Так» = "*5*" (балів); OS_{22} = «Ні» = "*0*" (балів); OS_{31} = «Так» = "*5*" (балів); OS_{32} = «Ні» = "*0*" (балів); OS_{41} = «Так» = "*5*" (балів); OS_{42} = «Ні» = "*0*" (балів); OS_{51} = «Так» = "*5*" (балів); OS_{52} = «Ні» = "*0*" (балів); OS_{61} = «Так» = "*5*" (балів); OS_{62} = «Ні» = "*0*" (балів); OS_{71} = «Так» = "*5*" (балів); OS_{72} = «Ні» = "*0*" (балів); OS_{81} = «Так» = "*5*" (балів); OS_{82} = «Ні» = "*0*" (балів); OS_{91} = «Так» = "*5*" (балів); OS_{92} = «Ні» = "*0*" (балів); OS_{101} = «Так» = "*5*" (балів); OS_{102} = «Ні» = "*0*" (балів); OS_{111} = «Так» = "*5*" (балів); OS_{112} = «Ні» = "*0*" (балів) [106].

Аналогічно, перетворивши формулу (2.48), ми отримаємо наступний вигляд другого рівня компоненту [106]:

$$\mathbf{CSP}_6 = \mathbf{OS} = \left\{\bigcup_{j=1}^{11}\left\{\bigcup_{k=1}^{m_{6j}}\left\{\bigcup_{l=1}^{m_{6jk}}\left\{\bigcup_{p=1}^{m_{6jkl}} OS_{jklp}\right\}\right\}\right\}\right\} =$$

$$\begin{gathered}
\{\{OS_{11}, OS_{12}, OS_{13}, OS_{14}, OS_{15},\}, \\
\{\{\{OS_{2111}, OS_{2112}\}\}, OS_{22}\}, \{OS_{31}, OS_{32}\}, \{OS_{41}, OS_{42}\}, \\
\{OS_{51}, OS_{52}\}, \{OS_{61}, OS_{62}\}, \{OS_{71}, OS_{72}\}, \{OS_{81}, OS_{82}\}, \\
\{OS_{91}, OS_{92}\}, \{OS_{101}, OS_{102}\}, \{OS_{111}, OS_{112}\}\} = \\
\{\{"5","3","2","1","0"\}, \{\{\{"5","0"\}\},"0"\}, \{"5","0"\}, \\
\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\
\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\},
\end{gathered} \tag{2.91}$$

де: OS_{2111} = «Так» = “*5*” (балів); OS_{2112} = «Ні» = “*0*” (балів) [106].

Визначення рівня захищеності модуля управління контейнеризацією хмарного сервісу (ЗМУК)

Етап 7 – визначення рівня захищеності системи управління контейнерами та контейнеризацією, що використовується компаніями-замовниками [106].

Для даного етапу, шляхом перетворення формули (2.53), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP}_7 = \mathbf{CT} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{7j}} CT_{jk}\right\}\right\} =$$

$$\begin{gathered}
\{\{CT_{11}, CT_{12}\}, \{CT_{21}, CT_{22}\}, \{CT_{31}, CT_{32}\}, \{CT_{41}, CT_{42}\}, \\
\{CT_{51}, CT_{52}\}, \{CT_{61}, CT_{62}\}, \{CT_{71}, CT_{72}\}, \{CT_{81}, CT_{82}\}, \\
\{CT_{91}, CT_{92}\}, \{CT_{101}, CT_{102}\}\} = \\
\{\{"5","3"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\
\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \\
\{"5","0"\}, \{"5","0"\}\},
\end{gathered} \tag{2.92}$$

де: CT_{11} = «Самостійно встановлювати систему для управління контейнерами» = “*5*” (балів); CT_{12} = «Надає готову платформу для управління та розгортання контейнерів» = “*3*” (бали); CT_{21} = «Так» = “*5*” (балів); CT_{22} = «Ні» = “*0*” (балів); CT_{31} = «Так» = “*5*” (балів); CT_{32} = «Ні» = “*0*” (балів); CT_{41} = «Так» = “*5*” (балів); CT_{42} = «Ні» = “*0*” (балів); CT_{51} = «Так» = “*5*” (балів); CT_{52} = «Ні» = “*0*” (балів); CT_{61} = «Так» = “*5*” (балів); CT_{62} = «Ні» = “*0*” (балів); CT_{71} =

«Так» = “*5*” (балів); CT_{72} = «Ні» = “*0*” (балів); CT_{81} = «Так» = “*5*” (балів); CT_{82} = «Ні» = “*0*” (балів); CT_{91} = «Так» = “*5*” (балів); CT_{92} = «Ні» = “*0*” (балів); CT_{101} = «Так» = “*5*” (балів); CT_{102} = «Ні» = “*0*” (балів) [106].

Визначення рівня захищеності модуля забезпечення безперервної роботи хмарного сервісу (ЗЗБР)

Етап 8 – визначення рівня захищеності засобів хмарного сервісу, що відповідають за забезпечення безперервної роботи розгорнутих сервісів компаній-замовників [106].

Для даного етапу, шляхом перетворення формули (2.58), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP_8} = \mathbf{R} = \left\{ \bigcup_{j=1}^{13} \left\{ \bigcup_{k=1}^{m_{8j}} R_{jk} \right\} \right\} = \tag{2.93}$$

$$\{\{R_{11}, R_{12}\},\{R_{21}, R_{22}\},\{R_{31}, R_{32}\},\{R_{41}, R_{42}\},\{R_{51}, R_{52}\},$$
$$\{R_{61}, R_{62}\},\{R_{71}, R_{72}\},\{R_{81}, R_{82}\},\{R_{91}, R_{92}\},\{R_{101}, R_{102}\},$$
$$\{R_{111}, R_{112}\},\{R_{121}, R_{122}\},\{R_{131}, R_{132}\}\} =$$
$$\{\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},$$
$$\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},$$
$$\{"5","0"\},\{"5","0"\},\{"5","0"\}\},$$

де: R_{11} = «Так» = “*5*” (балів); R_{12} = «Ні» = “*0*” (балів); R_{21} = «Так» = “*5*” (балів); R_{22} = «Ні» = “*0*” (балів); R_{31} = «Так» = “*5*” (балів); R_{32} = «Ні» = “*0*” (балів); R_{41} = «Так» = “*5*” (балів); R_{42} = «Ні» = “*0*” (балів); R_{51} = «Так» = “*5*” (балів); R_{52} = «Ні» = “*0*” (балів); R_{61} = «Так» = “*5*” (балів); R_{62} = «Ні» = “*0*” (балів); R_{71} = «Так» = “*5*” (балів); R_{72} = «Ні» = “*0*” (балів); R_{81} = «Так» = “*5*” (балів); R_{82} = «Ні» = “*0*” (балів); R_{91} = «Так» = “*5*” (балів); R_{92} = «Ні» = “*0*” (балів); R_{101} = «Так» = “*5*” (балів); R_{102} = «Ні» = “*0*” (балів); R_{111} = «Так» = “*5*” (балів); R_{112} = «Ні» = “*0*” (балів); R_{121} = «Так» = “*5*” (балів); R_{122} = «Ні» = “*0*” (балів); R_{131} = «Так» = “*5*” (балів); R_{132} = «Ні» = “*0*” (балів) [106].

Визначення рівня захищеності модуля управління додатками хмарного сервісу (ЗУД)

Етап 9 – визначення рівня захищеності додатків, що підтримуються постачальником хмарного сервісу і надаються компаніям-замовникам лише для проведення налаштувань [106].

Для даного етапу, шляхом перетворення формули (2.63), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP_9} = \mathbf{A} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{9j}} A_{jk} \right\} \right\} = \tag{2.94}$$

$$\{\{A_{11}, A_{12}\}, \{A_{21}, A_{22}\}, \{A_{31}, A_{32}, A_{33}\}, \{A_{41}, A_{42}\}, \{A_{51}, A_{52}\},$$
$$\{A_{61}, A_{62}\}, \{A_{71}, A_{72}\}, \{A_{81}, A_{82}\}, \{A_{91}, A_{92}\}, \{A_{101}, A_{102}\}\} =$$
$$\{\{"5","0"\}, \{"5","0"\}, \{"5","3","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\},$$

де: A_{11} = «Так» = “*5*” (балів); A_{12} = «Ні» = “*0*” (балів); A_{21} = «Так» = “*5*” (балів); A_{22} = «Ні» = “*0*” (балів); A_{31} = «Власний персонал» = “*5*” (балів); A_{32} = «Субпідрядні організації» = “*3*” (бали); A_{33} = «Нікого не залучає» = “*0*” (балів); A_{41} = «Так» = “*5*” (балів); A_{42} = «Ні» = “*0*” (балів); A_{51} = «Так» = “*5*” (балів); A_{52} = «Ні» = “*0*” (балів); A_{61} = «Так» = “*5*” (балів); A_{62} = «Ні» = “*0*” (балів); A_{71} = «Так» = “*5*” (балів); A_{72} = «Ні» = “*0*” (балів); A_{81} = «Так» = “*5*” (балів); A_{82} = «Ні» = “*0*” (балів); A_{91} = «Так» = “*5*” (балів); A_{92} = «Ні» = “*0*” (балів); A_{101} = «Так» = “*5*” (балів); A_{102} = «Ні» = “*0*” (балів) [106].

Визначення рівня захищеності модуля обробки та управління даними хмарного сервісу (ЗОУД)

Етап 10 – визначення рівня захищеності даних компаній-замовників, що циркулюють на ресурсах хмарного провайдера [106].

Для даного етапу, шляхом перетворення формули (2.68), отримаємо наступний вигляд компоненту [106]:

$$\mathbf{CSP_{10}} = \mathbf{D} = \left\{ \bigcup_{j=1}^{12} \left\{ \bigcup_{k=1}^{m_{10j}} D_{jk} \right\} \right\} =$$

$$\{\{D_{11}, D_{12}\}, \{D_{21}, D_{22}\}, \{D_{31}, D_{32}\}, \{D_{41}, D_{42}\}, \{D_{51}, D_{52}\},$$
$$\{D_{61}, D_{62}\}, \{D_{71}, D_{72}\}, \{D_{81}, D_{82}\}, \{D_{91}, D_{92}\}, \{D_{101}, D_{102}\},$$
$$\{D_{111}, D_{112}\}, \{D_{121}, D_{122}\}\} = \quad (2.95)$$
$$\{\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}\},$$

де: D_{11} = «Так» = "*5*" (балів); D_{12} = «Ні» = "*0*" (балів); D_{21} = «Так» = "*5*" (балів); D_{22} = «Ні» = "*0*" (балів); D_{31} = «Так» = "*5*" (балів); D_{32} = «Ні» = "*0*" (балів); D_{41} = «Так» = "*5*" (балів); D_{42} = «Ні» = "*0*" (балів); D_{51} = «Так» = "*5*" (балів); D_{52} = «Ні» = "*0*" (балів); D_{61} = «Так» = "*5*" (балів); D_{62} = «Ні» = "*0*" (балів); D_{71} = «Так» = "*5*" (балів); D_{72} = «Ні» = "*0*" (балів); D_{81} = «Так» = "*5*" (балів); D_{82} = «Ні» = "*0*" (балів); D_{91} = «Так» = "*5*" (балів); D_{92} = «Ні» = "*0*" (балів); D_{101} = «Так» = "*5*" (балів); D_{102} = «Ні» = "*0*" (балів) [106].

Визначення критеріїв для обчислення суми набраних балів на основі відповідей аудитора (КОБ)

Задля того, щоб вірно оцінити важливість кожного із етапів оцінки, скористаємося Табл. 2.2, що містить в собі детальний опис максимально можливої кількості балів по кожному із етапів оцінки [106]:

Таблиця 2.2.

Максимальна кількість балів в розрізі параметрів оцінки

№ п/п	Параметр	Максимальна кількість балів
1	$\boldsymbol{CSP_1 = GP}$	0
2	$\boldsymbol{CSP_2 = N}$	110
3	$\boldsymbol{CSP_3 = S}$	95
4	$\boldsymbol{CSP_4 = SR}$	60
5	$\boldsymbol{CSP_5 = V}$	65

№ п/п	Параметр	Максимальна кількість балів
6	$CSP_6 = OS$	60
7	$CSP_7 = CT$	50
8	$CSP_8 = R$	65
9	$CSP_9 = A$	50
10	$CSP_{10} = D$	60
Загалом:		**615 балів**

Необхідно врахувати, що загальна максимальна кількість балів по всім 10 параметрам в розмірі **615 балів** є максимальним значенням, але не завжди це буде максимальним числом, і буде завжди залежати від типу хмарного сервісів та їх відповідним залежностям від оцінюваних параметрах, описаних в Табл. 2.1. Наприклад [106]:

- для сервісу **IaaS** максимальна кількість балів буде складати: **330 балів**;
- для сервісу **CaaS** – **440 балів**;
- для сервісу **PaaS** – **505 балів**;
- для сервісу **FaaS** – **555 балів**;
- для сервісу **SaaS** – **615 балів**.

Після обрахунку оцінки по всіх відповідях, сума для кожного параметру кортежу буде записана у його власний ідентифікатор CSP_i. Враховуючи вище описану інформацію, для того, щоб обрахувати кількість отриманих балів по результатам оцінки, необхідно додати всі ідентифікатори, де вираз буде мати наступний вигляд [106]:

$$\sum_{i=1}^{10} \mathbf{CSP_i} = \mathbf{CSP_1} + \mathbf{CSP_2} + \mathbf{CSP_3} + \mathbf{CSP_4} + \mathbf{CSP_5} + \mathbf{CSP_6} + \mathbf{CSP_7} + \mathbf{CSP_8} + \mathbf{CSP_9} + \mathbf{CSP_{10}} = \mathbf{GP} + \mathbf{N} + \mathbf{S} + \mathbf{SR} + \mathbf{V} + \mathbf{OS} + \mathbf{CT} + \mathbf{R} + \mathbf{A} + \mathbf{D} \quad (2.96)$$

де: $\mathbf{CSP_i} \subseteq \mathbf{CSP}$ $(i = \overline{1,10})$ – сума всіх обчислених балів, отриманих на основі відповідей аудитора [106].

Щоб обчислити коефіцієнт кількості отриманих балів на основі отриманих відповідей від аудитора, введено нову змінну **CC** (Calculated Coefficient), де формула набуде наступного вигляду [106]:

$$\mathbf{CC} = \frac{\sum_{i=1}^{10} \mathbf{CSP_i}}{< CSP\ type\ selected >} * 100\% \tag{2.97}$$

де: $\sum_{i=1}^{10} \mathbf{CSP_i}$ – сума всіх обчислених балів, отриманих на основі відповідей аудитора, $< CSP\ type\ selected >$ – встановлення максимальної кількості балів залежить від вибраного типу хмарного сервісу (*IaaS=**330**, CaaS=**440**, PaaS=**505**, FaaS=**555**, SaaS=**615***) [106].

Також варто ввести нову змінну **RC** (resulting criterion), що буде визначати який ступінь рекомендації використання хмарного сервісу для розгортання бізнес сервісів компанії. Результатом оцінки даного критерію буде 3 варіанти відповіді аудитору [106]:

- «**Рекомендується до використання (Recommended)**» - хмарний сервісі повністю рекомендується до використання та розгортання бізнес сервісів та додатків компанії. *Застосовується, якщо значення змінної **CC** становить **від 76% до 100%***;
- «**Можливе до використання (Maybe)**» - хмарний сервіс можливо використовувати для розгортання бізнес сервісів та додатків компанії, проте рекомендується переглянути ступінь захищеності використовуваного рішення. *Застосовується, якщо значення змінної **CC** становить **від 26% до 75%***;
- «**Не рекомендується до використання (No Recommended)**» - хмарний сервіс не рекомендується до розгортання бізнес сервісів та додатків компанії, оскільки має низький рівень захищеності, як власної інфраструктури, так і ресурсів, що використовує замовник.

Застосовується, якщо значення змінної ***CC*** *становить* ***від 1% до 25%*** [106].

В розрізі кожного окремого параметру кортежу, вище описані результати оцінки критерію будуть виставлятися у відповідності до Табл. 2.3, а саме [106]:

Таблиця 2.3.

Визначення значення змінної **RC** в розрізі параметрів оцінки

№ п/п	Параметр	*No Recommended*	*Maybe*	*Recommended*
1	$CSP_1 = GP$	*0*	*0*	*0*
2	$CSP_2 = N$	*до* ***28*** *балів*	***29-83*** *балів*	*від* ***84*** *балів*
3	$CSP_3 = S$	*до* ***24*** *балів*	***25-72*** *балів*	*від* ***73*** *балів*
4	$CSP_4 = SR$	*до* ***15*** *балів*	***16-45*** *балів*	*від* ***46*** *балів*
5	$CSP_5 = V$	*до* ***16*** *балів*	***17-49*** *балів*	*від* ***50*** *балів*
6	$CSP_6 = OS$	*до* ***15*** *балів*	***16-45*** *балів*	*від* ***46*** *балів*
7	$CSP_7 = CT$	*до* ***13*** *балів*	***14-38*** *балів*	*від* ***39*** *балів*
8	$CSP_8 = R$	*до* ***16*** *балів*	***17-49*** *балів*	*від* ***50*** *балів*
9	$CSP_9 = A$	*до* ***13*** *балів*	***14-38*** *балів*	*від* ***39*** *балів*
10	$CSP_{10} = D$	*до* ***15*** *балів*	***16-45*** *балів*	*від* ***46*** *балів*

В розрізі кожного окремого типу хмарного сервісу, вище описані результати оцінки критерію будуть виставлятися у відповідності до Табл. 2.4, а саме [106]:

Таблиця 2.4.

Визначення значення змінної **RC** в розрізі типів хмарних сервісів

№ п/п	Параметр	*No Recommended*	*Maybe*	*Recommended*
1	**IaaS**	*до **83** балів*	***84-248** балів*	*від **249** балів*
2	**CaaS**	*до **110** балів*	***111-330** балів*	*від **331** балів*
3	**PaaS**	*до **126** балів*	***127-379** балів*	*від **380** балів*
4	**FaaS**	*до **139** балів*	***140-416** балів*	*від **417** балів*
5	**SaaS**	*до **154** балів*	***155-461** балів*	*від **462** балів*

2.3. Структурна модель системи оцінювання кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури

Для чіткого розуміння роботи та взаємодії всіх параметрів оцінювання моделі та методу, на Рис. 2.2 представлено структурну модель системи оцінювання, на якій описується послідовність виконання операцій та дій в межах розроблених моделі та методу оцінювання [104, 98].

Структурна модель системи оцінювання, представлена на Рис. 2.2 складається з наступних компонентів [104]:

- база даних результатів оцінювання (БДРО);
- база даних загальних запитань (БДЗЗ);
- база даних запитань мережевого модуля (БДЗММ);
- база даних запитань модуля збереження даних (БДЗМЗД);
- база даних запитань серверного модуля (БДЗСМ);
- база даних запитань модуля віртуалізації (БДЗМВ);
- база даних запитань модуля операційної системи (БДЗОС);
- база даних запитань модуля контейнеризації (БДЗМК);
- база даних запитань модуля безперервної роботи (БДЗМБР);
- база даних запитань модуля додатків (БДЗМД);

- база даних запитань модуля обробки даних (БДЗМОД);
- база даних рекомендацій (БДР);
- база даних еталонних значень (БДЕЗ);
- модуль ініціалізації оцінювання (МІО);
- модуль отримання загальних даних (МОЗД);
- модуль оцінки мережі (МОМ);
- модуль оцінки зберігання даних (МОЗіД);
- модуль оцінки серверного обладнання (МОСО);
- модуль оцінки системи віртуалізації (МОСВ)
- модуль оцінки операційної системи (МООС);
- модуль оцінки системи контейнеризації (МОСК);
- модуль оцінки безперервної роботи (МОБР);
- модуль оцінки додатків (МОД);
- модуль оцінки обробки даних (МООД);
- модуль запису результатів оцінювання в базу даних (МЗРОБД);
- модуль візуалізації результатів оцінювання (МВРО) [104].

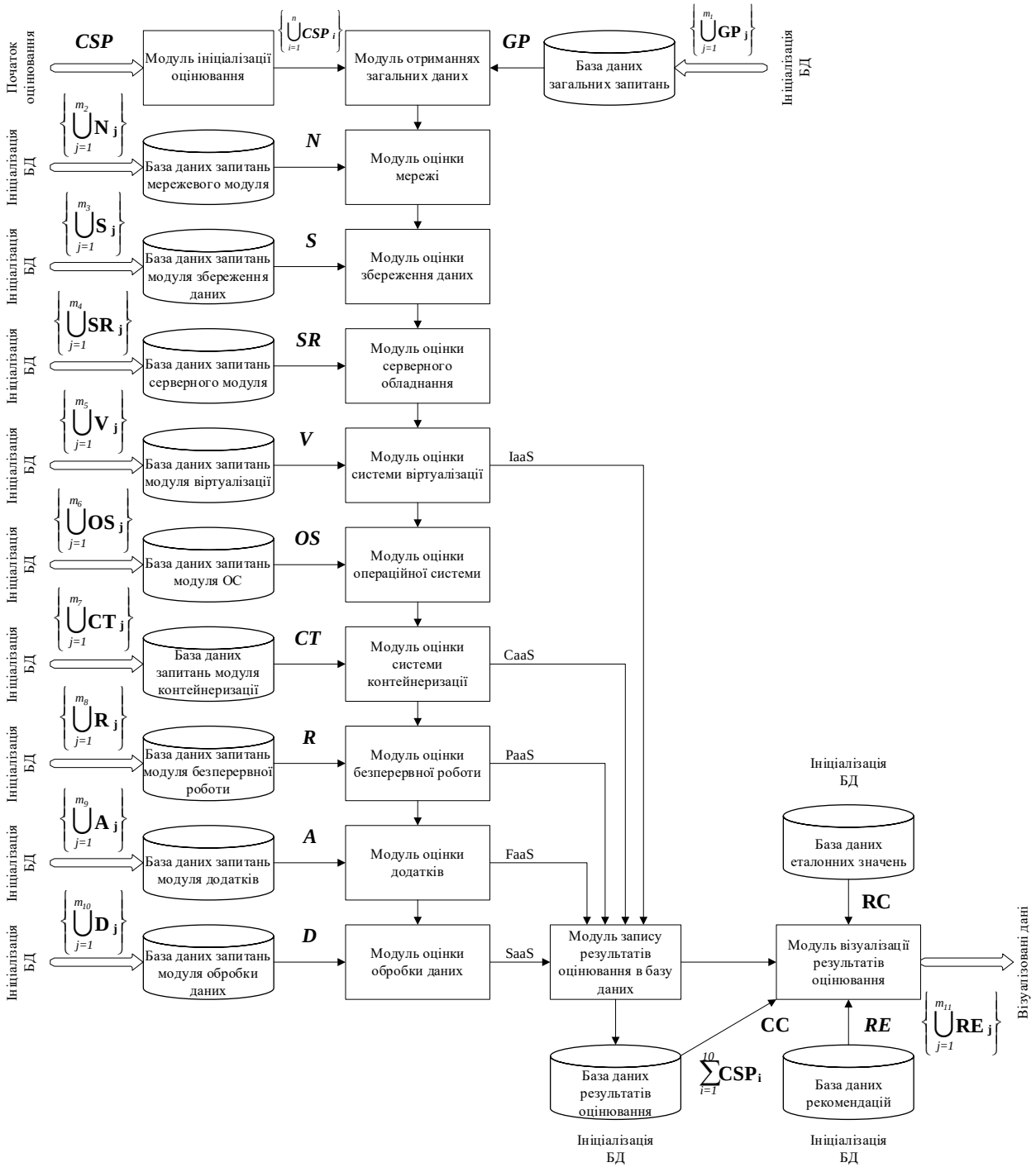


Рис. 2.2. Структурна модель системи оцінювання кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури

Напочатку роботи структурної моделі відбувається запуск модуля МІО, що ініціює запуск нового оцінювання хмарного сервісу, що запускає використання підмножини **CSP** [104, 99].

Після ініціалізації нового оцінювання, запускається модуль МОЗД, що використовує дані параметру **GP** та працює в парі з Базою БДЗЗ, який дозволяє визначити тип оцінюваного хмарного сервісу (IaaS, PaaS, CaasS, FaaS чи SaaS)

та визначити, які з параметрів підмножини CSP будуть задіяні для проведення оцінювання хмарного сервісу [104].

Після визначення типу хмарного сервісу, запускається новий модуль МОМ, що використовує дані параметру **N** та працює з Базою БДЗММ, який дозволяє оцінити стан захищеності мережі, в якій працює хмарний сервіс [104].

Після оцінки стану захищеності мережевого рівня, запускається новий модуль МОЗіД, що використовує дані параметру **S** та працює з Базою БДЗМЗД, який дозволяє оцінити стан захищеності середовища зберігання даних на ресурсах хмарного сервісу [104].

Після оцінки стану захищеності середовища зберігання даних, запускається новий модуль МОСО, що використовує дані параметру **SR** та працює з Базою БДЗСМ, який дозволяє оцінити стан захищеності середовища фізичного розташування серверного обладнання, що використовується для забезпечення роботи хмарного сервісу [104].

Після оцінки стану захищеності середовища фізичного розташування серверного обладнання, запускається новий модуль МОСВ, що використовує дані параметру **V** та працює з Базою БДЗМВ, який дозволяє оцінити стан захищеності середовища віртуалізації, що забезпечує роботу для VPC/VDS серверів хмарного сервісу [104].

Після оцінки стану захищеності середовища віртуалізації, запускається новий модуль МООС, що використовує дані параметру **OS** та працює з Базою БДЗОС, який дозволяє оцінити стан захищеності підтримуваної операційної системи, що пропонується до використання замовникам на базі хмарного сервісу [104].

Після оцінки стану захищеності операційної системи, запускається новий модуль МОСК, що використовує дані параметру **CT** та працює з Базою БДЗМК, який дозволяє оцінити стан захищеності середовища розгортання контейнерів [104].

Після оцінки стану захищеності середовища контейнеризації, запускається новий модуль МОБР, що використовує дані параметру **R** та працює з Базою БДЗМБР, який дозволяє оцінити стан захищеності безперебійної роботи всіх компонентів хмарного сервісу для надання сервісу замовникам [104].

Після оцінки стану захищеності середовища безперервної роботи, запускається новий модуль МОД, що використовує дані параметру **A** та працює з Базою БДЗМД, який дозволяє оцінити стан захищеності пропонованого хмарного застосунку на базі хмарного сервісу [104].

Після оцінки стану захищеності хмарного застосунку, запускається новий модуль МООД, що використовує дані параметру **D** та працює з Базою БДЗМОД, який дозволяє оцінити стан захищеності середовища обробки даних на ресурсах хмарного сервісу [104].

Після завершення опрацювання всіх вище описаних параметрів оцінки стану захищеності хмарного сервісу, запускається новий модуль МЗРОБД, що забезпечує обчислення отриманих результатів оцінювання та запис результатів в Базу БДРО [104].

Перед початком оцінювання визначається тип хмарного сервісу та кількість максимально можливих балів та за результатами знаходження суми всіх балів, запускається етап обчислення коефіцієнту **CC** [104].

На останньому етапі оцінювання, використовується новий параметр оцінювання **RC**, що визначає набір рекомендацій перед початком використання хмарного сервісу для розгортання бізнес додатків на ресурсах хмарного сервісу [104].

Після запису результатів оцінювання в базу БДРО, запускається новий модуль МВРО, для якого дані беруться з баз даних: БДРО, БДР та БДЕЗ, - та надає комплексний звіт за результатами проведеного оцінювання хмарного сервісу типу SaaS (або інші), та надає рекомендації щодо можливості використання оцінюваного хмарного сервісу та, за необхідності, рекомендації, щодо покращення стану захищеності оцінюваних сервісів з метою

покращення рівня захищеності всіх програмних засобів, що плануються до розгортання компаніями замовниками [104].

Висновок до розділу 2

Розроблена модель оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, за рахунок таких модулів оцінювання, як: «General Points», «Network», «Storage», «Server», «Virtualization», «Operation System», «Container Technology», «Runtime», «Application», «Data» та «Requirements», - надала змогу структурувати, формалізувати та розширити визначені параметри оцінювання поточного стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, за результатами якої відкрилася можливість розробити метод оцінювання.

Розроблений метод оцінювання, що базується на теоретико-множинному підході розробленого методу оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури надав змогу для модулів та параметрів оцінювання стандартизувати бальну модель (від 0 до 5 балів), що залежить від критеріїв оцінювання, що прописані для кожного параметру оцінювання. Результатом виконання моделі оцінювання, є надання аудитору отриманої кількості балів, а також присвоєння оцінюваному хмарному сервісу, одного із трьох висновків: «Not Recommended», «Maybe» та «Recommended».

На основі розробленої моделі та методу, розроблено структурну модель системи оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури, що надає змогу побудувати логічну послідовність роботи розробленого методу дослідження, розпочинаючи із початкового етапу оцінювання, продовжуючи вибором типу хмарного сервісу, і завершуючи формуванням звіту по проведеній оцінці, а також надання рекомендацій щодо покращення захищеності оцінюваного хмарного сервісу.

РОЗДІЛ 3. АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕНЯ ЗАХИЩЕНОГО МЕРЕЖЕВОГО ЗАСТОСУНКУ ОЦІНЮВАННЯ КІБЕРЗАХИСТУ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

3.1. Алгоритмічне програмне забезпечення оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури

Захищений мережевий застосунок оцінювання кіберзахищеності хмарних сервісів розроблений на базі проведеного дослідження методів захищеності провайдерів хмарних сервісів. На базі проведеної оцінки, було розроблено загальний вигляд системи оцінювання захищеності хмарних сервісів, що будуть використані компаніями для оцінки провайдера хмарного сервісу, перед розгортанням на його ресурсах власні бізнес додатки та сервіси, від працездатності яких залежить функціонування діяльності компанії. Для візуального схематичного представлення роботи мережевого застосунку, було розроблено покрокову схему роботи, що представлена на Рисунку 3.1. На даному рисунку описана наступна послідовність:

1) Аудитор відкриває браузер, переходить на адресу мережевого застосунку та вводить власні облікові дані.
2) Проводиться перевірка облікових даних аудитора зі збереженими хеш-сумами облікових даних в базі даних застосунку, і у випадку правильного введення облікових даних, аудитору присвоюється одноразовий токен входу, що діє тільки в рамках однієї сесії, в результаті чого, аудитор отримує доступ до застосунку.
3) Отримавши доступ до веб-консолі мережевого застосунку, аудитор має змогу, як переглянути вже наявні оцінювання, так і провести нову оцінку по дев'яти основних модулям оцінювання хмарного сервісу, що описані в попередньому розділі.

4) Результати оцінювання та всі відповіді записуються в базу даних мережевого застосунку, які можна буде як повторно переглянути, так і сформувати за ними фінальний звіт.
5) Аудитор може сформувати звіт за результатами проведеного оцінювання, що буде включати в себе надання деталей, щодо кожного оцінюваного модуля/параметру оцінки хмарного сервісу, та загальну кількість отриманих балів, що буде мати рекомендації, щодо подальшого використання хмарного сервісу. Також у готовому звіті, аудитор зможе знайти рекомендації по всім запитанням, на які аудитором було надані відповіді, що будуть описувати яким чином краще застосувати той чи інший функціонал сервісу, а також чим можна замінити відсутність описаного функціоналу хмарного сервісу.

Рис. 3.1. Схематичне представлення роботи мережевого застосунку оцінювання кіберзахищеності хмарних сервісів

Для надання повної інформації по кожному із описаних модулів на Рис. 3.1. та розробленої структурної моделі оцінювання стану кіберзахисту хмарних сервісів в п.2.3 Розділу 2, було розроблено алгоритмічне представлення роботи захищеного мережевого застосунку оцінювання кіберзахищеності хмарних сервісів. На Рис. 3.2. зображено загальну послідовність дій, що описує роботу вастосунку та дозволяє аудитору якісно провести оцінювання хмарного сервісу. Підпроцес «Авторизація аудитора» описує, яким чином відбувається авторизація аудитора на веб-консолі.

Підпроцес «Проведення нової оцінки» описує дії, що виконуються, коли аудитор проводить оцінювання вибраного хмарного сервісу. Процес «Вибір проведено оцінки» вказує тільки на те, що аудитор вибирає вже готову оцінку та може, як переглянути загальну інформацію, сформувати звіт чи видалити оцінку. Підпроцес «Формування звіту» включає в себе формування відповідних запитів до бази даних, що містить результати оцінювання, де буде обчислено отримані бали по всіх параметрах оцінки, загальну рекомендацію та повноцінні рекомендації по всіх запитаннях, на які аудитором було надані відповіді.

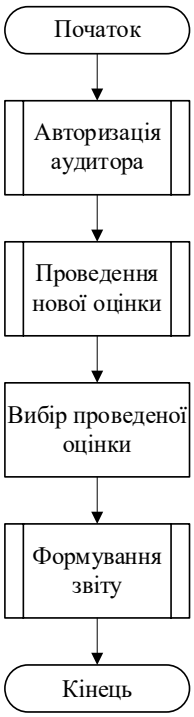


Рис. 3.2. Алгоритм послідовного виконання ключових пунктів захищеного мережевого застосунку оцінювання кібрезахищеності хмарних сервісів

Відповідно до вказаного підпроцесу «Авторизація аудитора» на Рис. 3.2., зобразимо на Рис. 3.3. детальну послідовність проведення авторизації аудитора на консолі управління мережевого застосунку. Дана послідовність включає в себе отримання від аудитора логіну та паролю, формування сесійного токену, та формування єдиного токену для входу до застосунку. Варто зауважити, що при даній перевірці – прямі запити до бази даних зі сторони аудитора повністю відсутні, оскільки перевірка легітимності

підключення відбувається у відповідності до порівняльної перевірки логіну та паролю аудитора на сервері застосунку.

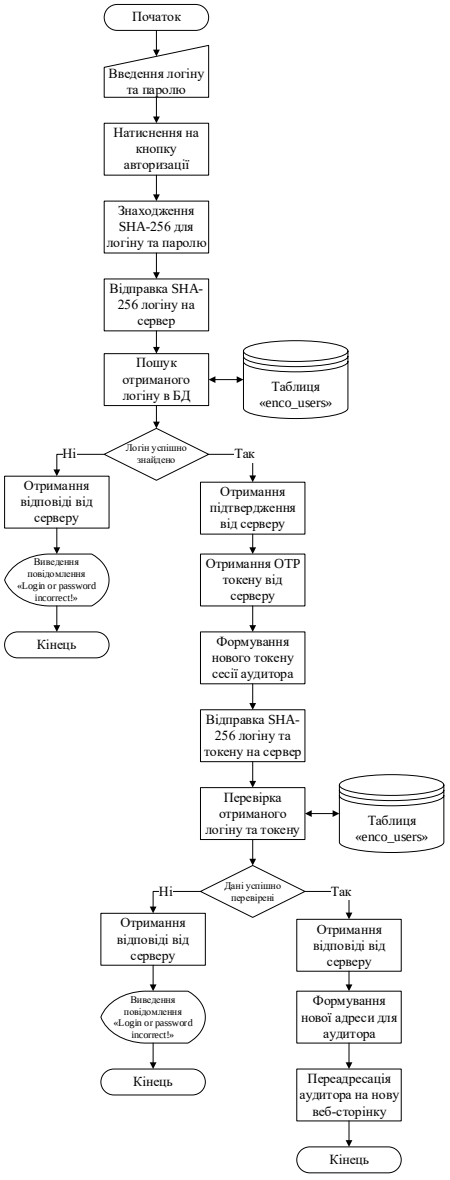


Рис. 3.3. Процес проведення авторизації аудитора на мережевому застосунку оцінювання кіберзахищеності хмарних сервісів

Відповідно до вказаного підпроцесу «Проведення нової оцінки» на Рис. 3.2., зобразимо на Рис. 3.4. детальну послідовність проведення оцінювання вибраного хмарного сервісу аудитором. Як можна бачити, на рисунку зображена послідовність введення загальних відомостей про оцінюваний хмарний застосунок із вибором типу хмарного сервісу, його назви та роботи на окупованих територіях.

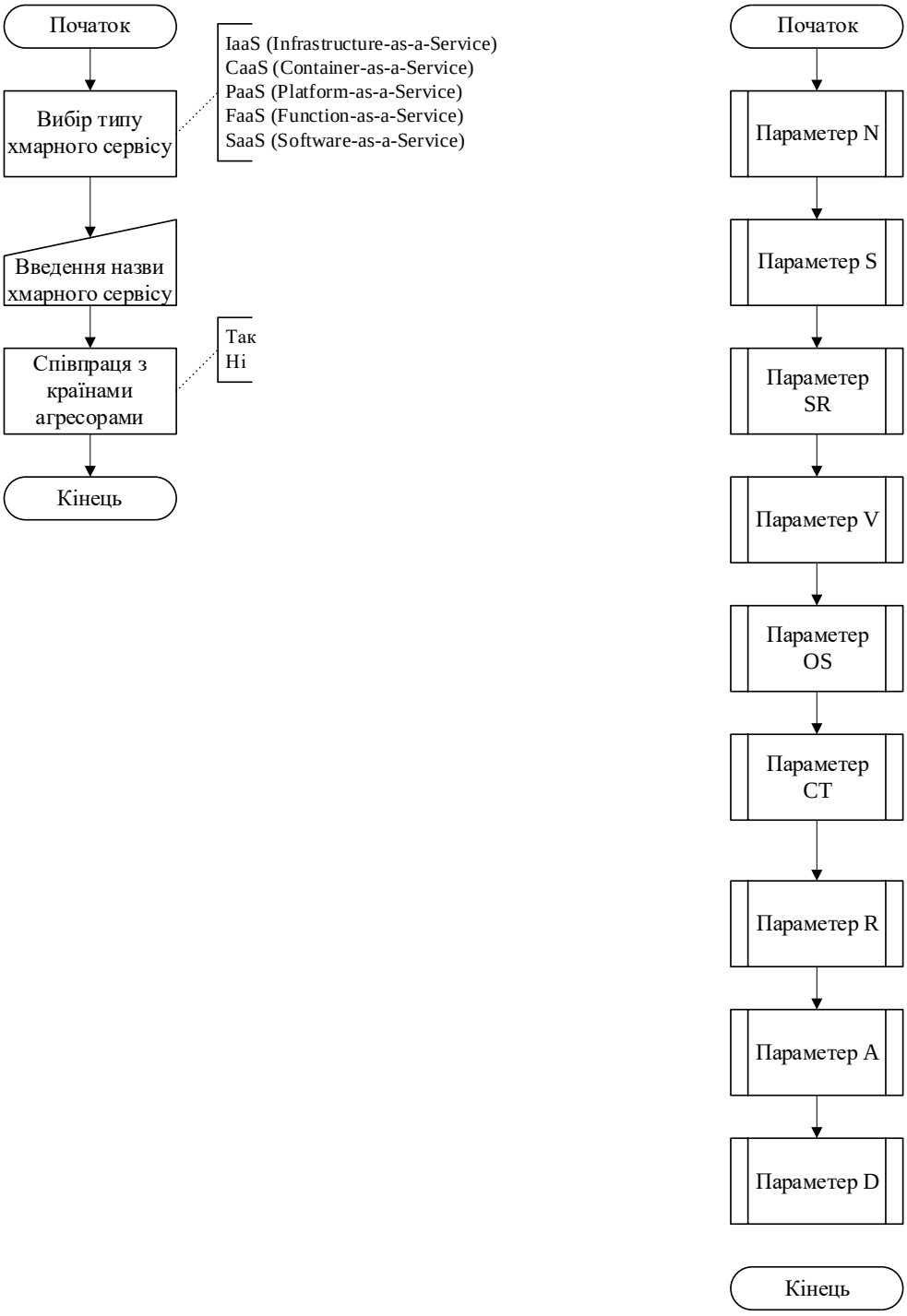


Рис. 3.4. Представлення виконання перших кроків перед початком оцінювання кіберзахищеності хмарного сервісу

Відповідно до Рис. 3.4. видно, що оцінювання кіберзахищеності хмарного сервісу складається із 9 основних пунктів. Для чіткого представлення виконання кожного із 9-ти пунктів, на Рис. 3.5. представлено виконання оцінювання Параметру N, що включає в себе всі питання та відповіді, а також залежності, що забезпечують якісним оцінювання мережевого модуля хмарного сервісу. Інші 8-м пунктів (параметрів) оцінювання будуть

представлені в Додатку А, оскільки вони будуть подібними до пункту, представленого на Рис. 3.5.

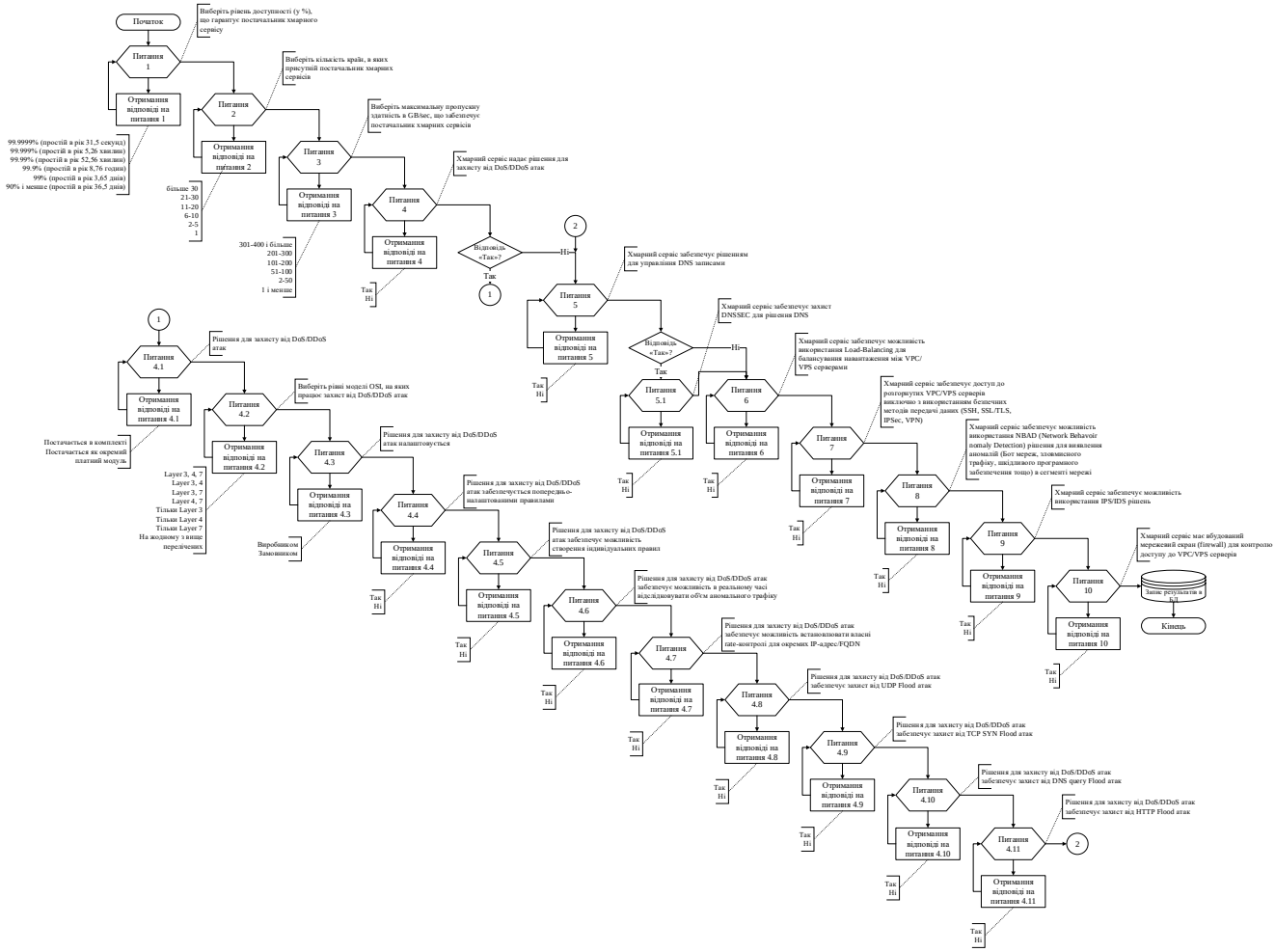


Рис. 3.5. Топологія «Параметру N» для оцінювання мережевого модуля хмарного сервісу розробленим захищеним мережевим застосунком

Також, відповідно до Рис. 3.2. видно, що крок «Формування звіту» також є підроцесом, тому на Рис. 3.6. представлено покрокове формування звіту відображення його на веб-сторінці з метою візуалізувати результати проведеного оцінювання кіберзахищеності хмарного сервісу та надання рекомендацій щодо подальшого використання/невикористання хмарного сервісу.

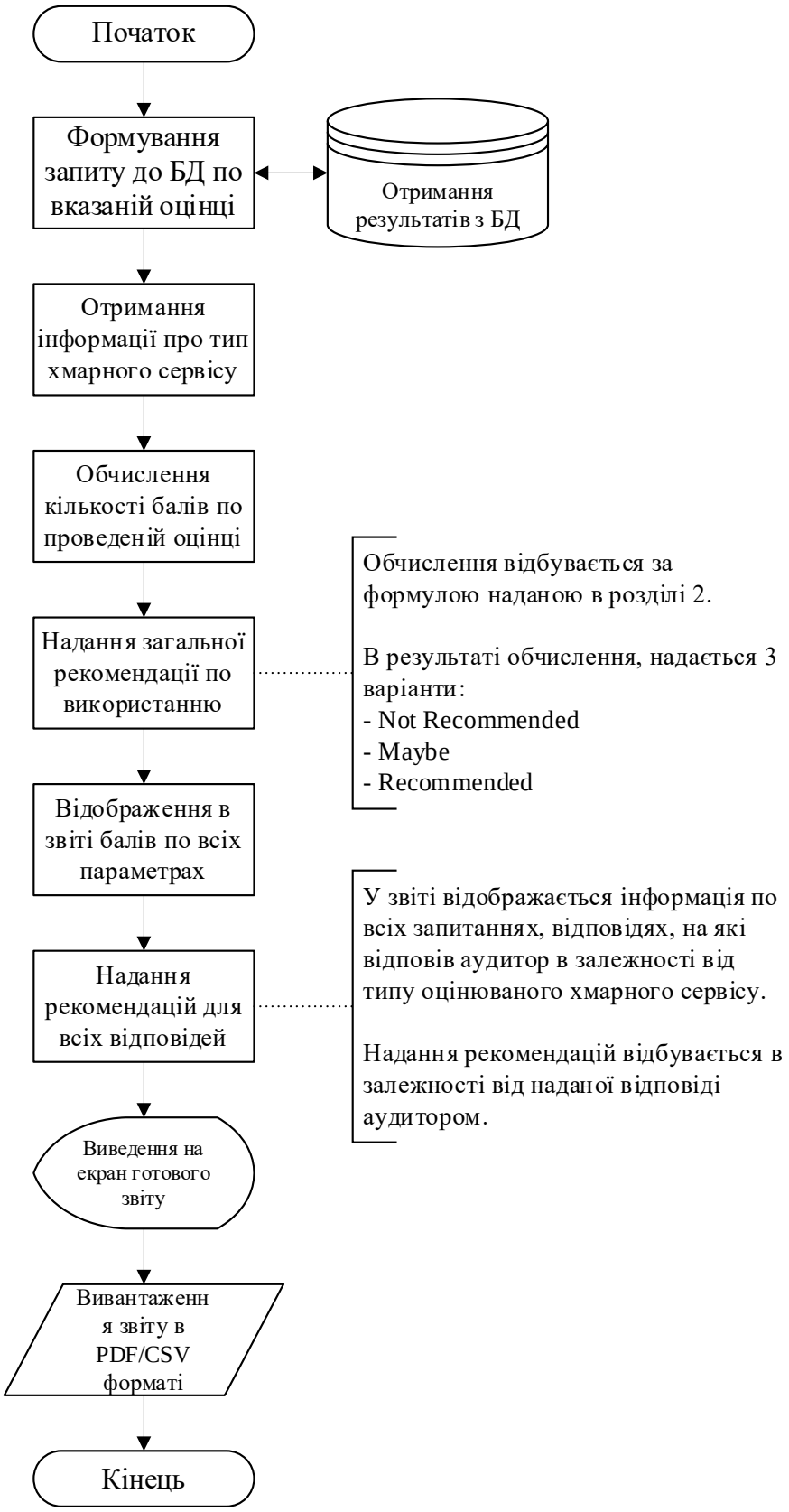


Рис. 3.6. Процес формування звіту за результатами проведеного оцінювання кіберзахищеності хмарного сервісу

Продовження опису алгоритмічного програмного забезпечення оцінювання стану кіберзахисту хмарних сервісів див. додаток А.

На основі вище описаної розробки, моделі, методу та структурної моделі оцінювання кіберзахищеності хмарних сервісів відкривається можливість для аудиторів проведення повноцінної оцінки кіберзахищеності хмарних сервісів від витоку даних, їх захищеності, пропускної здатності мережі, відмовостійкості сервісів тощо. Завдяки даній розробці, аудитор та бізнес отримують наступні переваги щодо використання запропонованої розробки:

- використання 11 етапів оцінювання хмарних сервісів, що включають в себе всі рівні роботи провайдерів та пропонованими ними сервісів;
- використання більше 120 варіантів питань, які налічують більше 350 варіантів відповідей та для яких запропоновано більше 350 різноманітних варіантів рекомендацій щодо покращення кіберзахищеності хмарних сервісів;
- оцінка 5 різних типів хмарних сервісів: IaaS, PaaS, CaaS, FaaS та SaaS;
- використання зручного та інтуїтивно-простого веб-інтерфейсу із можливістю, як проведення нового оцінювання, так і управління всіма проведеними оцінюваннями;
- надання узагальненої інформації, про кількість набраних балів та статус рекомендації за результатами проведеного оцінювання;
- можливість отримання деталізованого звіту по кожному завершеному оцінюванню із детальним описом по кожному із оцінюваних параметрів та отриманням рекомендацій для кожної відповіді аудитора;
- можливість використання світлої або темної теми інтерфейсу.

3.2. Методика проведення експерименту

Експериментальне дослідження розробленого захищеного мережевого застосунку оцінювання кіберзахищеності хмарних сервісів проводиться з метою якісної та кількісної перевірки функціональних можливостей розроблених моделі, методу, системи та програмного застосунку задля оцінки існуючого хмарного сервісу, отримання підтвердження/непідтвердження щодо використання даного хмарного сервісу, а також отримання

рекомендацій, щодо покращення кіберзахищеності вибраного хмарного сервісу.

Для повноцінної та точної представлення коректності функціонування всіх модулів розробленого мережевого застосунку, буде надано результати одого експеримент. При проведенні даного експерименту було вибрано найпопулярніший на сьогоднішній день хмарний сервіс, якому довіряють компанії зі всього світу.

Розпочинаючи роботу із мережевим застосунком – аудитору необхідно авторизуватися на порталі Enco Console та отримати доступ до платформи оцінювання хмарних сервісів, перегляду існуючих оцінок, їх управління чи створення звіту за результатами проведеного оцінювання.

Після авторизації аудитора в мережевому застосунку, необхідно вибрати вкладку “Assessment”, щоб отримати доступ саме до модуля оцінювання кіберзахищеності хмарних сервісів. На даній вкладці аудитор буде мати змогу переглянути вже проведені оцінювання, де вказано буде назви хмарних рішень, їх оцінку та рекомендацію. Також, аудитор буде мати змогу, розпочати нове оцінювання, отримати детальну інформацію про проведену оцінку, згенерувати звіт за результатами оцінювання хмарного сервісу та отримає можливість видалити проведену оцінку.

При натисненні на кнопку початку нового оцінювання хмарного сервісу, аудитору необхідно вибрати один із п’яти типів хмарного сервісу, вказати назву оцінюваного хмарного сервісу та вказати, чи працює даний провайдер на окупованих територіях та країн-терористів.

Після внесення загальної інформації, щодо оцінюваного хмарного сервісу, аудитор отримує доступ до запитань, що згруповані між дев’яти параметрів від N до D. Під час проведення оцінювання, аудитор буде бачити, як змінюється кількість набраних балів по кожному параметру у вигляді графіку. Після проведення оцінювання, всі відповіді будуть збережені в базу даних додатку, результати яких будуть використані для формування фінального звіту.

Після проведення оцінювання, аудитору пропонується відразу згенерувати звіт по проведеній оцінці або повернутися на сторінку зі всіма оцінками. Після переходу на сторінку генерації звіту, аудитору надається звіт у вигляді HTML сторінки, в рамках якої у першому блоку, аудитор бачить загальну інформації по оцінці, а також графічне представлення отриманої кількості балів, як загальної, так і по кожному із оцінюваних параметрів. У другому блоці аудитор має змогу побачити свої відповіді на запитання та рекомендації, щодо покращення кіберзахищеності оцінюваного хмарного сервісу.

3.3. Експериментальне дослідження програмного застосунку оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури

Під час залучення відповідальної особи від компанії чи аудитора до проведення експериментального дослідження розробленого захищеного мережевого застосунку оцінювання кіберзахищеності хмарних сервісів, буде перевірено функціональні можливості рішення. Для перевірки буде використано хмарний сервіс під назвою Amazon Web Services та тип SaaS.

Для початку роботи з мережевим застосунком та початком проведення оцінювання кіберзахищеності хмарного сервісу, аудитор має ввести власні облікові дані для проведення автентифікації користувача (Рис. 3.7.) [105]:

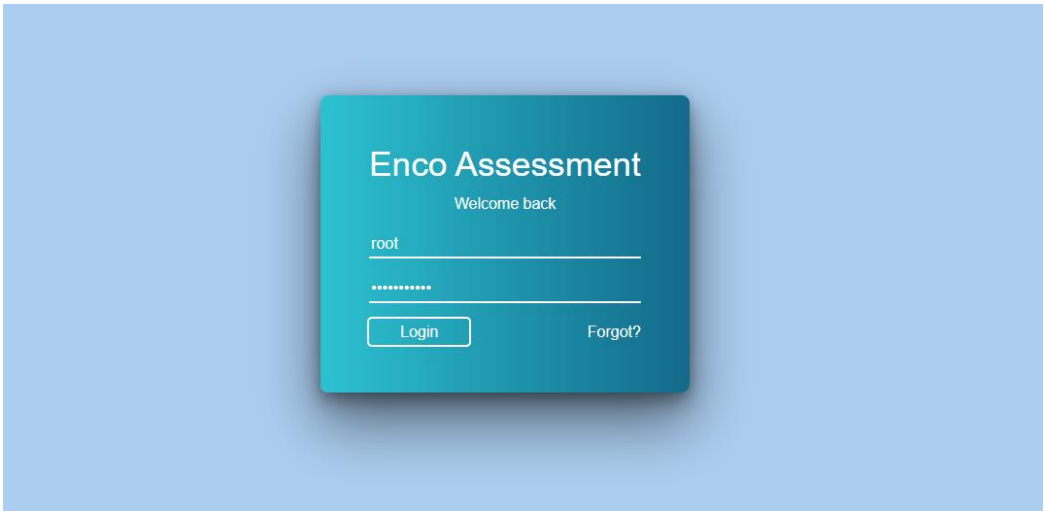


Рис. 3.7. Проведення автентифікації аудитора на веб-консолі мережевого застосунку

Після успішної автентифікації, аудитор має перейти на вкладку Assessment, де аудитору будуть доступні для перегляду вже існуючі проведені оцінювання хмарних сервісів. З даної веб сторінки, аудитор має змогу провести нове оцінювання (Рис. 3.10.), ознайомитися наявними оцінками, отримати детальну інформацію про проведене оцінювання (Рис. 3.11. та Рис. 3.12.), згенерувати звіт по проведеній оцінці (Рис. 3.13.) чи видалити її (Рис. 3.14.). Представлена сторінка доступна в світлій та темній темі (Рис.3.8. та Рис. 3.9.):

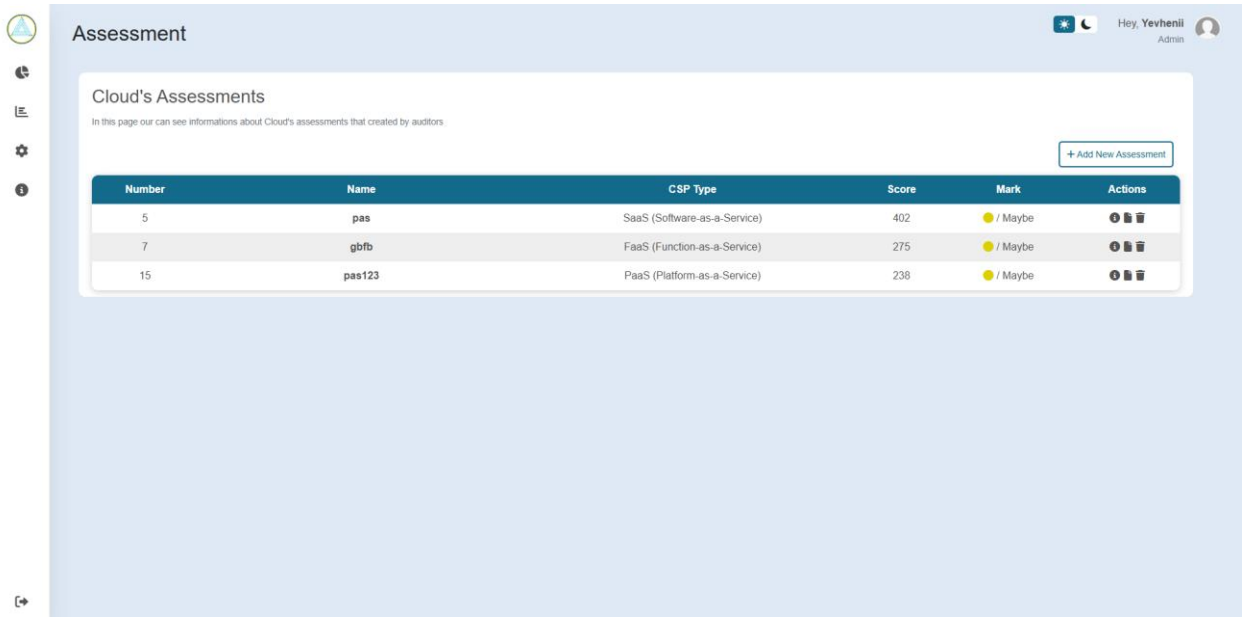


Рис. 3.8. Сторінка представлення проведених оцінок аудитором у світлій темі

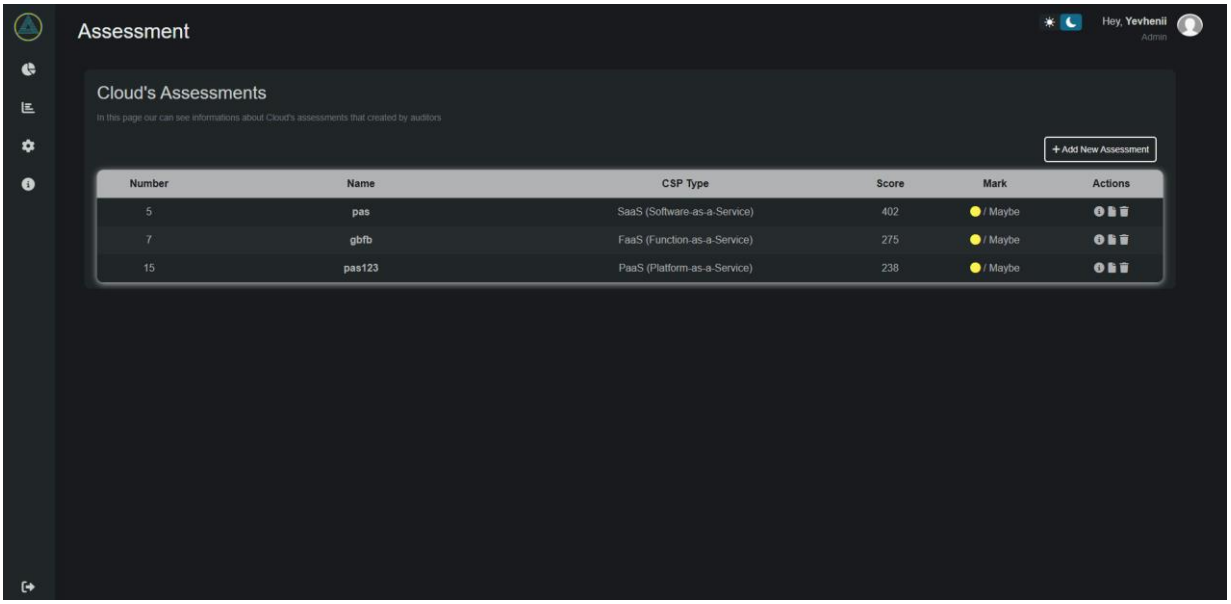


Рис. 3.9. Сторінка представлення проведених оцінок аудитором у темній темі

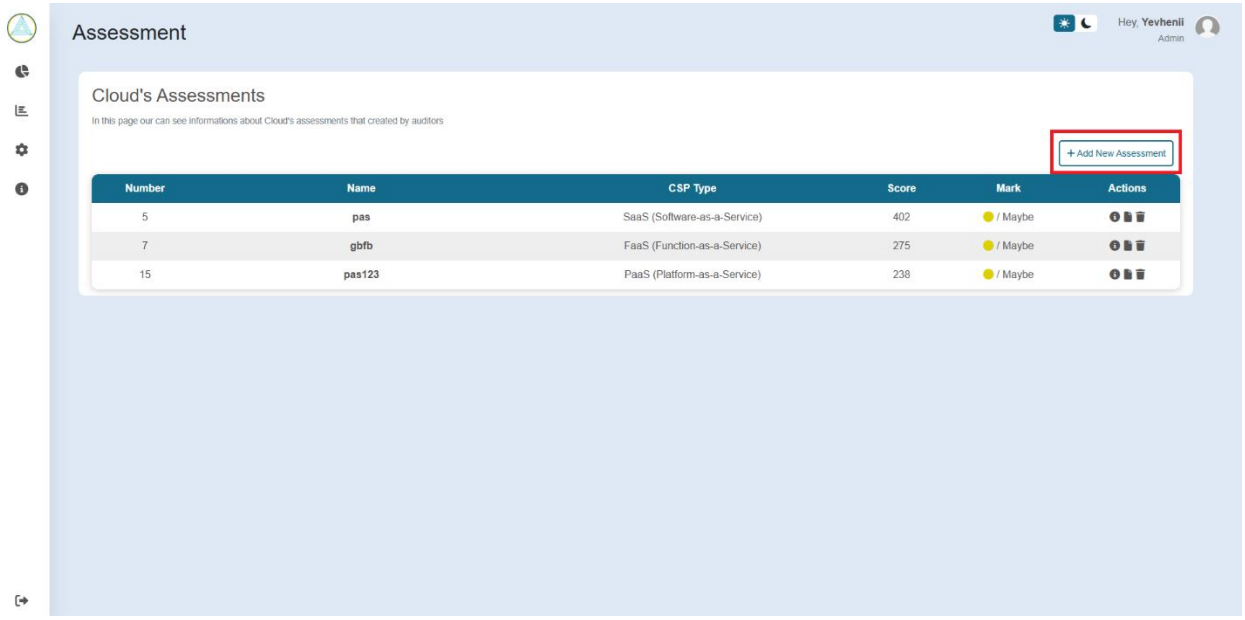


Рис. 3.10. Кнопка «+ Add New Assessment» відповідає за початок нової оцінки хмарного сервісу

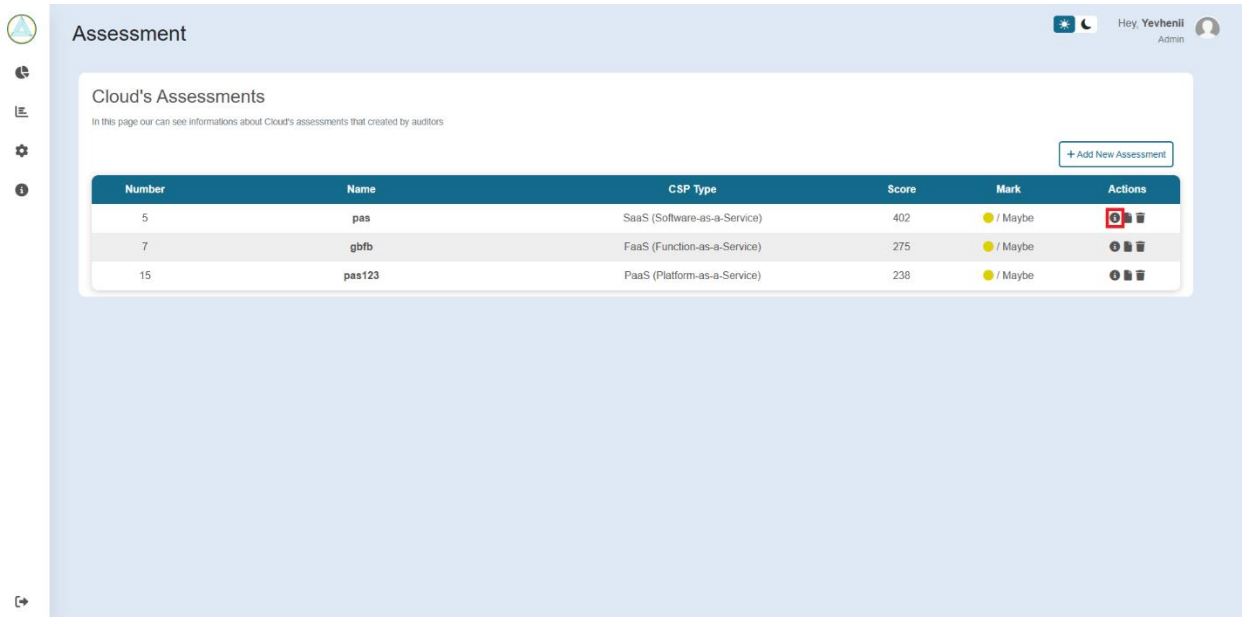


Рис. 3.11. Кнопка відповідає за отримання детальної інформації, щодо проведеної оцінки

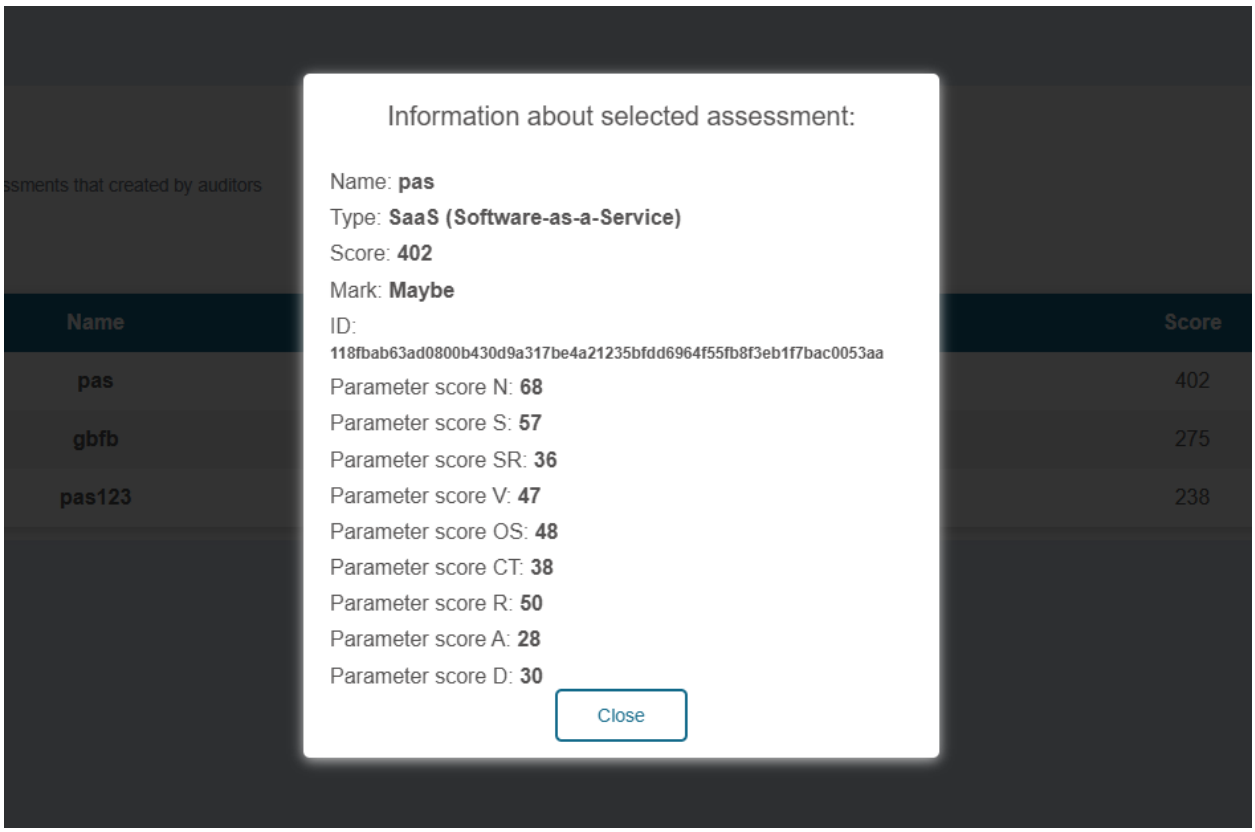


Рис. 3.12. Представлення детальної інформації, щодо проведеної оцінки

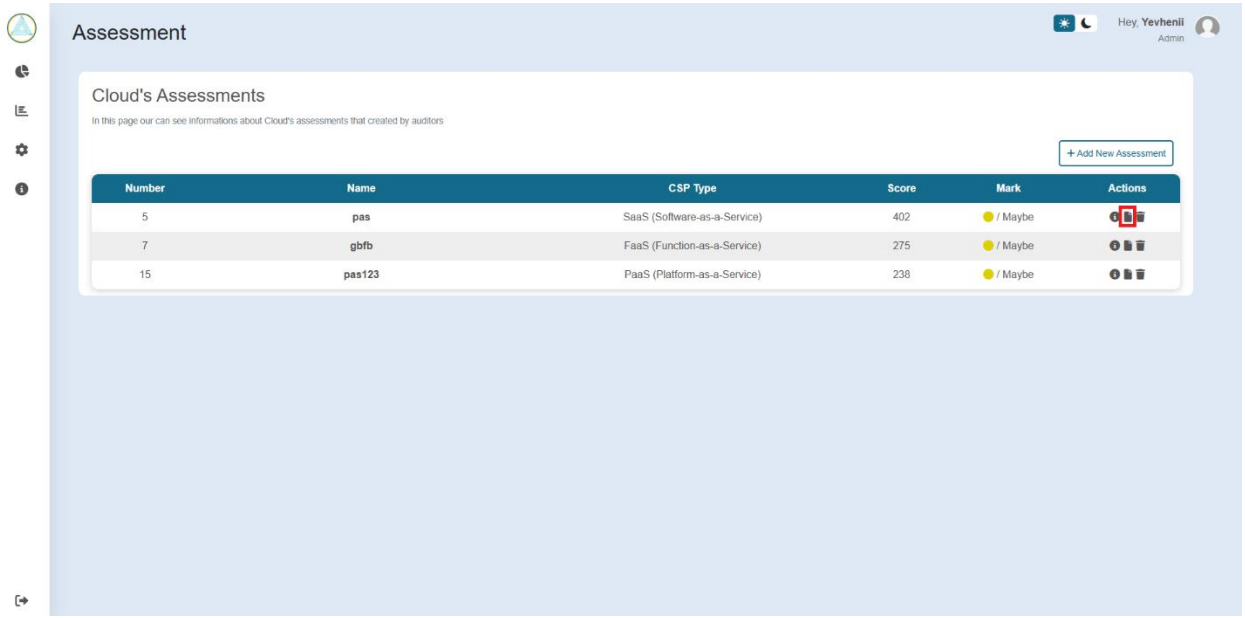


Рис. 3.13. Кнопка відповідає за формування звіту по проведеному оцінюванні хмарного сервісу

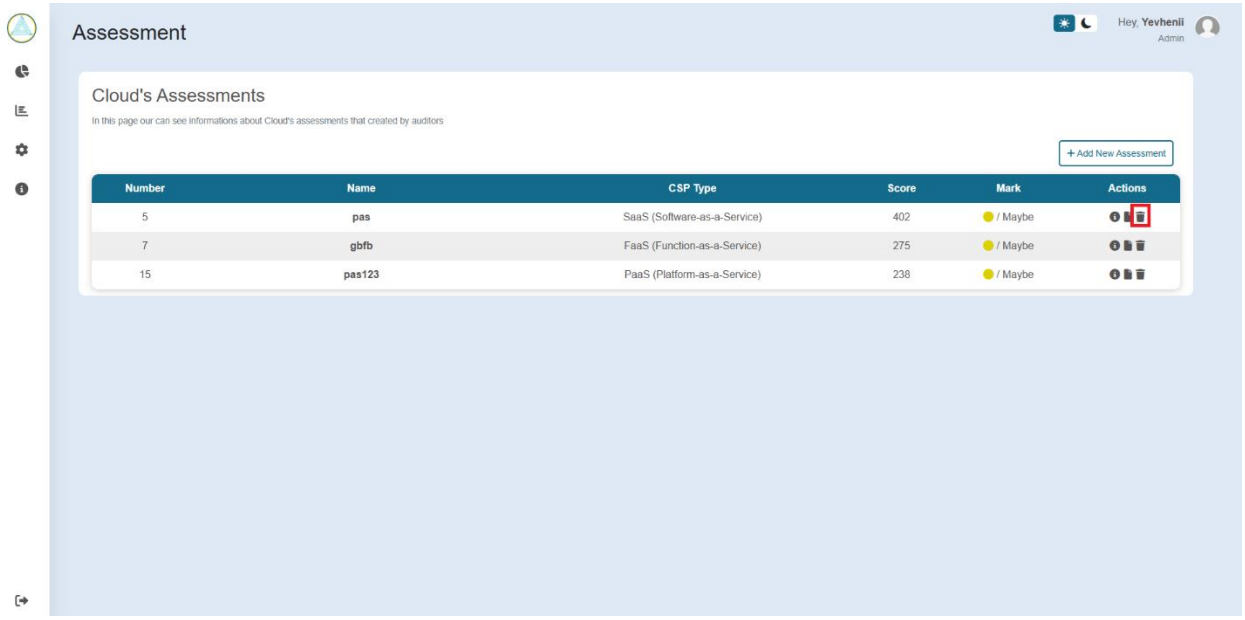


Рис. 3.14. Кнопка відповідає за видалення вибраної оцінки

Після натиснення аудитором кнопки «+ Add New Assessment», аудитор переходить на сторінку введення загальної інформації про оцінюваний хмарний сервіс, із наданням повної інформації, щодо типу, назви та співпраці хмарного сервісу з країнами агресорами і на окупованих територіях (Рис. 3.15.):

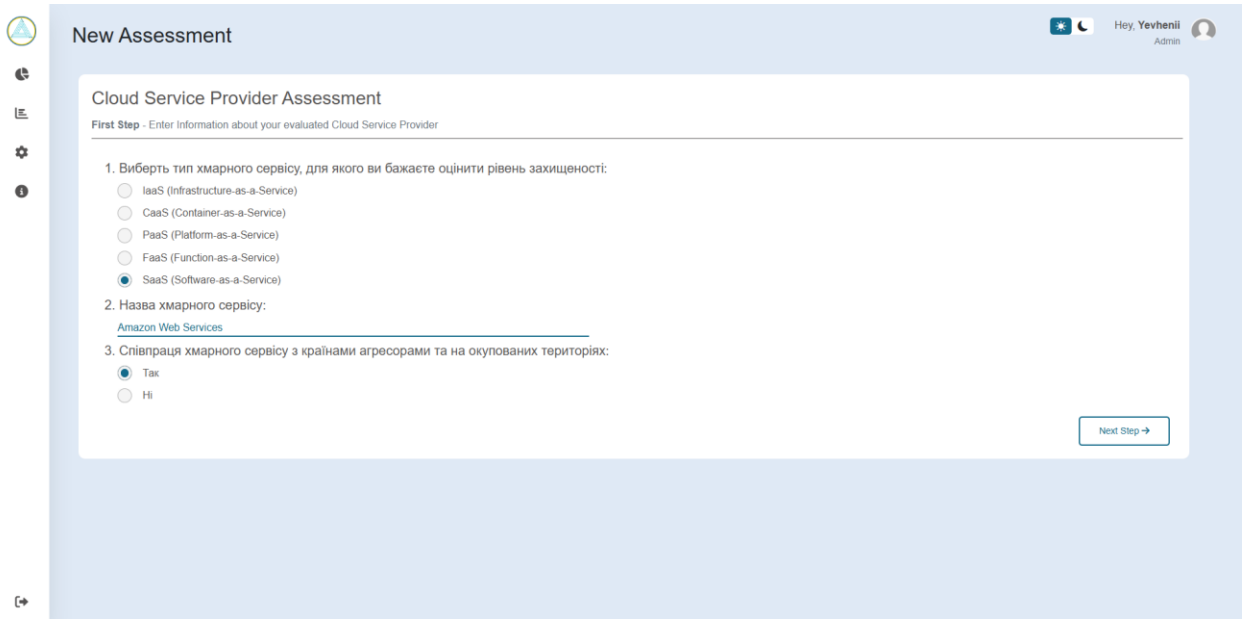


Рис. 3.15. Введення загальної інформації про оцінюваний хмарний сервіс

Після введення загальної інформації, аудитор потрапляє на сторінку оцінювання по параметру «Network Module», де аудитору необхідно надати інформацію, щодо мережевої частини оцінюваного хмарного сервісу, в межах

якого буде оцінюватися здатність постачальника працювати в незалежності від навантаження, розгалуження по світу тощо (Рис. 3.16.):

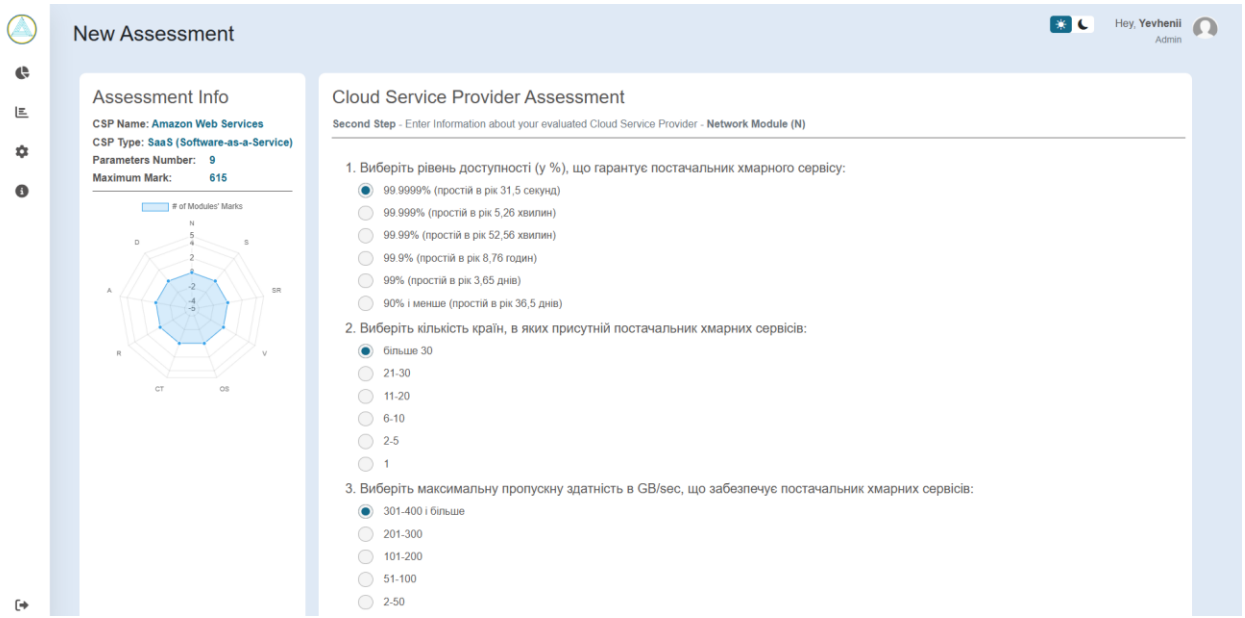


Рис. 3.16. Оцінювання мережевої частини хмарного сервісу

Після оцінювання мережевої частини, аудитор потрапляє на сторінку оцінювання по параметру «Storage Module», де аудитору необхідно надати інформацію, щодо середовища зберігання даних, VPC/VDS серверів, можливості швидкого відновлення через використання реплікації даних тощо (Рис. 3.17.):

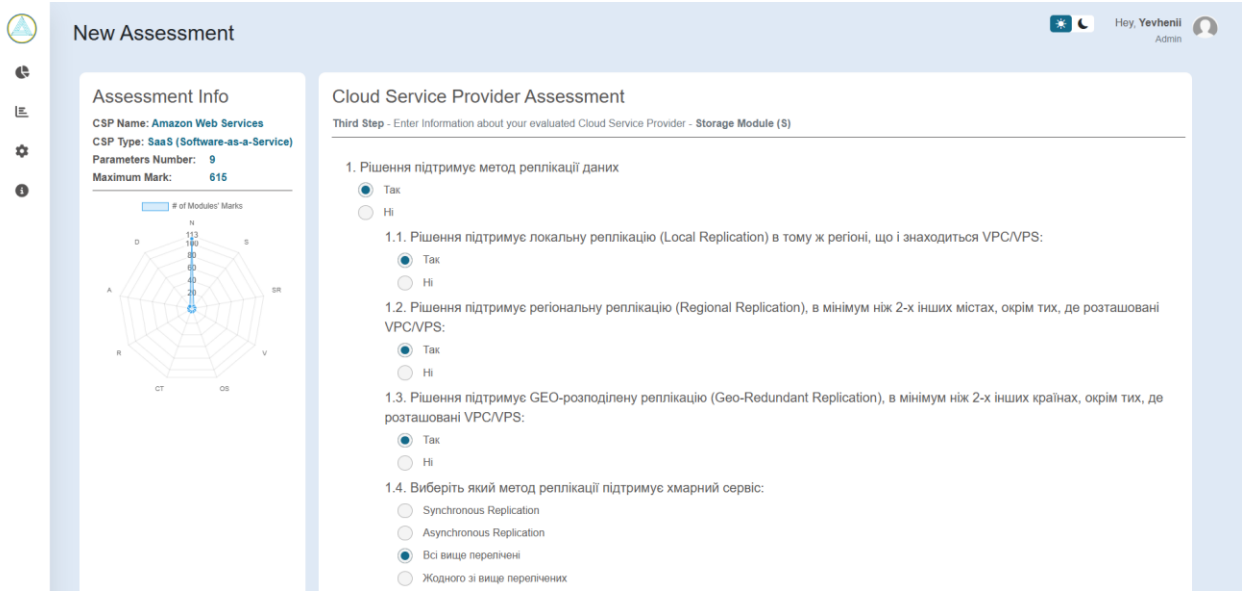


Рис. 3.17. Оцінювання середовища зберігання даних хмарного сервісу

Після оцінювання середовища зберігання даних, аудитор потрапляє на сторінку оцінювання по параметру «Servers Module», де аудитору необхідно

надати інформацію, щодо серверної частини, де вказується інформація щодо захищеності ЦОДів провайдера, наявність безперебійного живлення, протипожежної безпеки тощо (Рис. 3.18.):

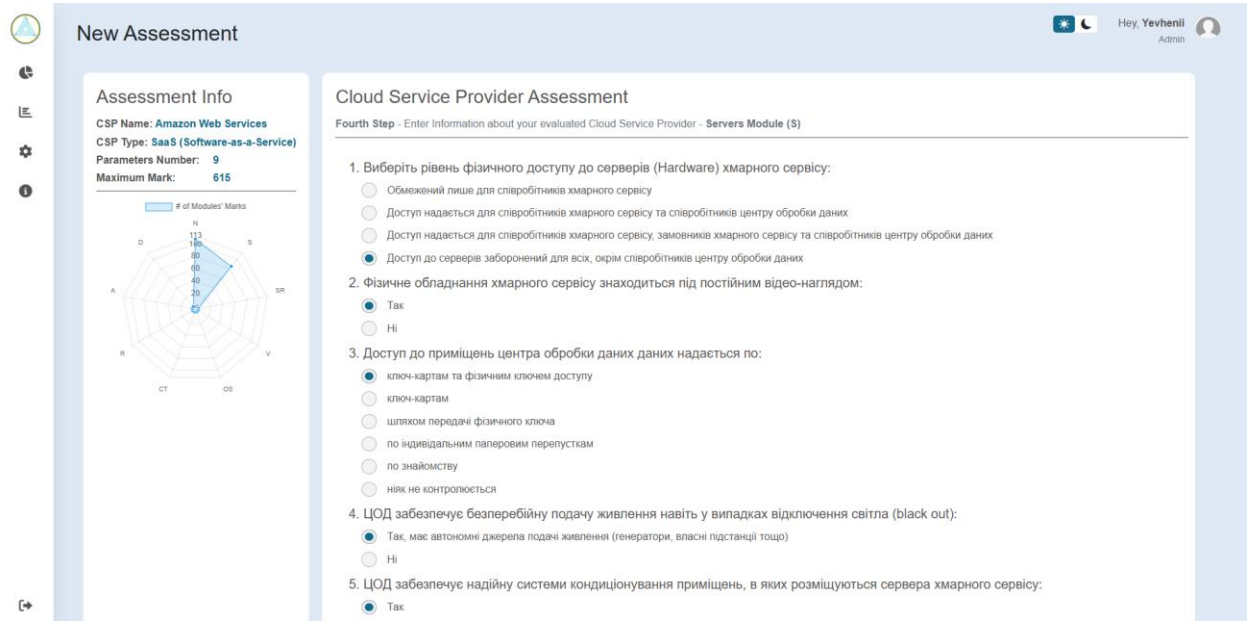


Рис. 3.18. Оцінювання серверної частини хмарного сервісу

Після оцінювання серверної частини, аудитор потрапляє на сторінку оцінювання по параметру «Virtualization Module», де аудитору необхідно надати інформацію, щодо частини віртуалізації, де надається інформація, щодо використовуваного середовища віртуалізації, систем безпеки, доступів до VPS/VDC, систем управління ключами тощо (Рис. 3.19.):

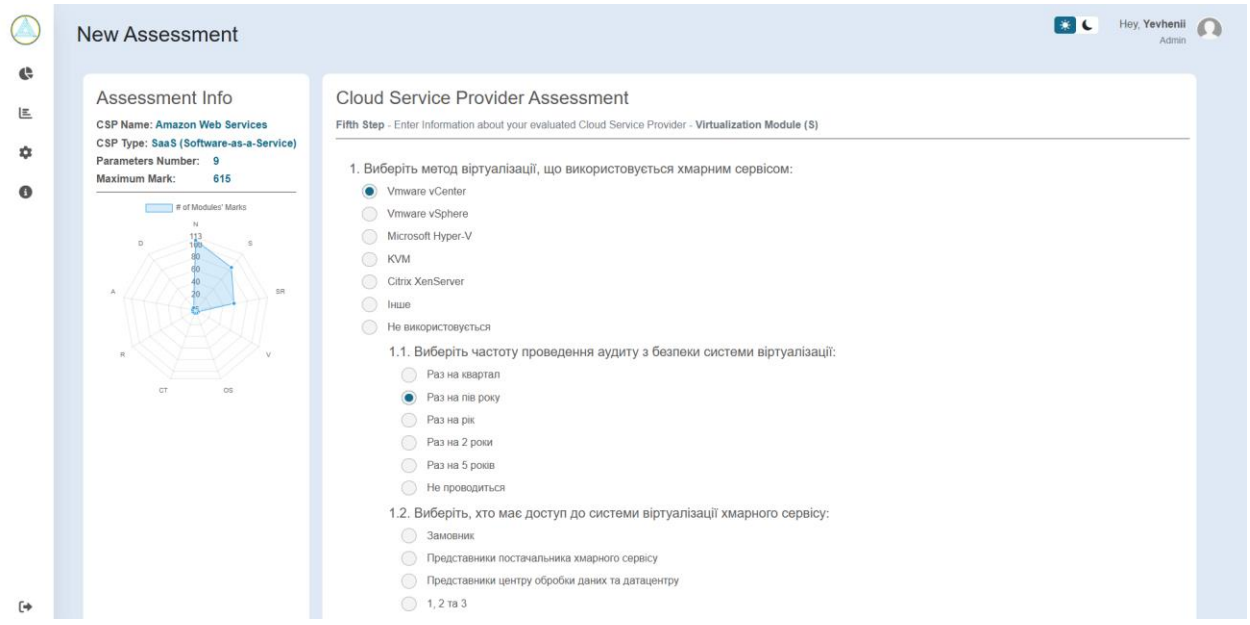


Рис. 3.19. Оцінювання частини віртуалізації хмарного сервісу

Після оцінювання частини віртуалізації, аудитор потрапляє на сторінку оцінювання по параметру «Operation System Module», де аудитору необхідно надати інформацію, щодо частини операційної системи, де надається інформація, щодо можливостей використання готових образів систем, можливості, розгортання власних образів та програмного забезпечення, доступність операційних систем з будь-якої точки світу, контроль доступу до розгорнутих образів тощо(Рис. 3.20.):

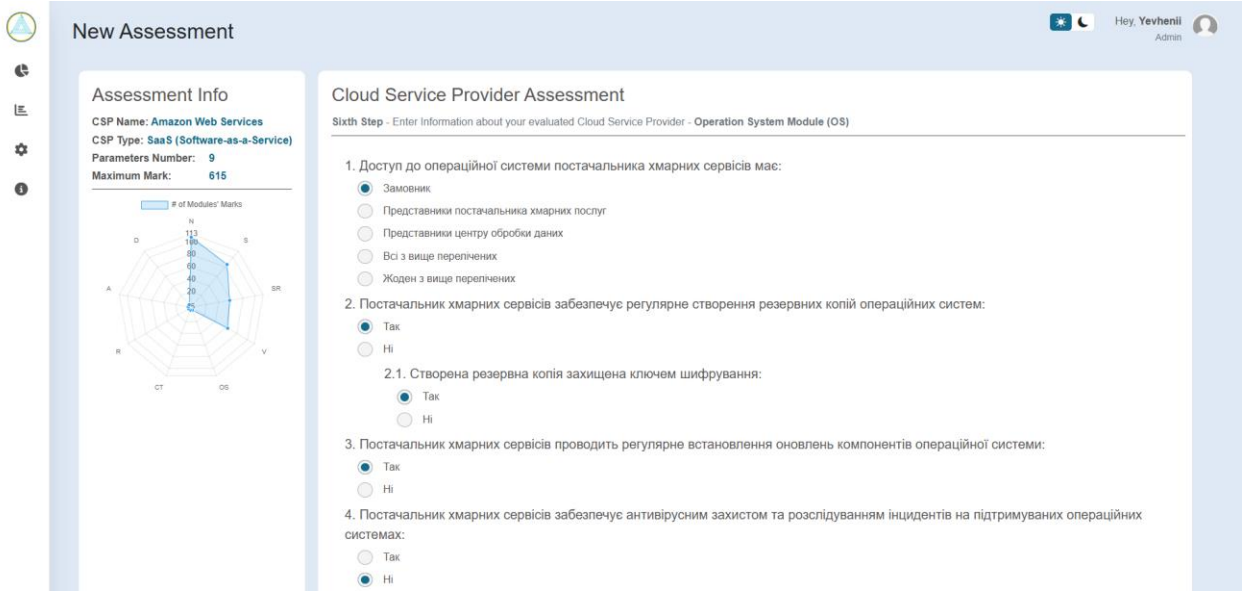


Рис. 3.20. Оцінювання частини операційної системи хмарного сервісу

Після оцінювання частини операційної системи, аудитор потрапляє на сторінку оцінювання по параметру «Container Technology Module», де аудитору необхідно надати інформацію, щодо частини управління контейнеризацією, де надається інформація, щодо можливостей системи контейнеризації, використання внутрішнього репозиторію провайдера, можливість створення резервних копій, моніторинг використання контейнерів тощо (Рис. 3.21.):

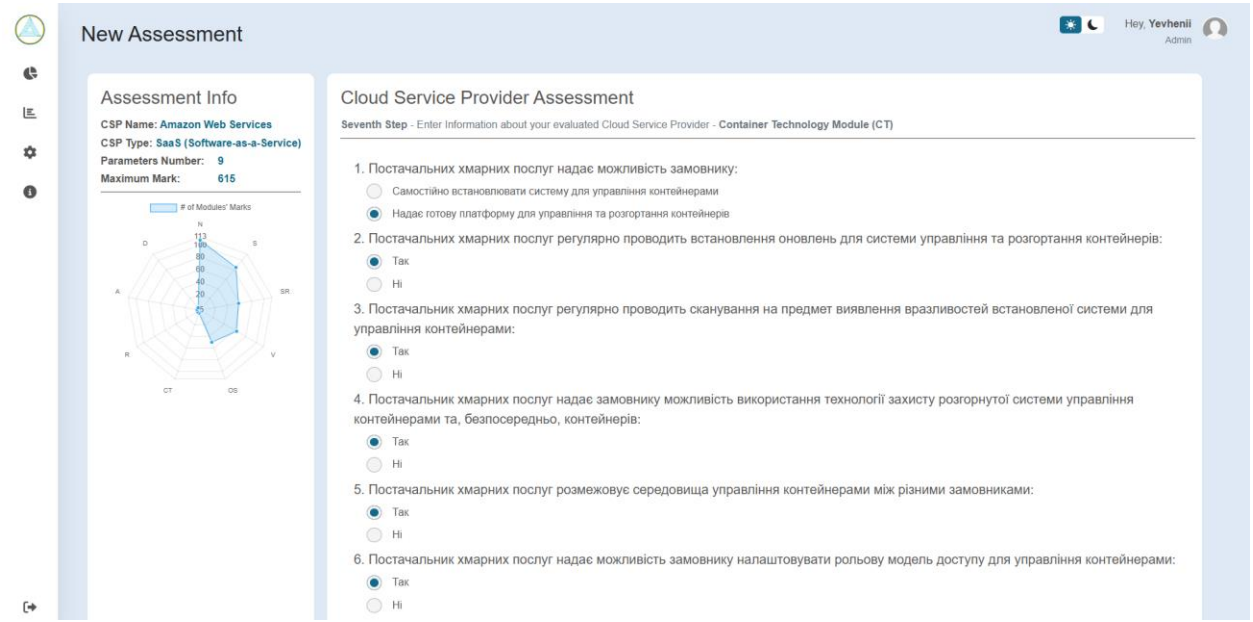


Рис. 3.21. Оцінювання частини управління контейнеризацією хмарного сервісу

Після оцінювання частини управління контейнеризацією, аудитор потрапляє на сторінку оцінювання по параметру «Runtime Module», де аудитору необхідно надати інформацію, щодо частини моніторингу, де надається інформація, щодо можливостей збору журналів подій, аудиту систем, проведення виявлення та аналіз вразливостей, аудит парольної політики тощо (Рис. 3.22.):

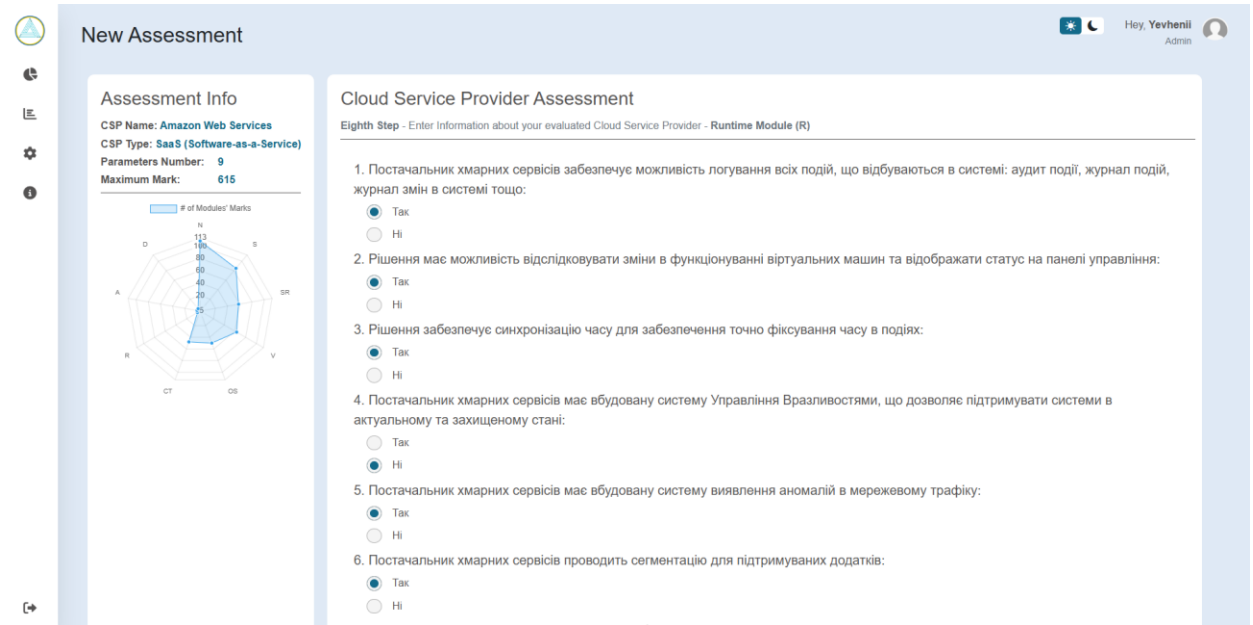


Рис. 3.22. Оцінювання частини моніторингу хмарного сервісу

Після оцінювання частини моніторингу, аудитор потрапляє на сторінку оцінювання по параметру «Application Module», де аудитору необхідно надати інформацію, щодо частини застосунку, де надається інформація, щодо підтримки пропонованого застосунку провайдером, регулярне оновлення, забезпечення безпеки на основі операційної системи додатку, підтримка крос-платформенного використання тощо (Рис. 3.23.):

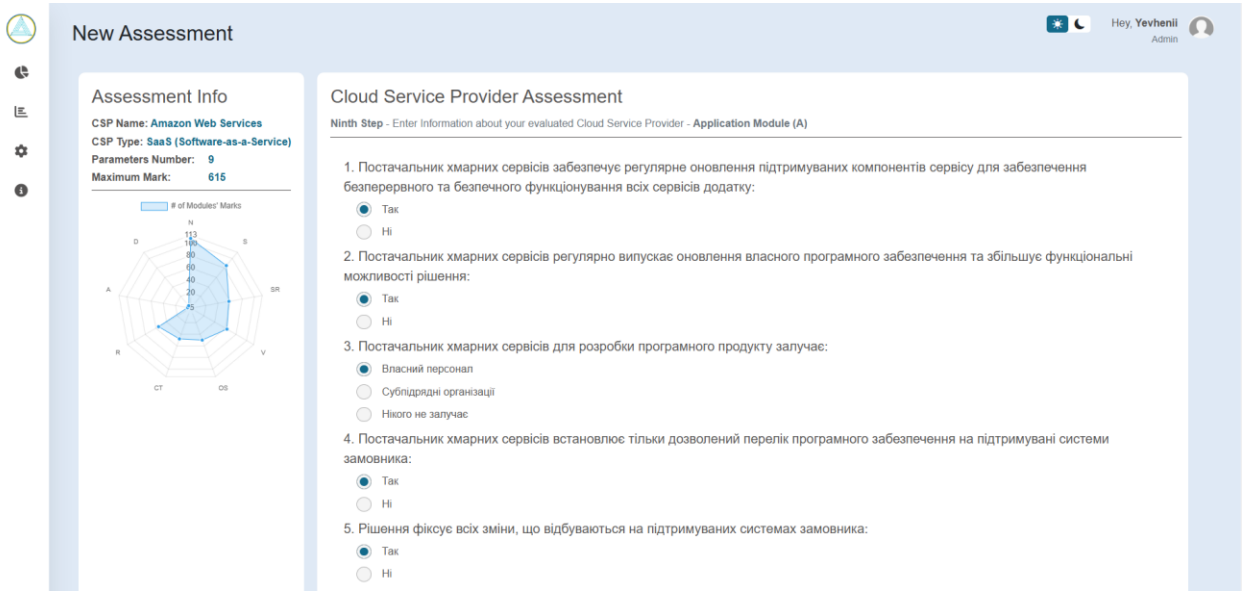


Рис. 3.23. Оцінювання частини додатку хмарного сервісу

Після оцінювання частини даних, аудитор потрапляє на сторінку оцінювання по параметру «Data Module», де аудитору необхідно надати інформацію, щодо частини застосунку, де надається інформація, щодо управління даними, які обробляються на розгорнутих образах, перевірки текстових файлів, перевірка наявності рішень data Classification та Data Leak Prevention, перевірка SLA провайдера тощо (Рис. 3.24.):

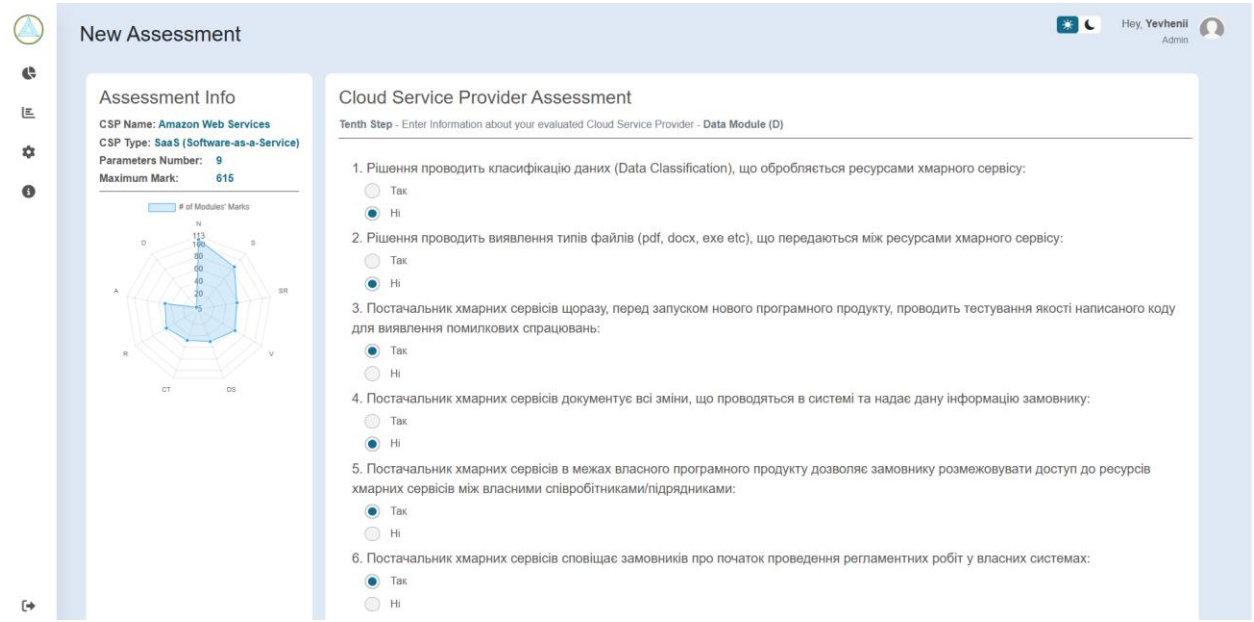


Рис. 3.24. Оцінювання частини даних хмарного сервісу

Після проведеного оцінювання хмарного провайдера, аудитору пропонується на вибір три варіанти дій (Рис. 3.25.):

1- Варіант «Yes» - при натисненні на дану кнопку, аудитор зберігає результати оцінювання та переходить на сторінку формування звіту.

2- Варіант «Only Save» - аудитор зберігає результати оцінювання та переходить на сторінку зі всіма проведеними оцінками, як це зображено на Рис. 3.8.

3- Варіант «No» - аудитор повертається до редагування проведеного оцінювання хмарного сервісу.

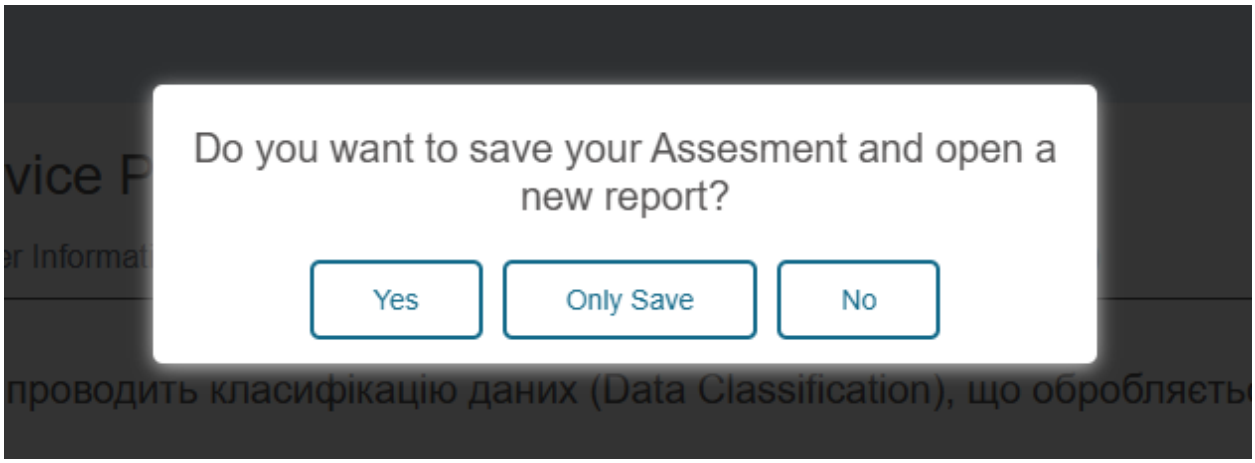


Рис. 3.25. Вибір дії після завершення оцінювання хмарного сервісу

Після натиснення на кнопку «Yes» на Рис. 3.25., аудитору відкриється сформований звіт по проведеній оцінці, де буде зображено статистичні дані по

проведеному оцінюванні у вигляді кругових діаграм та набраних балів на Рис. 3.26., а також надання рекомендацій для кожної наданої відповіді аудитору по результатам оцінювання хмарного сервісу на Рис. 3.27:

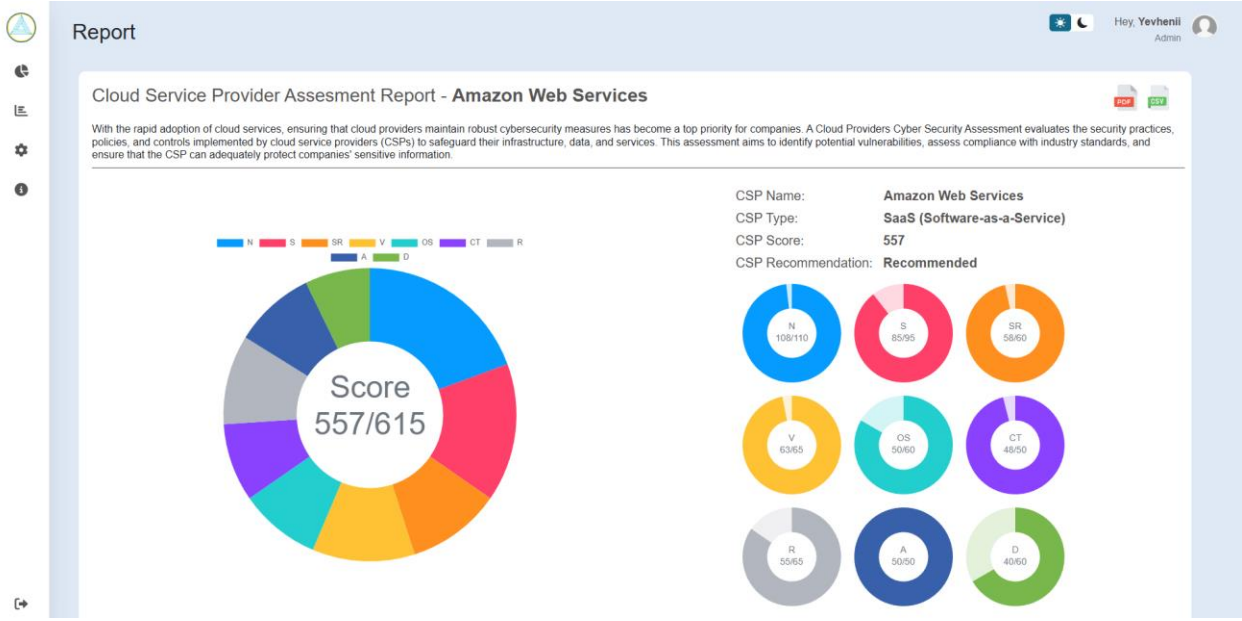


Рис. 3.26. Загальний вигляд звіту по результатам проведеного оцінювання з представленням статистичних даних

Рис. 3.27. Загальний вигляд звіту по результатам проведеного оцінювання з представленням рекомендацій на надані відповіді аудитора

Продовження представлення роботи захищеного мережевого застосунку оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури див. додаток Б.

Висновок до розділу 3

Розроблене алгоритмічне програмне забезпечення для захищеного мережевого застосунку оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури розроблено на основі побудованих моделі, методу та системи оцінювання, що надає представлення чіткого та послідовного виконання оцінювання на базі захищеного мережевого застосунку у вигляді розроблених блок-схем кожного із використовуваних параметрів оцінювання хмарних сервісів, а також є основною для побудови захищеного мережевого застосунку оцінювання кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

Метою експериментального дослідження було проведення оцінювання стану кіберзахисту хмарного сервісу «Amazon Web Services» із використання розробленого захищеного мережевого застосунку, що включає покрокове проходження модулів та параметрів оцінювання стану кіберзахисту хмарного сервісу, та як результат надання рекомендацій стосовно його використання.

ВИСНОВКИ

Результатом виконання дисертаційної роботи є вирішення актуальної та сучасної науково-технічної задачі розробки моделі та методу оцінювання кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

За результатами виконання дисертаційної роботи було отримано такі наукові та практичні результати:

1. На основі проведеного аналізу методів та моделей оцінювання стану кіберзахисту хмарних сервісів на міжнародних ринках, визначено, що наявні лише частково покривають дане питання та є вузькоспеціалізованими, і не дозволяють комплексно покривати задачу оцінювання стану кіберзахисту хмарних сервісів у можливих аспектах їх виконання, завдяки чому виділено ключові параметри оцінювання стану кіберзахисту хмарних сервісів, що покривають всі можливі напрямки роботи найпопулярніших типів хмарних сервісів з точки зору кібербезпеки.

2. Розроблено узагальнену математичну модель параметрів на базі теоретико-множинного підходу формування множин та підножин критеріїв оцінювання хмарних сервісів, що мають за основу одинадцять ключових модулів (параметрів), націлених на комплексне покриття оцінювання стану кіберзахисту хмарних сервісів, яка надалі буде використана для розробки відповідного методу оцінювання стану кіберзахисту об’єктів інформаційної інфраструктури.

3. Розроблено математичний метод параметрів, що побудований на базі теоретико-множинного підходу моделі оцінювання і дозволяє визначити вагу кожного із розроблених параметрів та критеріїв оцінювання, та забезпечує можливістю обчислення стану кіберзахисту хмарних сервісів, що надає рекомендації щодо подальшого використання оцінюваного хмарного сервісу для розгортання бізнес-додатків компанії, а також буде використаний для подальшої розробки структурної моделі системи оцінювання хмарних сервісів об’єктів інформаційної інфраструктури.

4. Розроблено структурну модель системи оцінювання хмарних сервісів, що побудована на базі розроблених моделі та методів оцінювання стану захищеності, яка надає детальне послідовне використання розроблених параметрів оцінювання стану кіберзахисту хмарних сервісів із розподілом по різних типах хмарних сервісів, що включає в себе детальний опис взаємодії результатів оцінювання із базою даних збереження результатів, формування фінального звіту по проведеному оцінюванню, та в подальшому використання напрацювань дослідження для розробки алгоритмічного та програмного забезпечення.

5. Розроблено алгоритмічне забезпечення та побудовано мережевий застосунок оцінювання кіберзахисту хмарних сервісів на базі розроблених моделі, методу та структурної моделі системи оцінювання стану кіберзахисту хмарних сервісів, що надає можливість використання аудитором програмного забезпечення для проведення оцінювання планованих до використання чи використовуваних хмарних сервісів в інфраструктурі компанії, із поетапних проходом кожного із параметрів оцінювання унікальних для кожного типу хмарного сервісу, що в результаті надає фінальний звіт за результатами проведеного оцінювання, кількість набраних балів, набір рекомендацій щодо покращення кіберзахисту хмарного сервісу, а також фінальний висновок, щодо рекомендованого чи нерекомендованого використання хмарного сервісу в інфраструктурі компанії.

6. Проведене експериментальне дослідження програмного застосунку оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури дозволило оцінити стан кіберзахисту існуючих на сьогодні хмарних сервісів та визначити стан їх рівня кіберзахисту. Отримані результати можуть бути використані для оцінювання стану кіберзахисту інфраструктури компанії, яка планує використовувати хмарні сервіси у власній інфраструктурі для розгортання бізнес-процесів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Internet Solutions Division Strategy for Cloud Computing. *Compaq computer corporation*. 1996. 4 p. URL: https://s3.amazonaws.com/files.technologyreview.com/p/pub/legacy/compaq_cst_1996_0.pdf (date of access: 20.04.2024)
2. Dan Verton. Public/Private Security PartnershipGets Rocky. *ComputerWorld*. 2003. URL: link (date of access: 20.04.2024)
3. Camille Paloque-Bergès. Arpanet (1969–2019) / Camille Paloque-Bergès, Valérie Schafer. *Internet Histories*. 2019. Vol 1, № 3. P. 1-14. URL: https://www.researchgate.net/publication/330433261_Arpanet_1969-2019 (date of access: 20.04.2024)
4. S. Susnjara, I. Smalley. What is cloud computing? *IBM*. 2024. URL: https://www.ibm.com/topics/cloud-computing (date of access: 20.04.2024)
5. The History of Salesforce. *SalesForce*. 2024. URL: https://www.salesforce.com/news/stories/the-history-of-salesforce/ (date of access: 21.04.2024)
6. D. Farber. Oracle's Ellison nails cloud computing. *CNET : YourGuide toa better future*. 2008. URL: https://www.cnet.com/news/oracles-ellison-nails-cloud-computing/ (date of access: 21.04.2024)
7. What are Strategic Cloud Platform Services? *Gartner Peer Insights*. 2024. URL: https://www.gartner.com/reviews/market/public-cloud-iaas (date of access: 22.04.2024)
8. About CrowdStrike. *CrowdStrike*. 2024. URL: https://www.crowdstrike.com/about-crowdstrike/ (date of access: 22.04.2024)
9. CrowdStrike has become the leader in the Gartner Magic Quadrant 2021 for the second time among endpoint protection platforms! *IITD*. 2021. URL: https://iitd.com.ua/en/news/crowdstrike-vdruge-stala-liderom-v-gartner-magic-quadrant-2021-roku-sered-platform-zahistu-kincevih-tochok/ (date of access: 15.05.2023)

10. P. Mell, T. Grance. NIST SP 800-145 : The NIST Definition of Cloud Computing. *NIST*. 2011. URL: https://doi.org/10.6028/NIST.SP.800-145 (date of access: 16.05.2023)
11. What is a Public Cloud? *VMware by Broadcom*. 2020. URL: link (date of access: 22.11.2023)
12. What is private cloud? *VMware by Broadcom*. 2020. URL: https://www.vmware.com/topics/glossary/content/private-cloud.html (date of access: 22.11.2023)
13. Community Cloud. *Gartner*. 2020. URL: https://www.gartner.com/en/information-technology/glossary/community-cloud (date of access: 27.11.2023)
14. What is a hybrid cloud? *Microsoft Azure*. 2021. URL: https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud-computing/#:~:text=A%20hybrid%20cloud%E2%80%94sometimes%20called,to%20be%20shared%20between%20them (date of access: 29.11.2023)
15. Y2K problem. *PC Mag*. 2000. URL: https://www.pcmag.com/encyclopedia/term/y2k-problem (date of access: 29.11.2023)
16. Amazon CloudWatch. *Amazon Web Services*. 2024. URL: https://aws.amazon.com/ru/cloudwatch/ (date of access: 13.04.2024)
17. Amazon Virtual Private Cloud. *Amazon Web Services*. 2024. URL: https://aws.amazon.com/ru/vpc/ (date of access: 13.04.2024)
18. Amazon Relational Database Service // Amazon Web Services. 2024. URL: https://aws.amazon.com/ru/rds/ (date of access: 13.04.2024)
19. AWS Auto Scaling. *Amazon Web Services*. 2024. URL: https://aws.amazon.com/ru/autoscaling/ (date of access: 13.04.2024)
20. Cloud Computing Services and Solutions. *IBM*. 2024. URL: https://www.ibm.com/cloud/compute (date of access: 13.04.2024)

21. S. Paul. The History of Google Cloud Platform. *PluralSight*. 2023. URL: https://acloudguru.com/blog/engineering/history-google-cloud-platform (date of access: 15.02.2024)
22. C. Harvey. What is Microsoft Azure Cloud & What is It Used for?. *Datamation*. 2017. URL: https://www.datamation.com/cloud/microsoft-azure-cloud/ (date of access: 15.02.2024)
23. IBM Turbonomic. *IBM*. 2024. URL: https://blog.turbonomic.com/cloud-computing-two-decades-in-review (date of access: 15.02.2024)
24. B. Goswami. Gartner IaaS Magic Quadrant comparison from 2010 and 2013. *CloudHat*. 2013. URL: https://blog.cloudthat.com/gartner-iaas-magic-quadrant-comparison-from-2010-and-2013/ (date of access: 27.10.2023)
25. Janakiram MSV. A Look Back At Ten Years Of Microsoft Azure. *Forbes*. 2020. URL: https://www.forbes.com/sites/janakirammsv/2020/02/03/a-look-back-at-ten-years-of-microsoft-azure/?sh=73bed1414929 (date of access: 28.10.2023)
26. Introduction: A Bit of OpenStack History. *OpenStack*. 2021. URL: https://docs.openstack.org/project-team-guide/introduction.html (date of access: 27.01.2024)
27. CloudStack's History. *Cloudstack*. 2013. URL: https://cloudstack.apache.org/history.html (date of access: 27.01.2024)
28. Ram Kumar Shukla. What is Digital Ocean and it's history?. *Dev.to*. 2020. URL: https://dev.to/ramkshukla/what-is-digital-ocean-and-it-s-history-55dp (date of access: 27.01.2024)
29. IBM Cloud Reference Architectures unleashed. *IBM*. 2024. URL: https://www.ibm.com/new/announcements/ibm-cloud-reference-architectures-unleashed (date of access: 27.01.2024)
30. Cloud Foundry Ecosystem Celebrates First Anniversary. *Broadcom*. 2012. URL: https://news.broadcom.com/releases/vmw-cloud-foundry-041112 (date of access: 23.08.2023)

31. N. Wright. Everything you ever wanted to know about Microsoft Azure. *Nigel Frank International*. URL: https://www.nigelfrank.com/blog/everything-you-ever-wanted-to-know-about-microsoft-azure/ (date of access: 23.08.2023)
32. J. Kincaid. Google Names VMware Cofounder Diane Greene To Its Board. *TechCrunch*. 2012. URL: https://techcrunch.com/2012/01/12/google-names-vmware-cofounder-diane-greene-to-its-board/ (date of access: 23.08.2023)
33. J. Schwartz. Cloud Report. *Redmond Channel Partner*. 2012. URL: https://rcpmag.com/blogs/the-schwartz-cloud-report/2012/04/hp-sets-launch-of-public-cloud-service.aspx (date of access: 23.08.2023)
34. Announcing the AWS China (Beijing) Region. *Amazon Web Services*. 2013. URL: https://aws.amazon.com/about-aws/whats-new/2013/12/18/announcing-the-aws-china-beijing-region/ (date of access: 23.08.2023)
35. IBM reports 2018 IBM reports 2018 fourth-quarter quarter quarterand full and full and full-year results. *IBM*. 2018. URL: https://www.ibm.com/blogs/cloud-computing/2019/01/25/ibm-cloud-revenue-q4-2018/ (date of access: 19.04.2023)
36. VMware VCloud hybrid service now available to all us customers. *VMware*. 2013.
URL: https://blogs.vmware.com/cloudprovider/2013/08/vmware-vcloud-hybrid-service-now-available-to-all-u-s-customers.html (date of access: 19.04.2023)
37. Upcoming Name Change for Windows Azure. *Microsoft Azure*. 2014. URL: https://azure.microsoft.com/en-us/blog/upcoming-name-change-for-windows-azure/#:~:text=Today%20we%20are%20announcing%20that,%2C%20Skype%2C%20and%20Xbox%20Live (date of access: 18.06.2024)

38. Introducing Sustained Use Discounts - Automatically pay less for sustained workloads on Compute Engine. *GoogleCloud Platform*. 2014. URL: https://cloudplatform.googleblog.com/2014/04/introducing-sustained-use-discounts.html (date of access: 18.06.2024)
39. J. Barr. Amazon EC2 Container Service (ECS) – Container Management for the AWS Cloud. *Amazon Web Services*. 2014. URL: https://aws.amazon.com/blogs/aws/cloud-container-management/ (date of access: 18.06.2024)
40. IBM Turbonomic. *IBM*. 2024. URL: https://blog.turbonomic.com/cloud-computing-two-decades-in-review-2 (date of access: 18.06.2024)
41. F. Hámori. The History of Kubernetes on a Timeline. *RisingStack*. 2024. URL: https://blog.risingstack.com/the-history-of-kubernetes/ (date of access: 18.06.2024)
42. J. Novet. Amazon Web Services brings in $2.4B in revenue in Q4 2015, up 69% over last year. *VentureBeat*. 2016. URL: https://venturebeat.com/2016/01/28/amazon-web-services-brings-in-2-4b-in-revenue-in-q4-2015-up-69-over-last-year/ (date of access: 10.08.2023)
43. Y. Sverdlik. Verizon Shutting Down Public Cloud, Gives Two Months to Move Data. *DataCenterKnowledge*. 2016. URL: https://www.datacenterknowledge.com/archives/2016/02/12/verizon-shutting-down-public-cloud-gives-users-one-month-to-move-data (date of access: 10.08.2023)
44. W. Oskay. HP is officially shutting down its Helion public cloud in January 2016. *VentureBeat*. 2015. URL: https://venturebeat.com/2015/10/21/hp-is-officially-shutting-down-its-helion-public-cloud-in-january-2016/ (date of access: 11.08.2023)
45. R. Hunt. Introducing AWS Fargate – Run Containers without Managing Infrastructure. *Amazon Web Services*. 2017. URL: https://aws.amazon.com/blogs/aws/aws-fargate/ (date of access: 12.08.2023)

46. Introducing Amazon SageMaker. *Amazon Web Services*. 2017. URL: https://aws.amazon.com/about-aws/whats-new/2017/11/introducing-amazon-sagemaker/ (date of access: 13.08.2023)
47. Infrastructure Cloud Services. *VMware by Broadcom*. 2024. URL: https://www.vmware.com/in/cloud-services/infrastructure.html (date of access: 11.03.2024)
48. IBM and Red Hat - choice and control, in your hands. *IBM*. 2024. URL: https://www.ibm.com/cloud/redhat (date of access: 12.05.2024)
49. Microsoft acquires GitHub. *Microsoft*. 2018. URL: https://news.microsoft.com/announcement/microsoft-acquires-github/ (date of access: 12.05.2024)
50. K. Marko. Google Anthos features and updates. *Tech Target* : Cloud Computing. 2021. URL: link (date of access: 12.05.2024)
51. Azure Arc. *Microsoft*. 2024. URL: https://azure.microsoft.com/en-us/services/azure-arc/ (date of access: 12.05.2024)
52. IBM Turbonomic. *IBM*. 2024. URL: https://blog.turbonomic.com/cloud-computing-two-decades-in-review-3 (date of access: 12.05.2024)
53. What are Strategic Cloud Platform Services? *Gartner Peer Insights*. 2024. URL: https://www.gartner.com/reviews/market/public-cloud-iaas (date of access: 12.05.2024)
54. A Framework for Comparing and Ranking Cloud Services. *SMICloud*. 2011. URL: link (date of access: 14.07.2023)
55. A. Abuhussein, S. Shiva, Frederick T. Sheldon. CSSR: Cloud Services Security Recommender. *IEEE Xplore*. 2016. URL: https://ieeexplore.ieee.org/abstract/document/7557392 (date of access: 14.07.2023)
56. M. Karthik, Mrs.M.Revati. A Novel Implementation Of Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services. International Journal For Advanced Research in Science & Technology. 2021. Vol. 11. 340-346 p. URL:

http://www.ijarst.in/public/uploads/paper/711181639296684.pdf (date of access: 14.07.2023)

57. Use containers to Build, Share and Run your applications. Docker. 2024. URL: https://www.docker.com/resources/what-container (date of access: 05.06.2024)
58. Containerized Architecture: Components and Design Principles. Cloud Native Wiki by Aqua. 2021. URL: link (date of access: 05.06.2024)
59. D. Jones. Containers vs. Virtual Machines (VMs): What's the Difference? *NetApp*. 2018. URL: link (date of access: 05.06.2024)
60. What is Docker? *DockerDocs*. 2024. URL: link (date of access: 05.06.2024)
61. What is container orchestration? *RedHat*. 2022. URL: https://www.redhat.com/en/topics/containers/what-is-container-orchestration (date of access: 05.06.2024)
62. Overview. *Kubernetes*. 2024. URL: https://kubernetes.io/docs/concepts/overview/ (date of access: 05.06.2024)
63. Social Engineering. *Imperva a Thales company*. 2024. URL: https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps (date of access: 05.06.2024)
64. Man in the Cloud (MITC) Attacks. *Imperva*. 2015. URL: https://www.imperva.com/docs/hii_man_in_the_cloud_attacks.pdf (date of access: 15.09.2023)
65. Session hijacking attack. *OWASP*. 2024. URL: link (date of access: 05.06.2024)
66. Introduction to session hijacking and riding. *Safe Security*. 2024. URL: https://www.safe.security/resources/blog/introduction-to-session-hijacking-and-riding/ (date of access: 05.06.2024)
67. R. Taylor. Four major DNS attack types and how to mitigate them. *BlueCat*. 2024. URL: https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/ (date of access: 05.06.2024)

68. SQL injection. *PortSwigger*. 2024. URL: https://portswigger.net/web-security/sql-injection (date of access: 05.06.2024)
69. Cryptanalysis and Types of Attacks. *Geek for Geeks*. 2024. URL: https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/ (date of access: 05.06.2024)
70. T. Keary. Dos vs DDoS Attacks: The Differences and How To Prevent Them. *CompariTech*. 2024. URL: link (date of access: 05.06.2024)
71. Man-in-the-browser attack. *OWASP*. 2024. URL: https://owasp.org/www-community/attacks/Man-in-the-browser_attack
72. CAPEC-690: Metadata Spoofing. *Mitre*. 2022. URL: https://capec.mitre.org/data/definitions/690.html (date of access: 02.02.2024)
73. R. Das. The types of malware injection attacks. *Keesing Technologies*. 2020. URL: https://platform.keesingtechnologies.com/malware-attacks/ (date of access: 12.05.2023)
74. Welcome to the OWASP Top 10 – 2021. *OWASP Top 10:2021*. 2021. URL: https://owasp.org/Top10/ (date of access: 07.11.2023)
75. 7 Layers of Security. *EgisTech*. 2024. URL: https://www.egistech.com/why-egis/7-layers-of-security/ (date of access: 08.05.2024)
76. Гнатюк С.Л. "Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики". Аналітична записка. *НІСД: Національний інститут стратегічних досліджень*. 2013. URL: посилання (дата звернення: 09.04.2024)
77. Про критичну інфраструктуру : Закон України від 21.09.2024 р. № 1882-IX. Верховна Рада України. 2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 09.04.2024)
78. ПОЯСНЮВАЛЬНА ЗАПИСКА до проекту Закону України "Про хмарні послуги". *Ліга Закон*. 2019. URL:

https://ips.ligazakon.net/document/gi01021a?an=4&ed=2019_12_20 (дата звернення: 09.04.2024)

79. Приватна хмара як сервіс (Private Cloud). *Denovo*. 2024. URL: https://denovo.ua/blog/kruglyi-stil-hmari-v-ukraini (дата звернення: 09.04.2024)
80. Мінцифри: Законопроект про хмарні сервіси прийнято в цілому. *Міністерство цифрової трансформації України*. 2022. URL: https://www.kmu.gov.ua/news/mincifri-zakonoproekt-pro-hmarni-servisi-prijnyato-v-cilomu (date of access: 22.03.2024)
81. Cloud Vs On Premise Software: Which is Best For Your Business? *Xperience*. 2017. URL: https://www.xperience-group.com/news-item/cloud-vs-on-premise-software/ (date of access: 06.02.2023)
82. K. Marko. When should you use cloud vs. on-premises storage? *TechTarget : Cloud Computing*. 2020. URL: https://www.techtarget.com/searchcloudcomputing/answer/When-should-you-use-cloud-vs-on-premises-storage (date of access: 04.09.2023)
83. Корченко О.Г. Системи захисту інформації : монографія. Київ. 2004. 264 с. URL: https://scholar.google.com/scholar?cluster=6804965558680208678&hl=en&oi=scholarr (дата звернення: 18.01.2024)
84. Dr. Rabi Prasad Padhy. Alibaba Anti-DDoS: The best Hybrid Cloud-based DDoS Protection Service. *Medium*. 2018. URL: https://medium.com/@rabi.padhy/alibaba-anti-ddos-the-best-hybrid-cloud-based-ddos-protection-service-9fc926b0bed0 (date of access: 03.03.2024)
85. How does DDoS protection work? *DataDome*. 2019. URL: https://datadome.co/guides/ddos/protection/ (date of access: 12.09.2023)
86. Nguyen Ngoc Tuan, Pham Huy Hung, Nguyen Danh Nghia, Nguyen Van Tho, Trung Van Phan, Nguyen Huu Thanh. A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. *Future*

Networks: New Advances and Challenges. 2020. URL: https://www.mdpi.com/2079-9292/9/3/413 (date of access: 12.10.2023)

87. Where to Park Your Data: A Roadmap for Cloud Storage Requirements. *CompTIA*. 2024. URL: https://www.comptia.org/content/infographic/cloud-storage-requirements-what-you-need-to-know (date of access: 02.04.2024)
88. Cloud Security Requirements. CMS Technical Reference Architecture. 2024. URL: https://www.cms.gov/tra/Infrastructure_Services/IS_0100_Cloud_Security_Requirements.htm (date of access: 02.02.2024)
89. IVS: Infrastructure & Virtualization Security. *CSF Tools*. 2019. URL: https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/ivs/ (date of access: 19.01.2024)
90. IAM: Identity & Access Management. *CSF Tools*. 2019. URL: https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/iam/ (date of access: 19.01.2024)
91. Cloud Controls Matrix v3.0.1. *CSF Tools*. 2019. URL: https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/ (date of access: 19.01.2024)
92. DSI: Data Security & Information Lifecycle Management. *CSF Tools*. 2019. URL: https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/dsi/ (date of access: 19.01.2024)
93. CCC: Change Control & Configuration Management. *CSF Tools*. 2019. URL: https://csf.tools/reference/cloud-controls-matrix/version-3-0-1/ccc/ (date of access: 19.01.2024)
94. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. Analysis of modern cloud services to ensure cybersecurity. *Procedia Computer Science*. 2022. Vol. 207. P. 110-117. Mode of access: https://www.sciencedirect.com/science/article/pii/S1877050922009164 .

DOI : https://doi.org/10.1016/j.procs.2022.09.043 (date of access: 17.01.2024)

95. Педченко Є.М., Корченко О.Г., Дрейс Ю.О., Лозова І.Л. Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*. 2020. Том. 22, № 2. С. 120-141. URL: https://doi.org/10.18372/2410-7840.22.14871 (дата звернення: 10.10.2024)
96. Pedchenko Y., Bystrova B., Lozova I., Petrovska M. Fuzzy standards system for negative consequences assessment from personal data leaks. *Polit. Challenges of science today, 5-7 April 2022* : abstracts of XXII International conference of higher education students and young scientists. Kyiv. 2022. P. 12-13. (date of access: 10.10.2024)
97. Педченко Є.М., Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. *Захист інформації*. 2023. Том 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232 (дата звернення: 10.10.2024)
98. Pedchenko Y., Ivanchenko I., Lozova I., Petrovska M. System incident management using cloud technologies. *Polit. Challenges of science today, 5-7 April 2023* : abstracts of XXIII International conference of higher education students and young scientists. Kyiv. 2023. P. 3-4. URL: http://www.kzzi.nau.edu.ua/wp-content/uploads/2023/05/Polit_2023_FCSSE.pdf (date of access: 14.10.2024)
99. Педченко Є.М., Іванченко Є.В., Іванченко І.С., Лозова І.Л., Петровська М.Г. Архітектура хмарного рішення для централізованого збору та обробки інцидентів інформаційної безпеки. *ITSec-2023: Безпека інформаційних технологій* : матеріали XII міжнар. наук.-тех. конф., м. Київ, 2-4 травня 2023 р. Київ, 2023. С. 69-73. URL:

http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf (date of access: 14.10.2024)

100. Педченко Є.М. Технології Akamai для доставки веб-контенту та його захисту. *Мережі та безпека : Захист даних*. Київ. 2023. 2 с. URL: https://www.seeton.pro/en/news/akamai-technologies-delivery-web-content-and-protection/ (date of access: 15.10.2024)

101. Pedchenko Y., Shulha V., Korchenko O., Ivanchenko Y., Vyshnevska N., Petrovska M. Mathematical model of security cloud services assessment. *Problems of scientific, technical and legal support for cybersecurity in the modern world* : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 13-21. DOI : 10.24917/9788668020861 .

102. Pedchenko Y., Karpinski M., Lozova I., Kotyk O., Petrovska M. Damage assessment from the personal data loss. *Problems of scientific, technical and legal support for cybersecurity in the modern world* : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 34-46. DOI : 10.24917/9788668020861.

103. Педченко Є.М., Іванченко Є.В., Іванченко І.С., Лозова І.Л., Петровська М.Г. Математична модель оцінки захищеності хмарних сервісів. *ITSec-2024: Безпека інформаційних технологій* : матеріали XII міжнар. наук.-тех. конф., м. Київ, 9-11 травня 2024 р. 2024. Київ, 2024. С. 102-105. URL: https://drive.google.com/file/d/1xbCeTF33YjZbgoXcYqAYz3ST-oKRPCgM/view (дата звернення: 14.11.2024)

104. Педченко Є.М., Іванченко І.С. Структурна модель системи оцінювання кібербезпеки хмарних сервісів об’єктів інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2024. Том 1, № 25. С. 505-515. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/667 . DOI : https://doi.org/10.28925/2663-4023.2024.25.505515 (дата звернення: 14.11.2024)

105. Pedchenko Y., Korchenko O., Ivanchenko Y., Ivanchenko I., Petrovska M. The system of secured user's credentials transfer. *CPITS-II 2024 : Cybersecurity Providing in Information and Telecommunication Systems II*. 2024. P. 168-173. URL: https://ceur-ws.org/Vol-3826/short3.pdf . ISSN: 1613-0073. (date of access: 15.11.2024)

106. Педченко Є.М., Іванченко І.С. Метод оцінювання кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. *Сучасний захист інформації*. 2024. Том. 59, №3. С. 75-84. URL: https://doi.org/10.31673/2409-7292.2024.030008 (дата звернення: 16.11.2024)

107. Педченко Є.М., Іванченко І.С. Аналіз моделей та методів оцінювання стану кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. *Безпека інформації*. 2024. Том. 30, №2. С. 279-287. URL: https://doi.org/10.18372/2225-5036.30.19240.

108. Педченко Є.М., Іванченко І.С. Модель захищеного мережевого додатку оцінювання Кібербезпеки постачальників хмарних сервісів. *Наукові записки ДУІКТ*. 2024. Том. 6, №2. С. 116-134. DOI: 10.31673/2518-7678.2024.025842

ДОДАТКИ

Додаток А

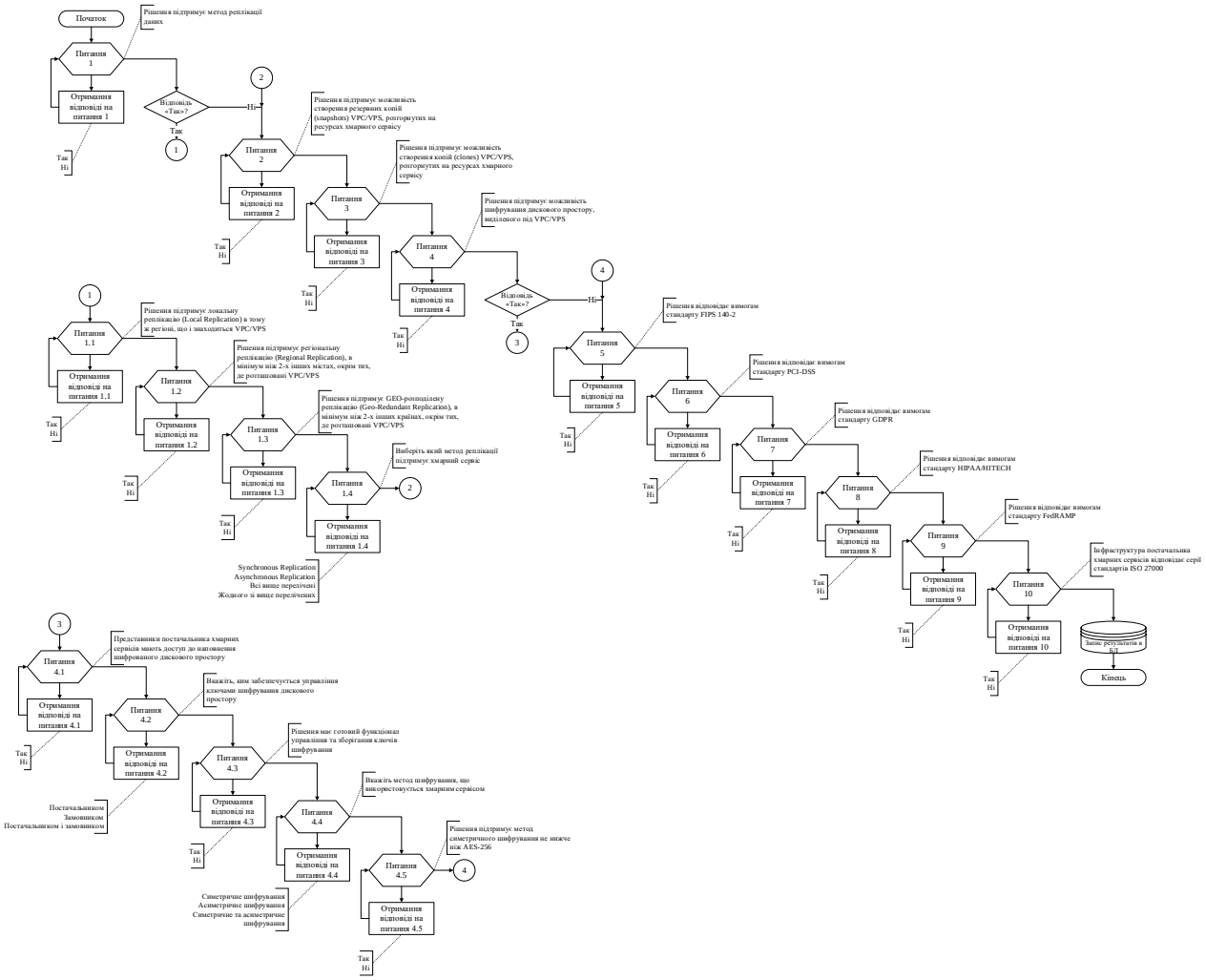


Рис. А.1. Топологія «Параметру S» для оцінювання модуля зберігання хмарного сервісу розробленим захищеним мережевим застосунком

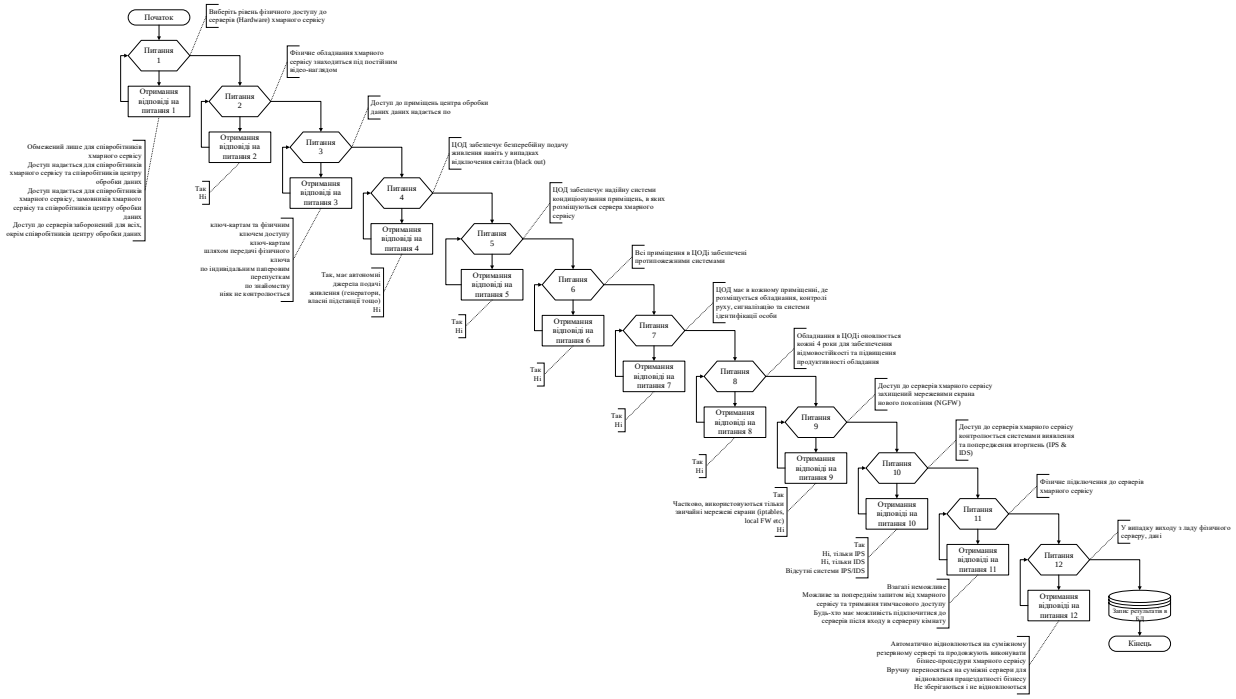


Рис. А.2. Топологія «Параметру SR» для оцінювання серверного модуля хмарного сервісу розробленим захищеним мережевим застосунком

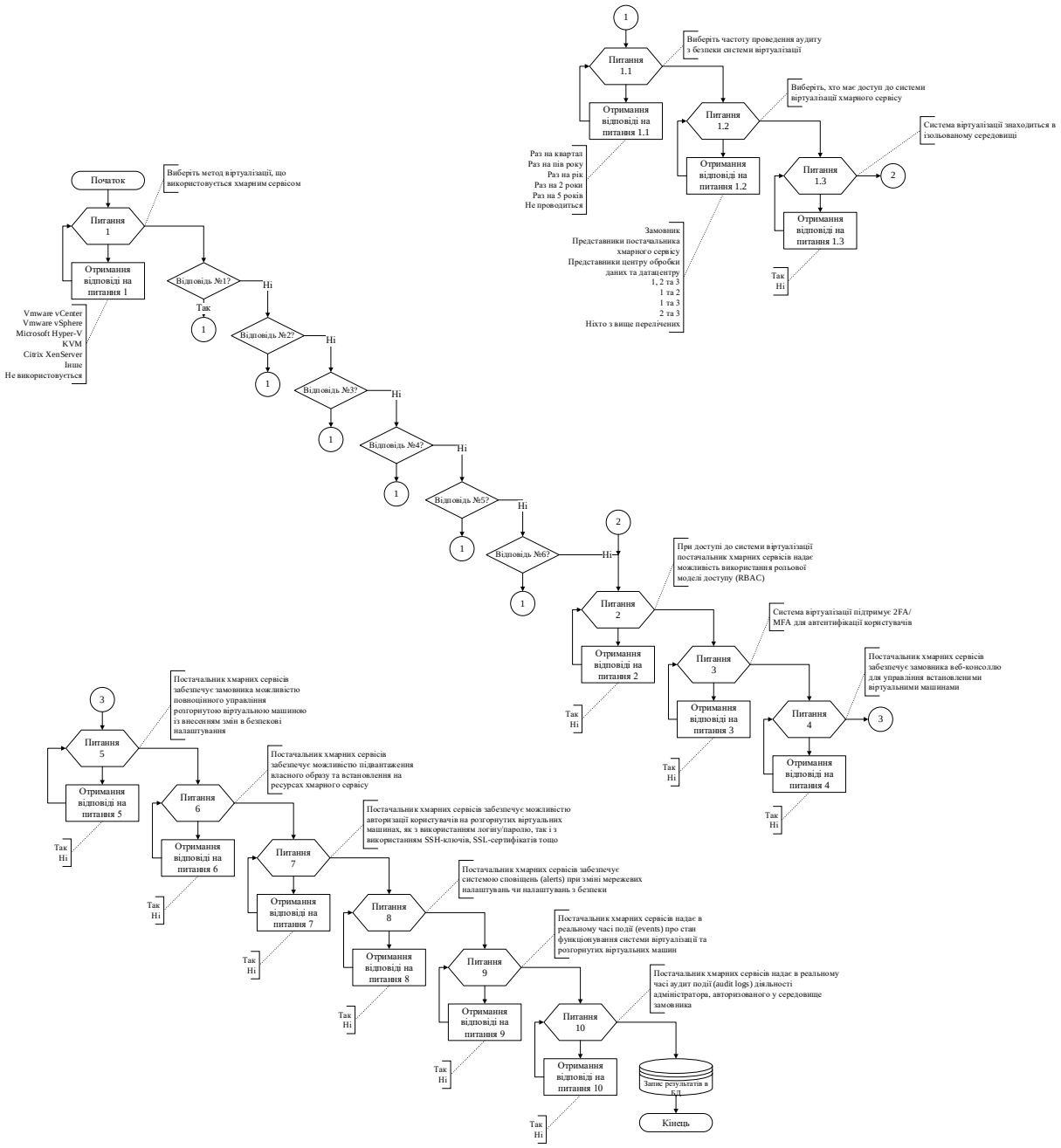


Рис. А.3. Топологія «Параметру V» для оцінювання модуля віртуалізація хмарного сервісу розробленим захищеним мережевим застосунком

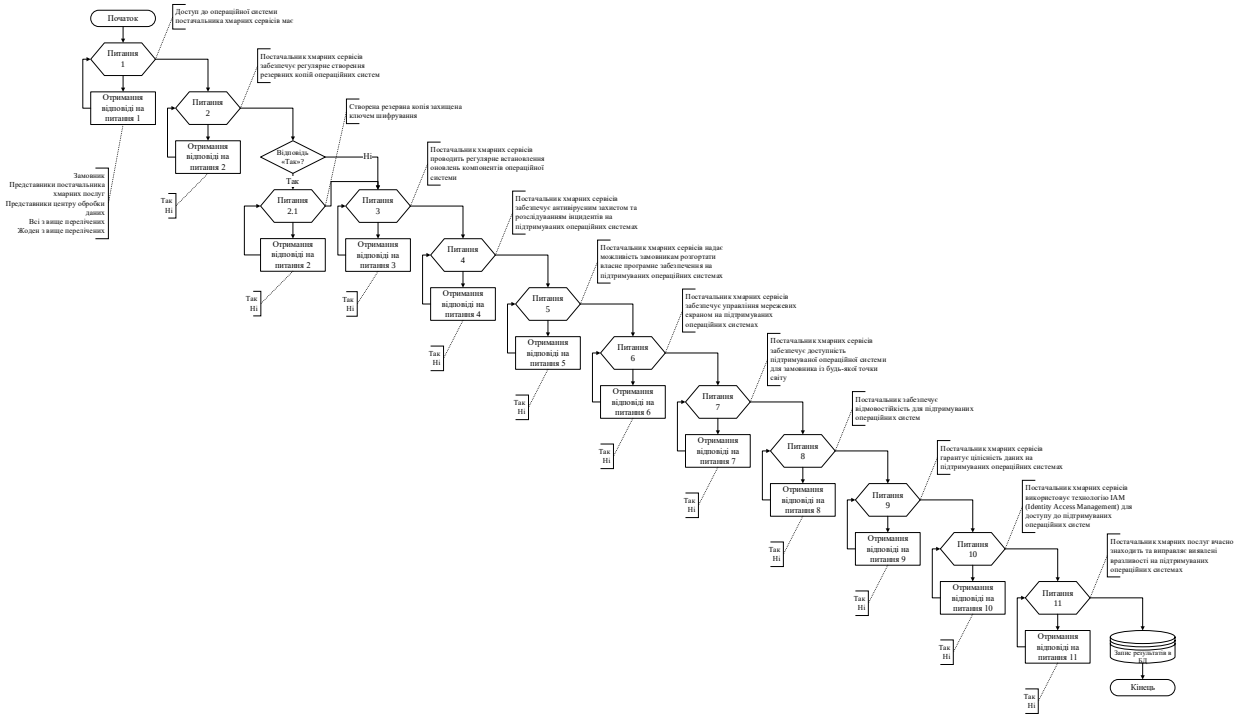


Рис. А.4. Топологія «Параметру OS» для оцінювання модуля операційної системи хмарного сервісу розробленим захищеним мережевим застосунком

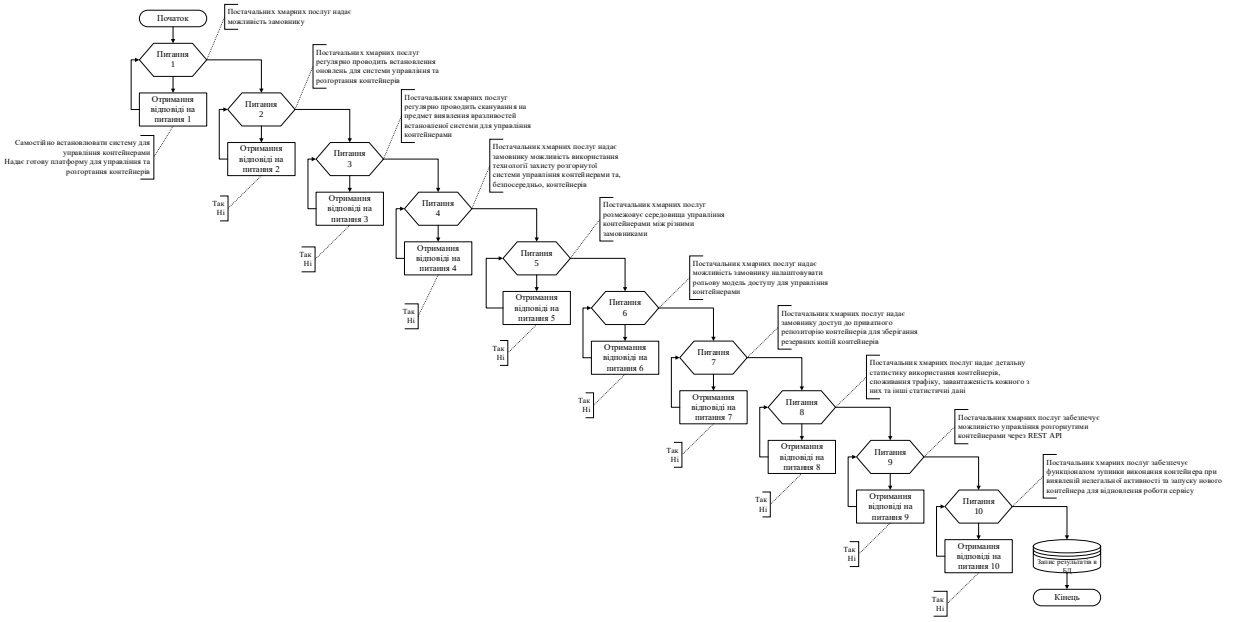


Рис. А.5. Топологія «Параметру CT» для оцінювання модуля контейнеризації хмарного сервісу розробленим захищеним мережевим застосунком

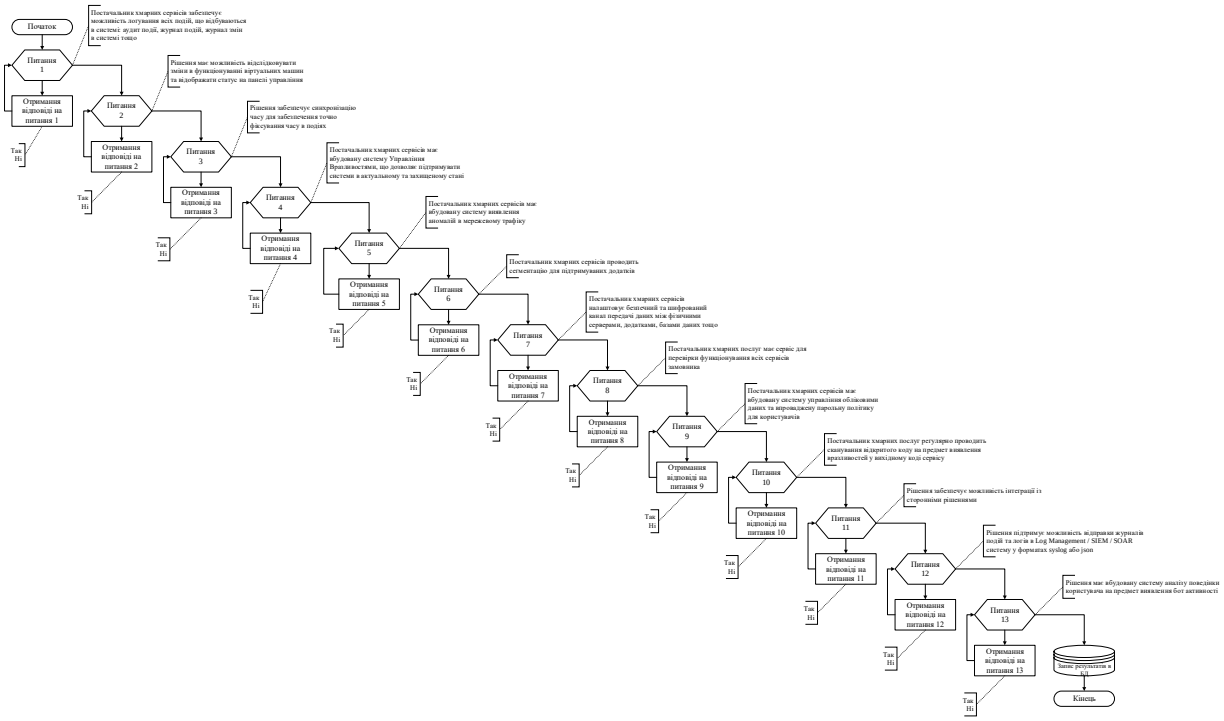


Рис. А.6. Топологія «Параметру R» для оцінювання модуля безперервної роботи хмарного сервісу розробленим захищеним мережевим застосунком

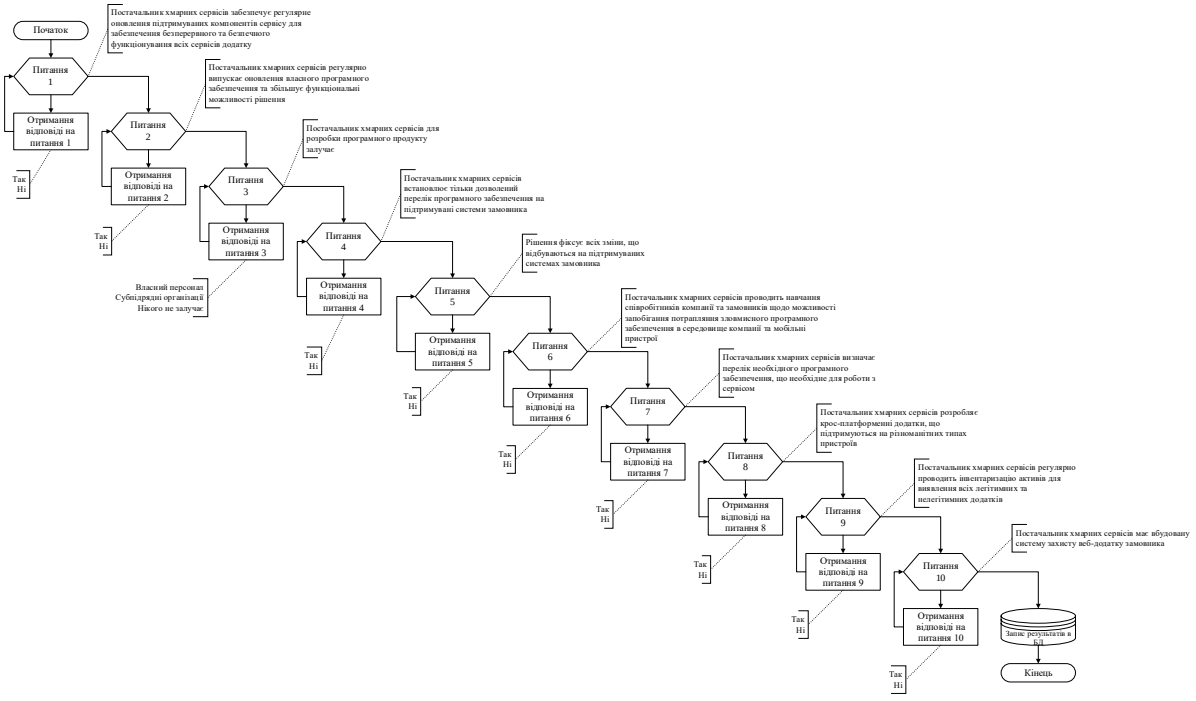


Рис. А.7. Топологія «Параметру A» для оцінювання модуль застосунків хмарного сервісу розробленим захищеним мережевим застосунком

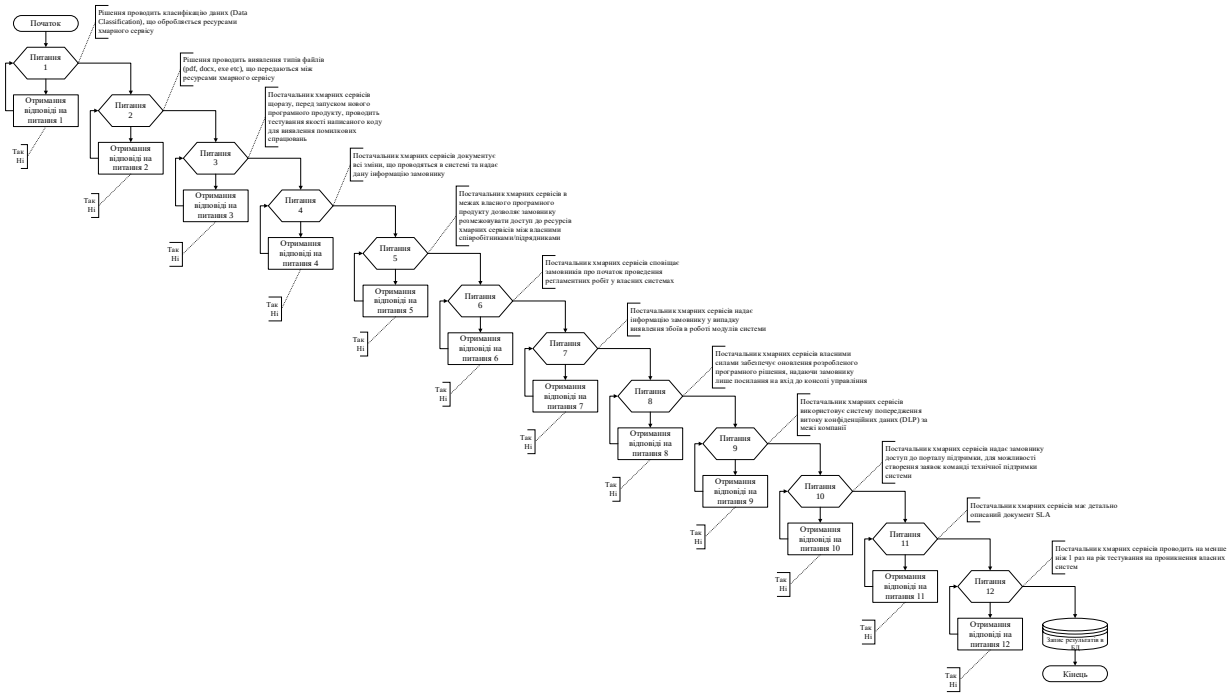


Рис. А.8. Топологія «Параметру D» для оцінювання модуль даних хмарного сервісу розробленим захищеним мережевим застосунком

Додаток Б

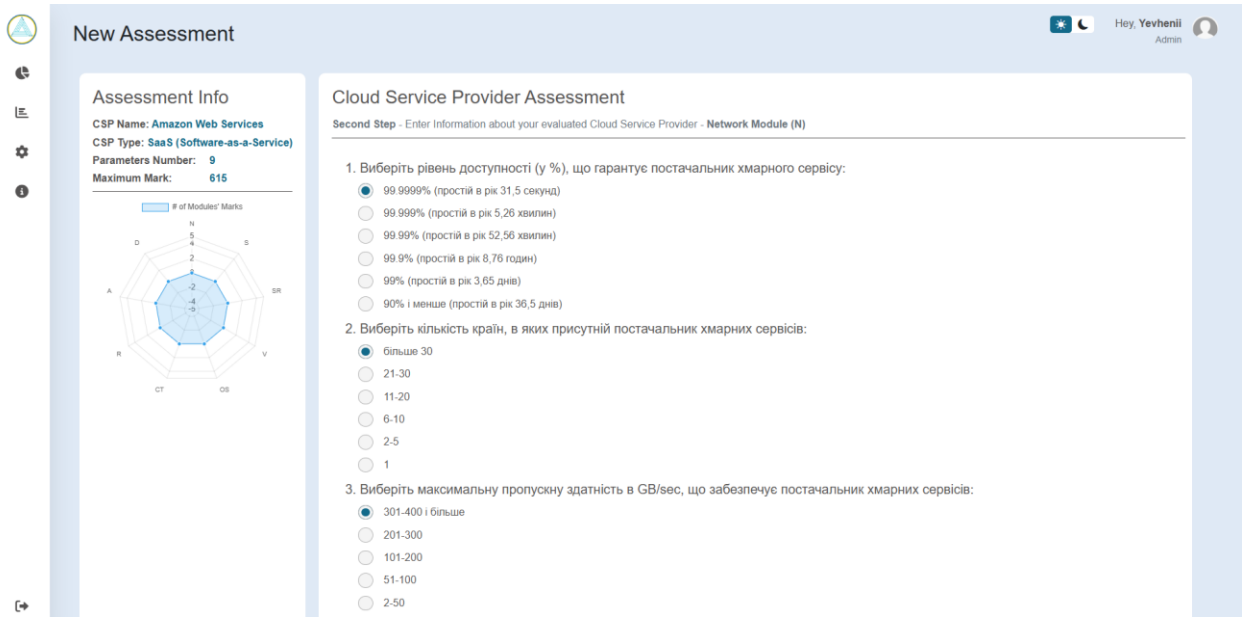


Рис. Б.1. Візуальне представлення переліку запитань для модуля оцінювання «Network Module»

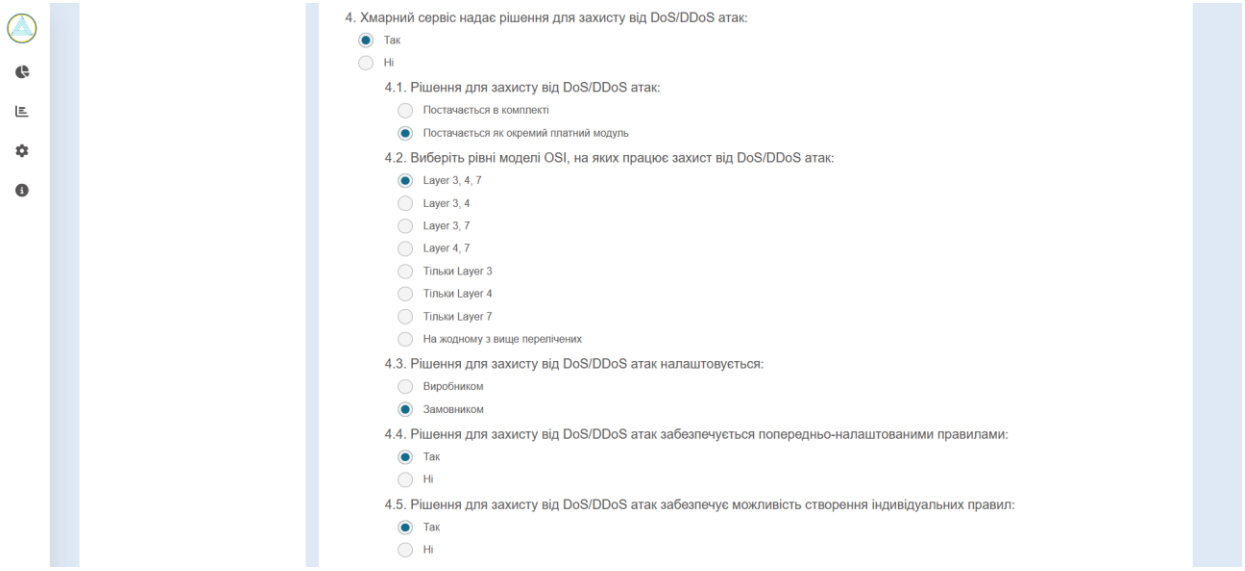


Рис. Б.2. Візуальне представлення переліку запитань для модуля оцінювання «Network Module»

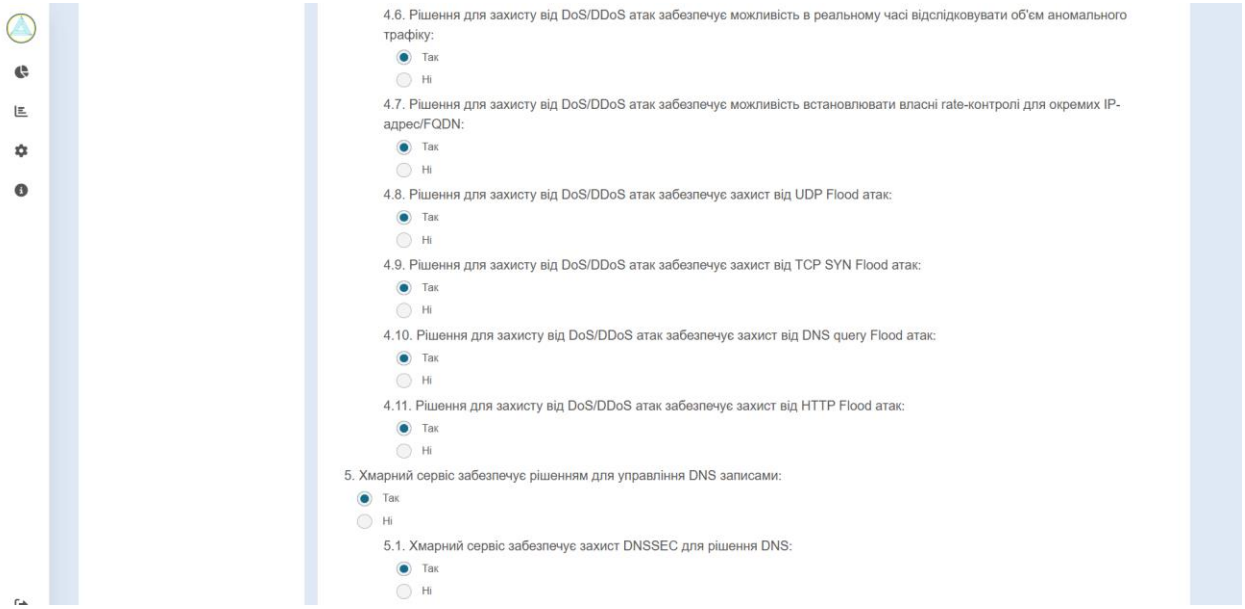


Рис. Б.3. Візуальне представлення переліку запитань для модуля оцінювання «Network Module»

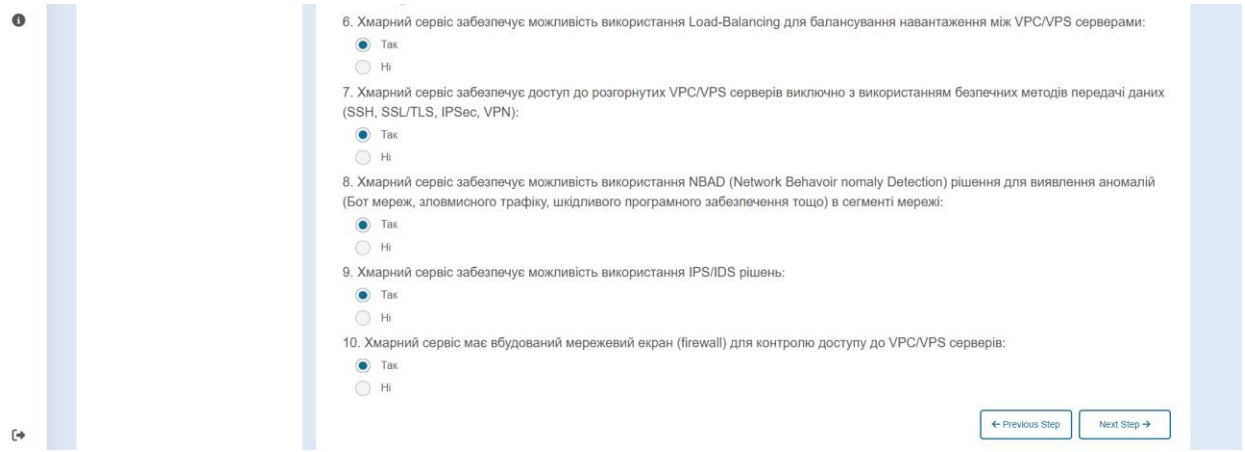


Рис. Б.4. Візуальне представлення переліку запитань для модуля оцінювання «Network Module»

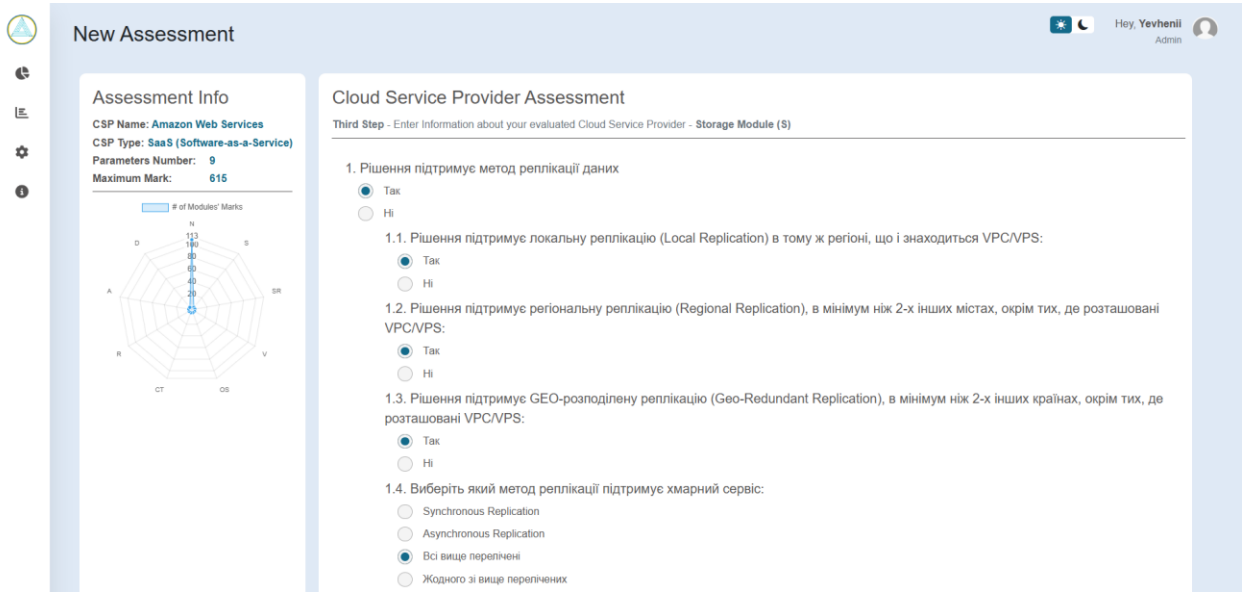


Рис. Б.5. Візуальне представлення переліку запитань для модуля оцінювання «Storage Module»

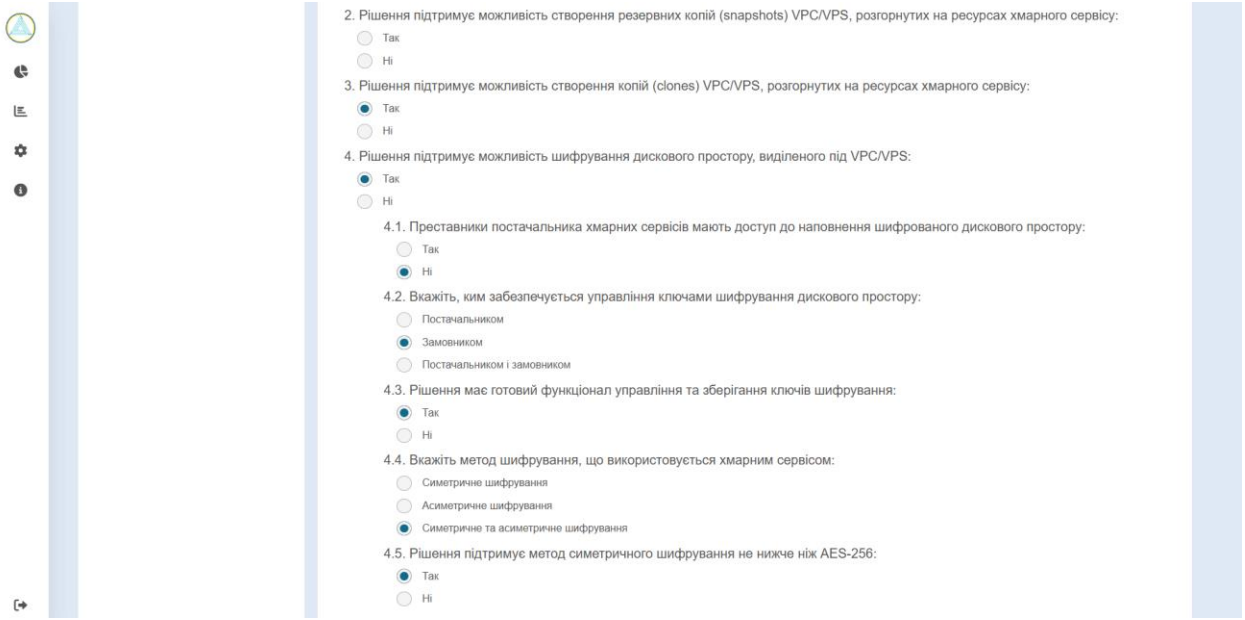


Рис. Б.6. Візуальне представлення переліку запитань для модуля оцінювання «Storage Module»

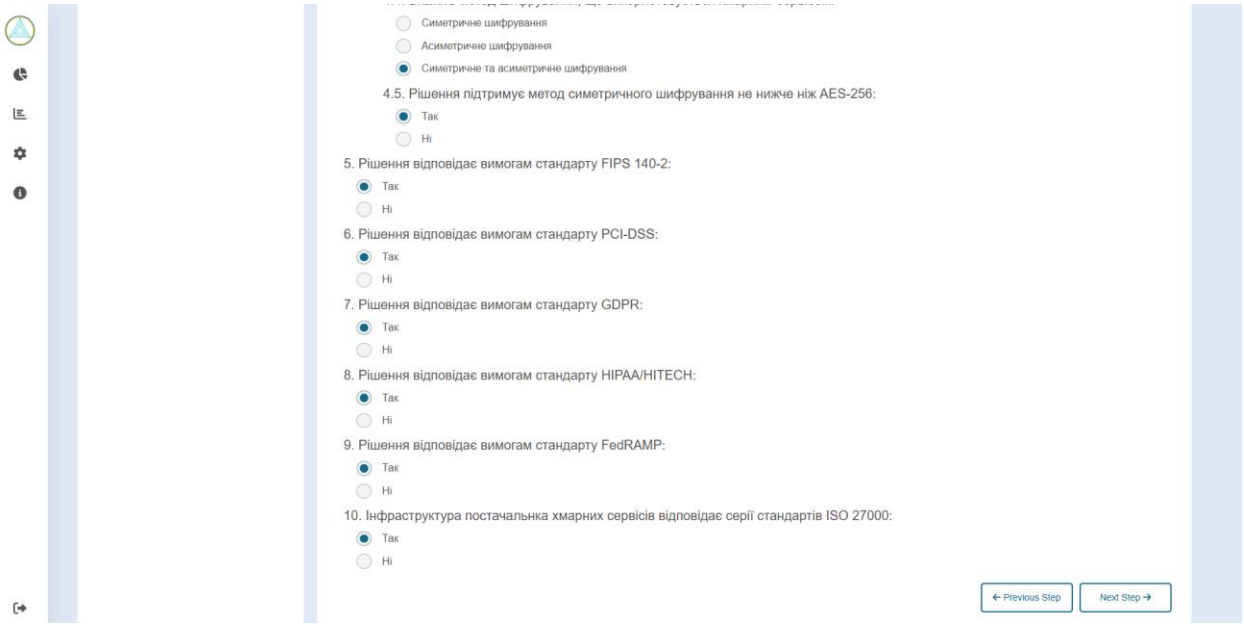


Рис. Б.7. Візуальне представлення переліку запитань для модуля оцінювання «Storage Module»

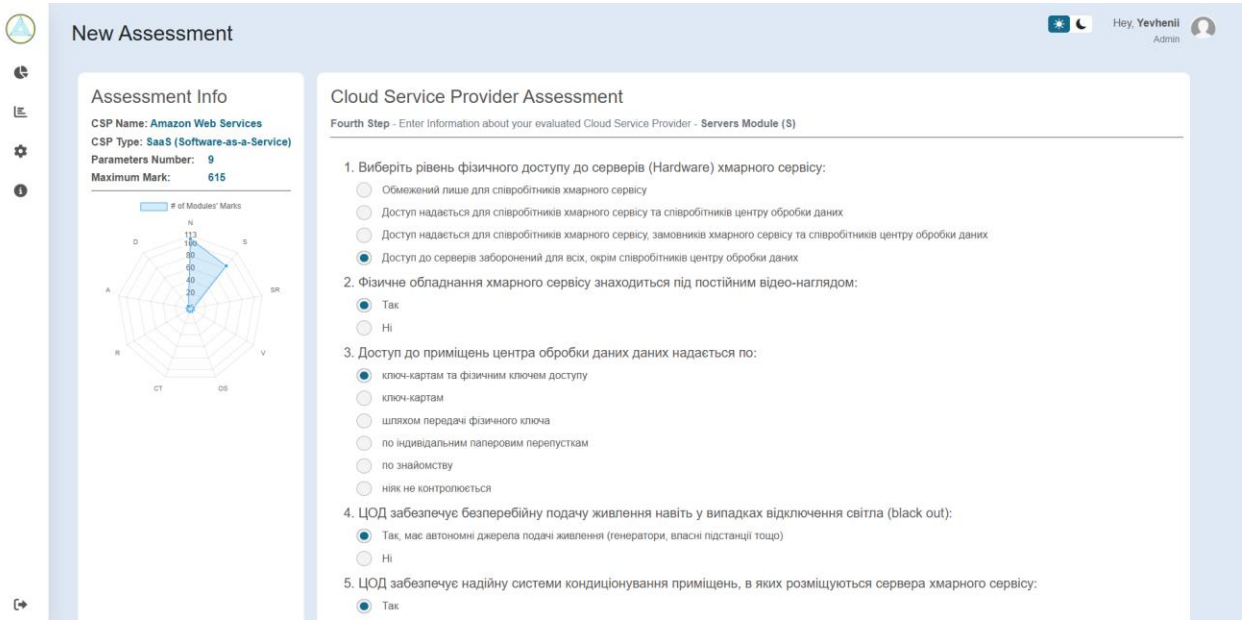


Рис. Б.8. Візуальне представлення переліку запитань для модуля оцінювання «Servers Module»

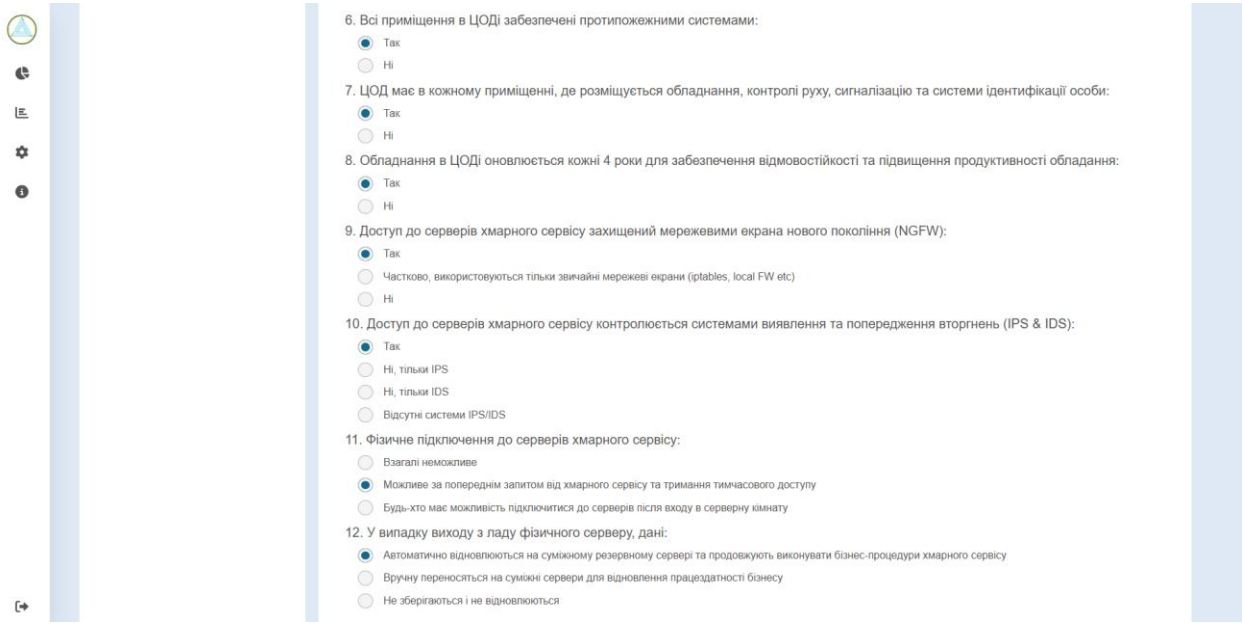


Рис. Б.9. Візуальне представлення переліку запитань для модуля оцінювання «Servers Module»

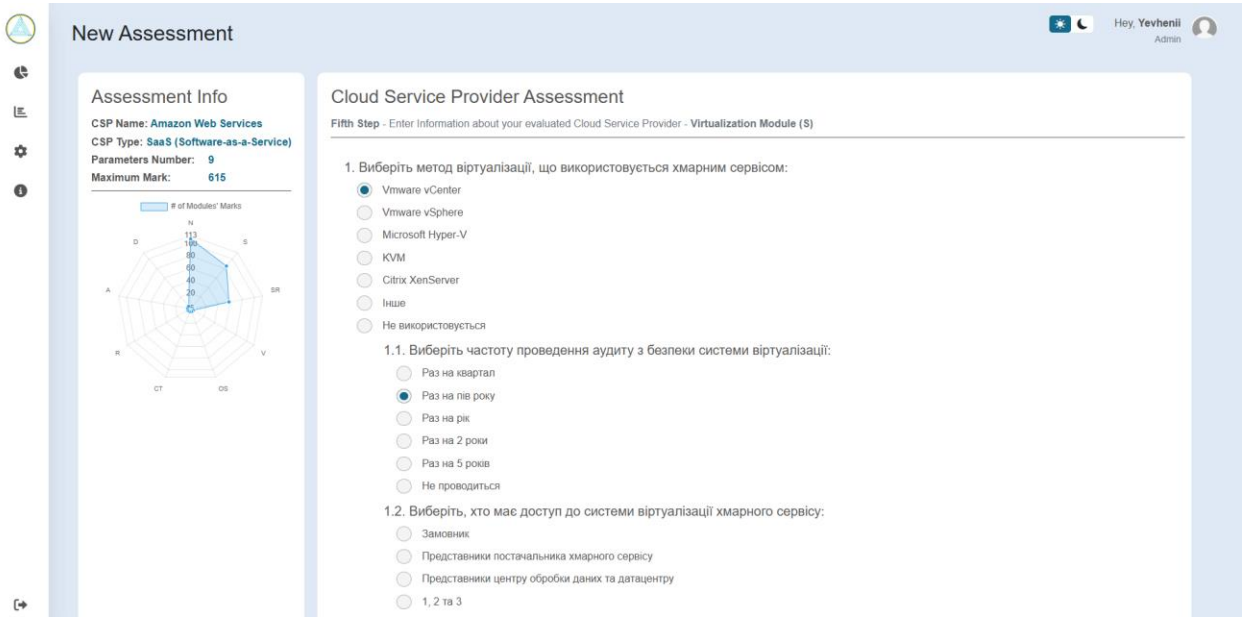


Рис. Б.10. Візуальне представлення переліку запитань для модуля оцінювання «Virtualization Module»

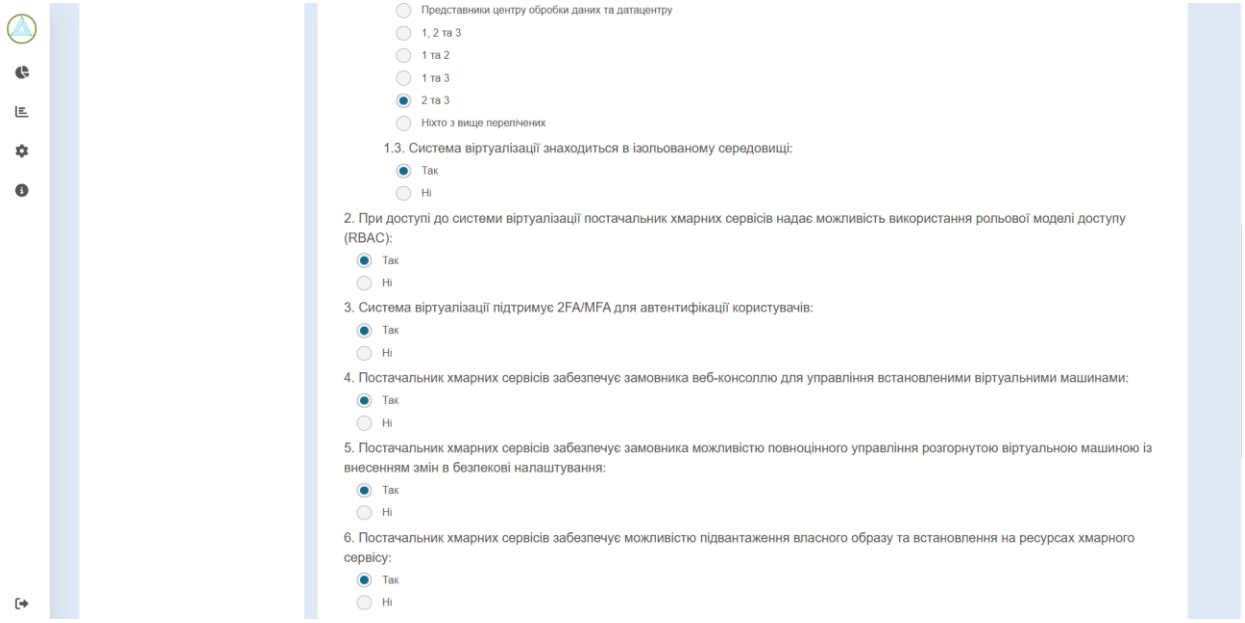


Рис. Б.11. Візуальне представлення переліку запитань для модуля оцінювання «Virtualization Module»

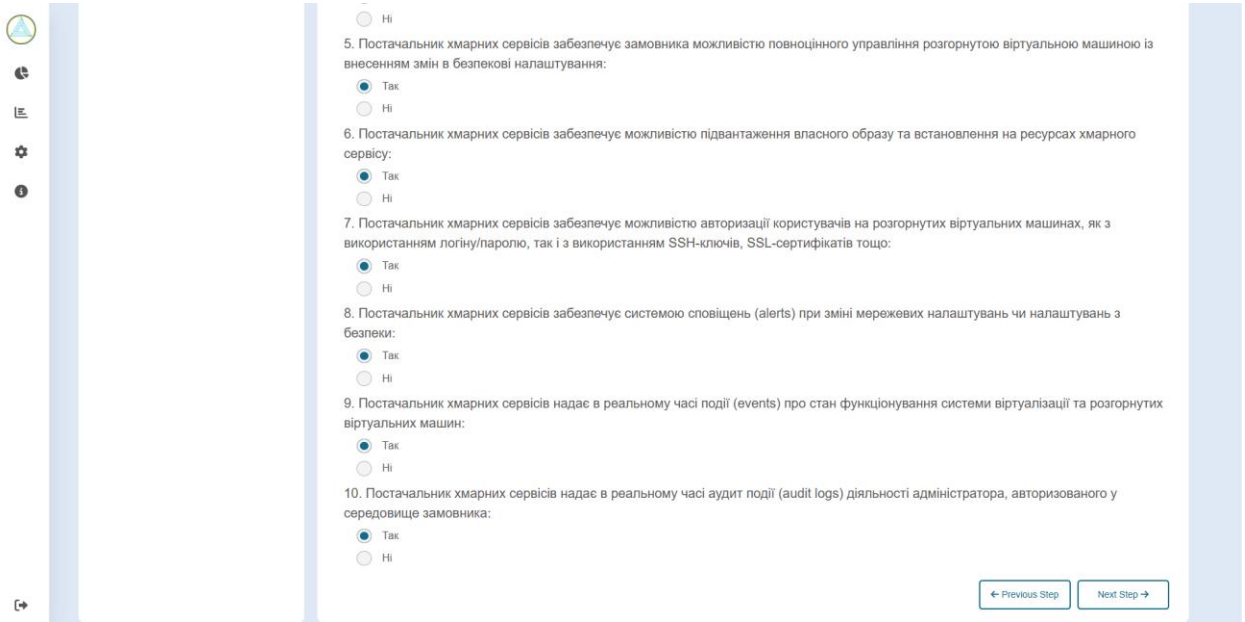


Рис. Б.12. Візуальне представлення переліку запитань для модуля оцінювання «Virtualization Module»

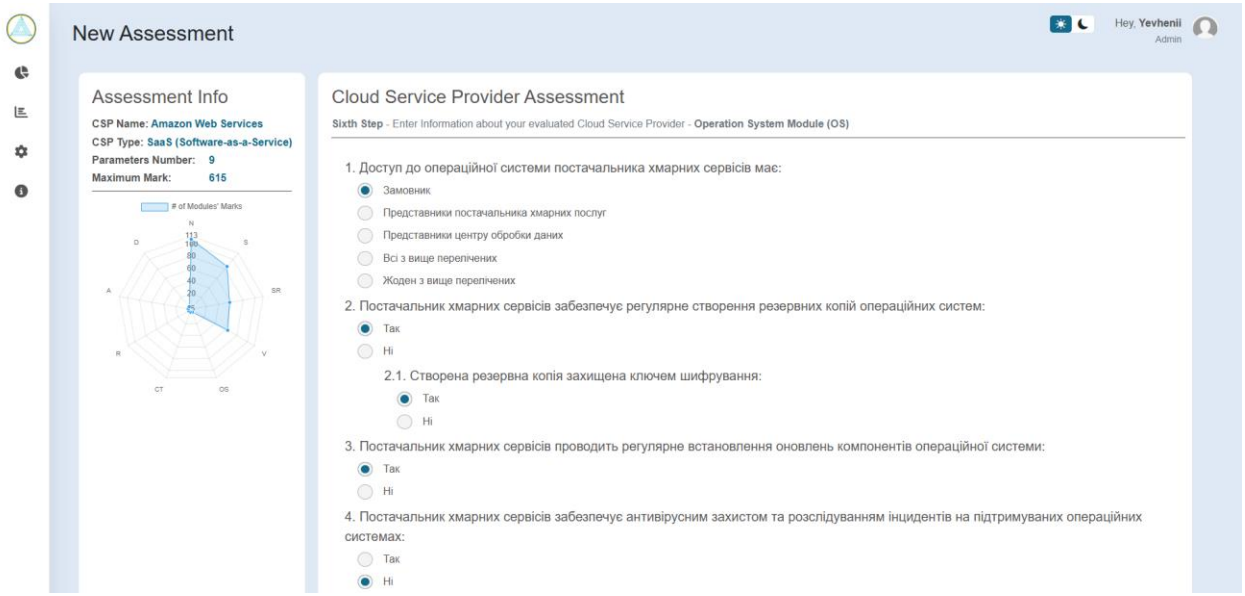


Рис. Б.13. Візуальне представлення переліку запитань для модуля оцінювання «Operation System Module»

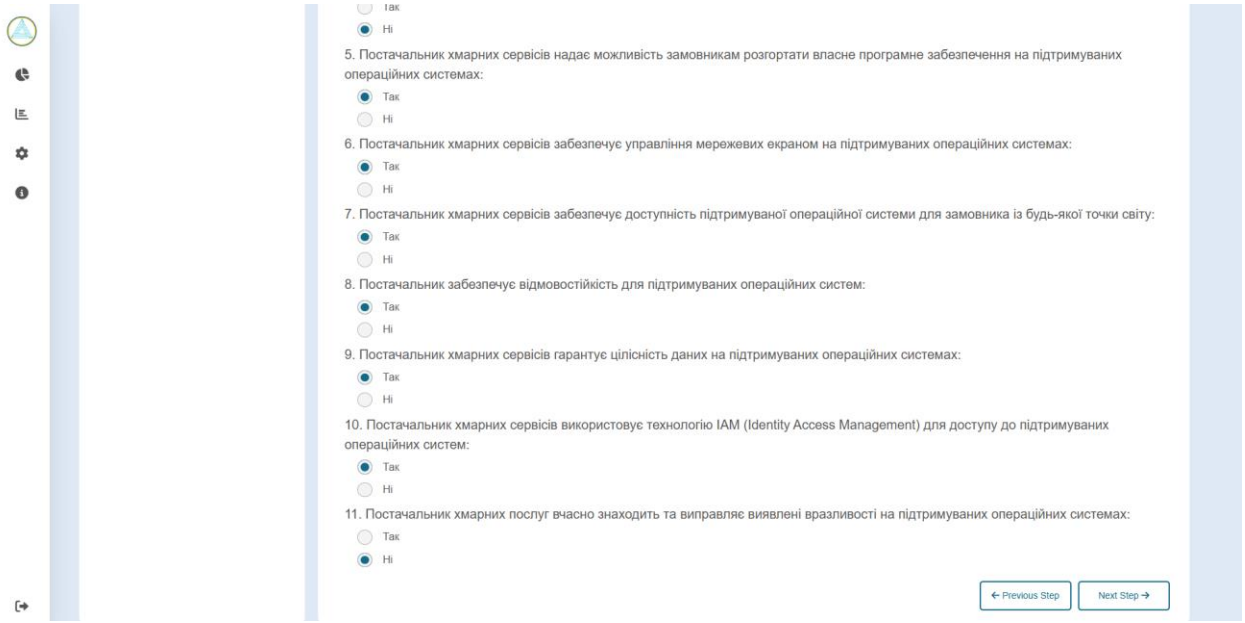


Рис. Б.14. Візуальне представлення переліку запитань для модуля оцінювання «Operation System Module»

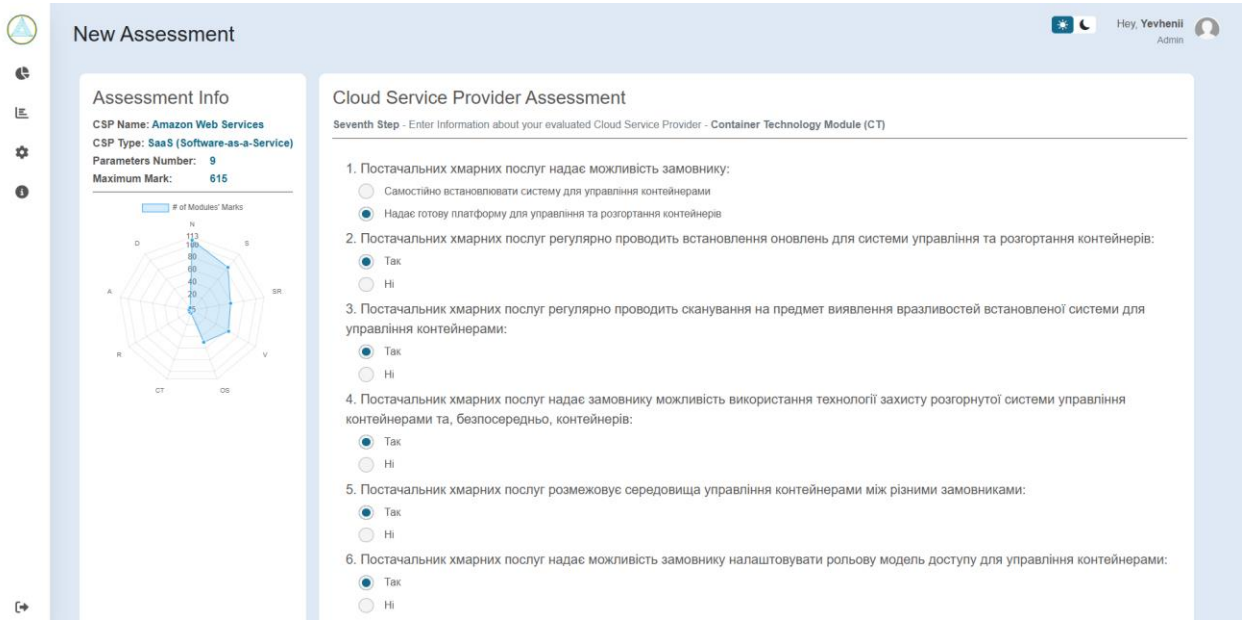


Рис. Б.15. Візуальне представлення переліку запитань для модуля оцінювання «Container Technology Module»

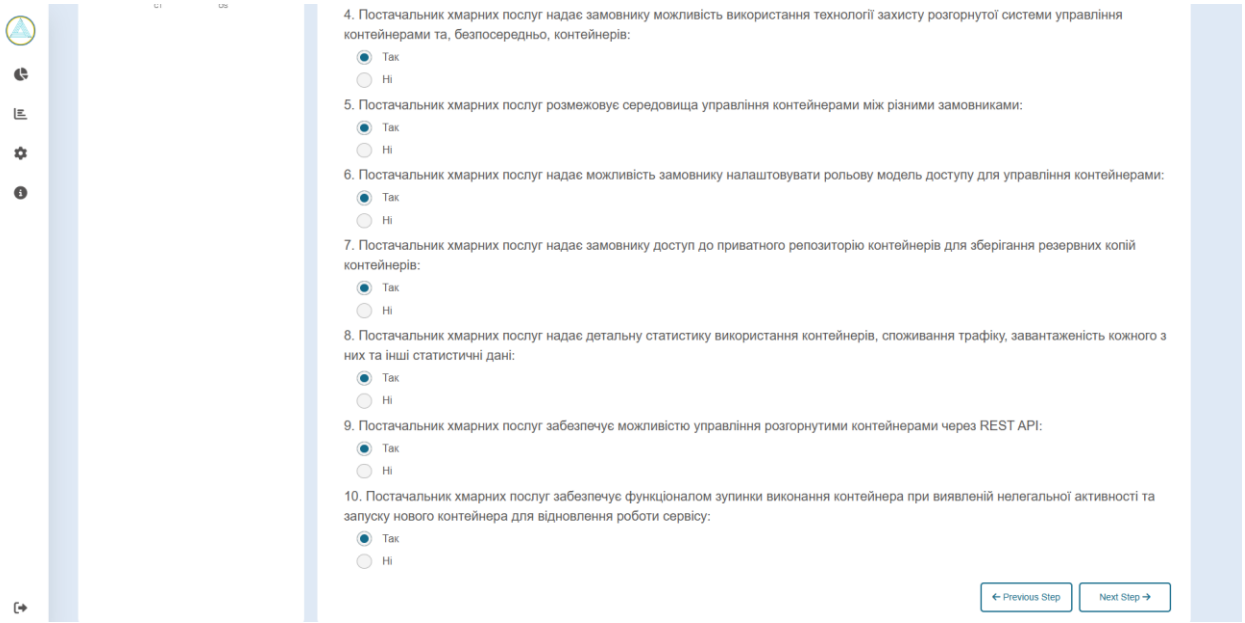


Рис. Б.16. Візуальне представлення переліку запитань для модуля оцінювання «Container Technology Module»

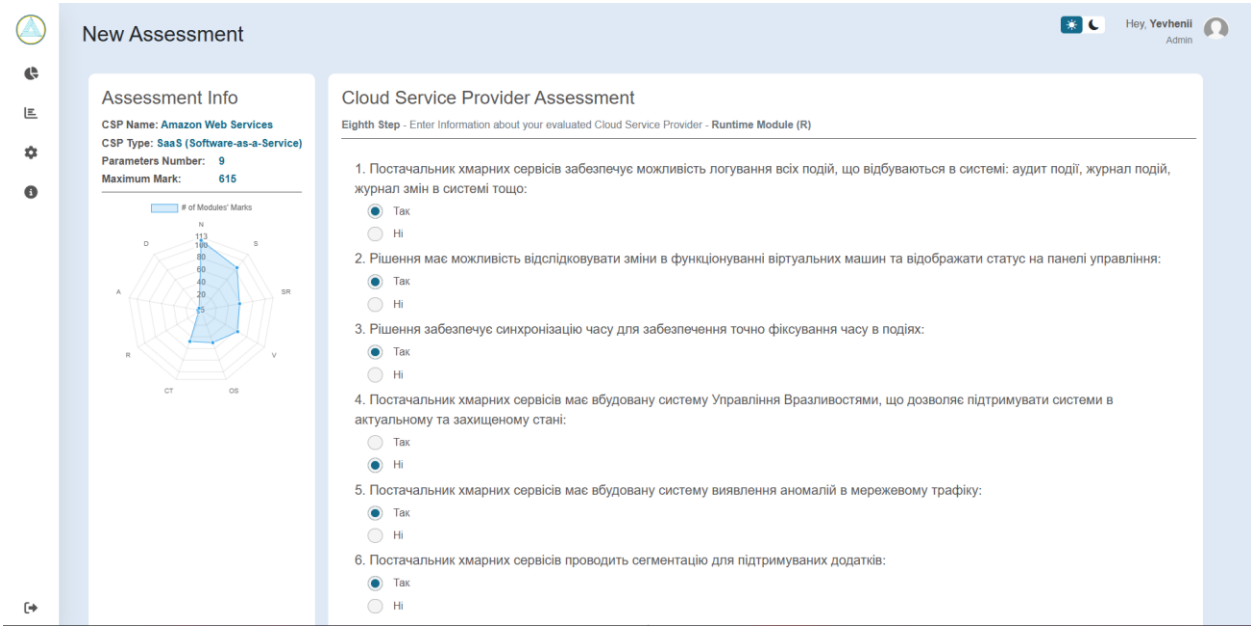


Рис. Б.17. Візуальне представлення переліку запитань для модуля оцінювання «Runtime Module»

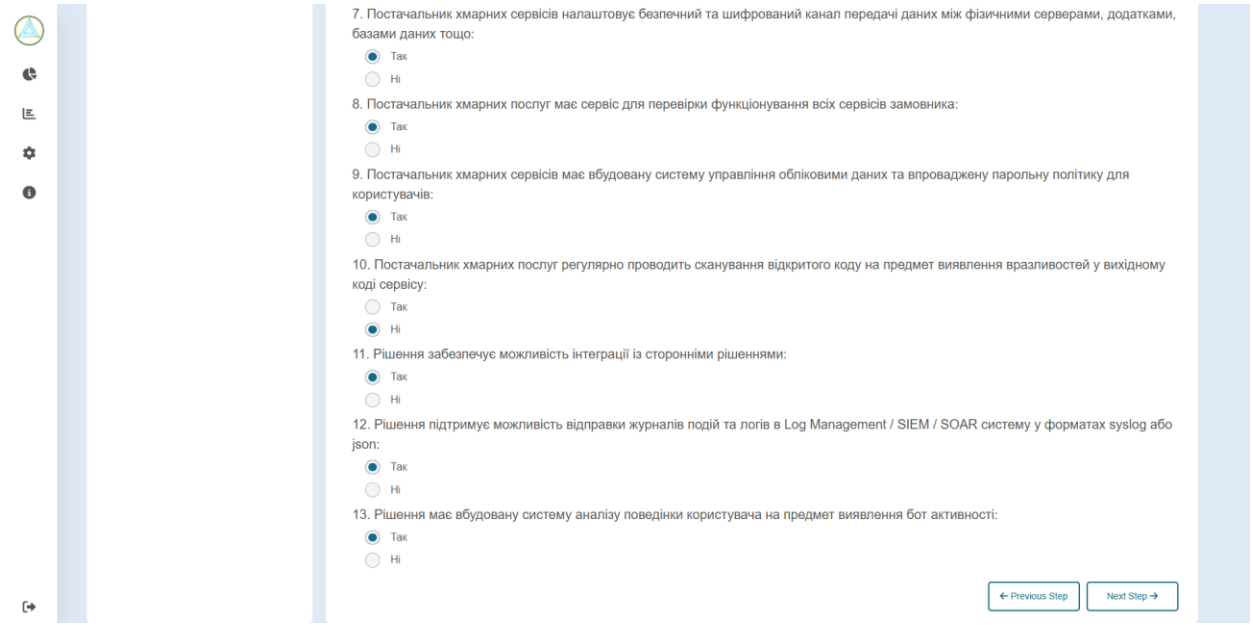


Рис. Б.18. Візуальне представлення переліку запитань для модуля оцінювання «Runtime Module»

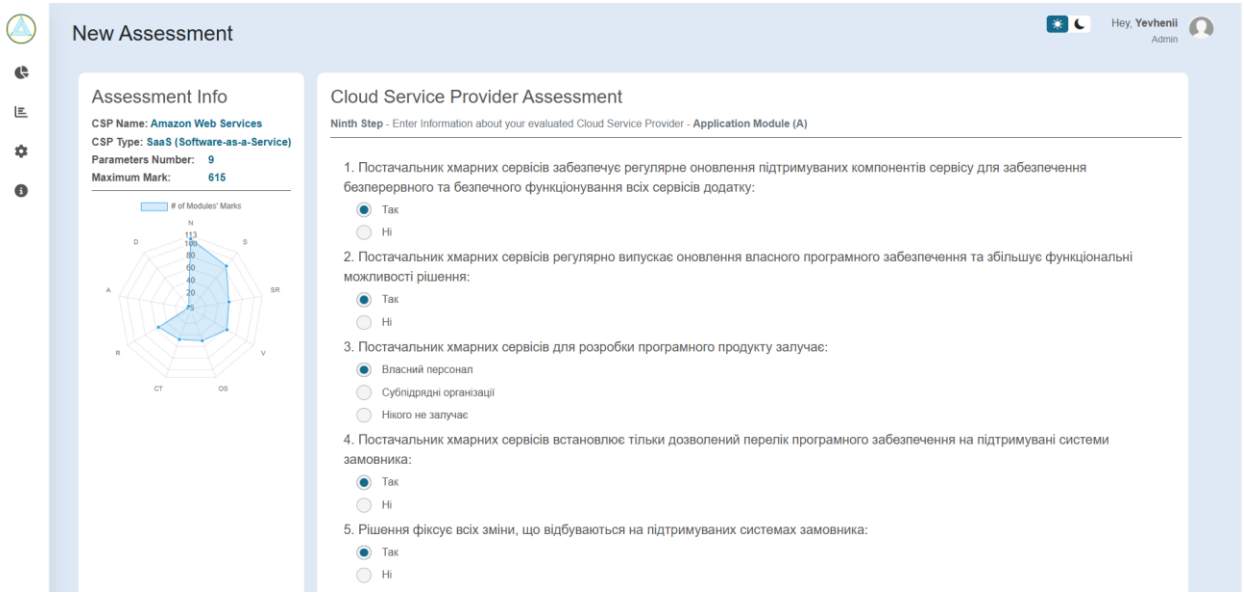


Рис. Б.19. Візуальне представлення переліку запитань для модуля оцінювання «Application Module»

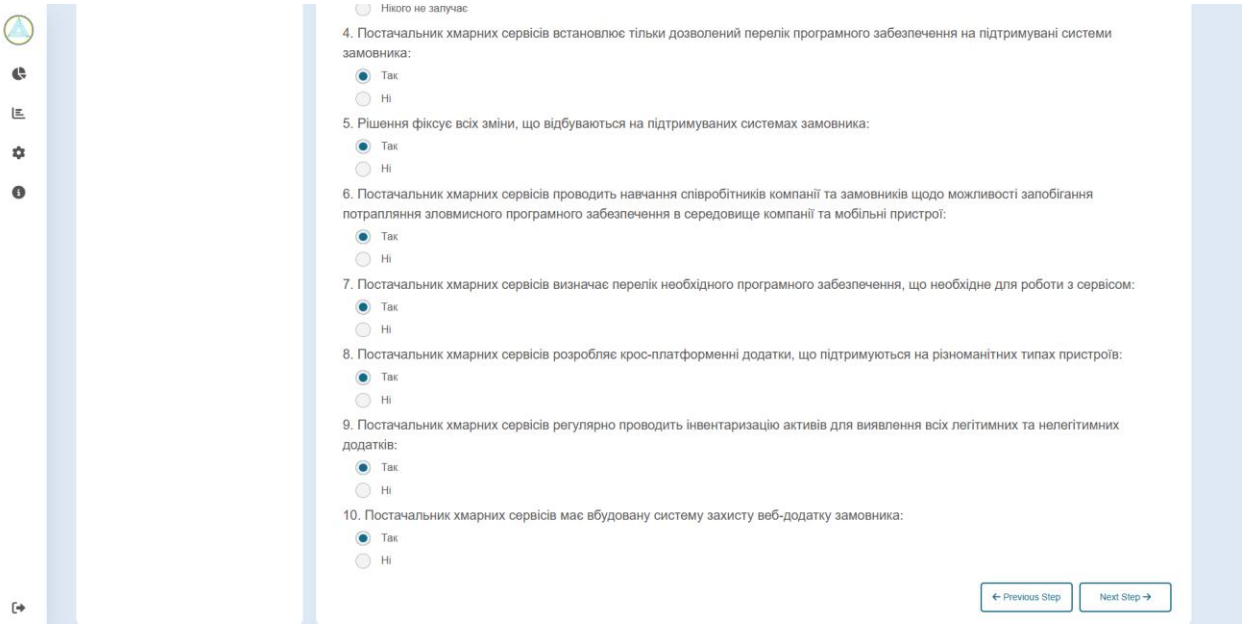


Рис. Б.20. Візуальне представлення переліку запитань для модуля оцінювання «Application Module»

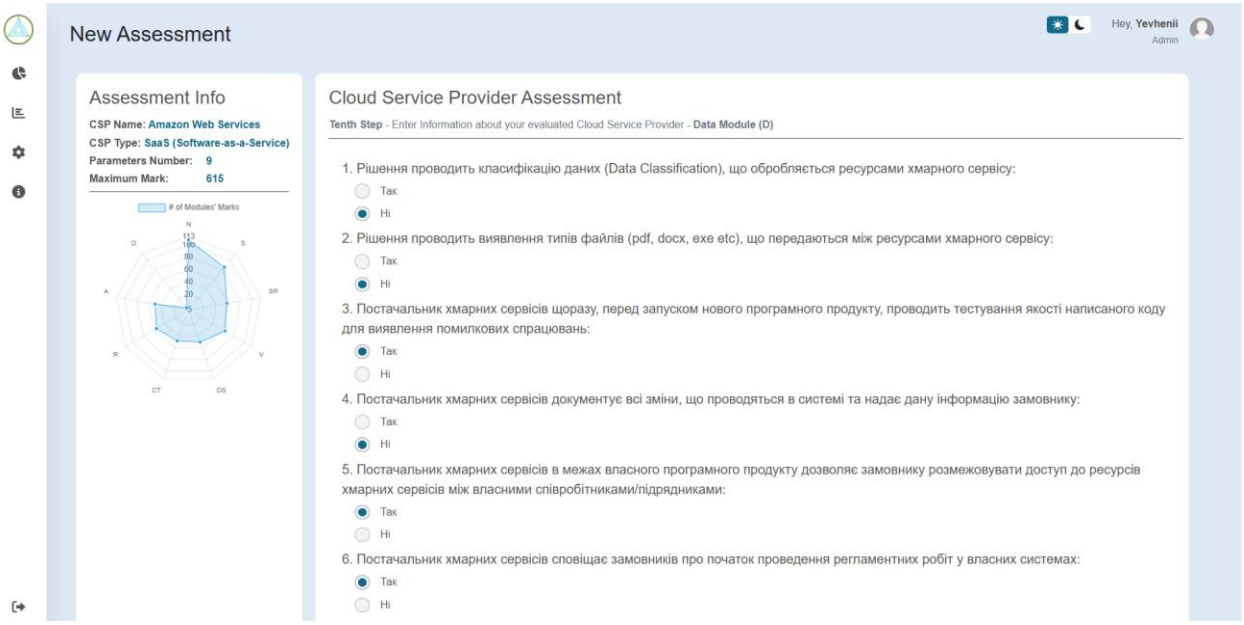


Рис. Б.21. Візуальне представлення переліку запитань для модуля оцінювання «Data Module»

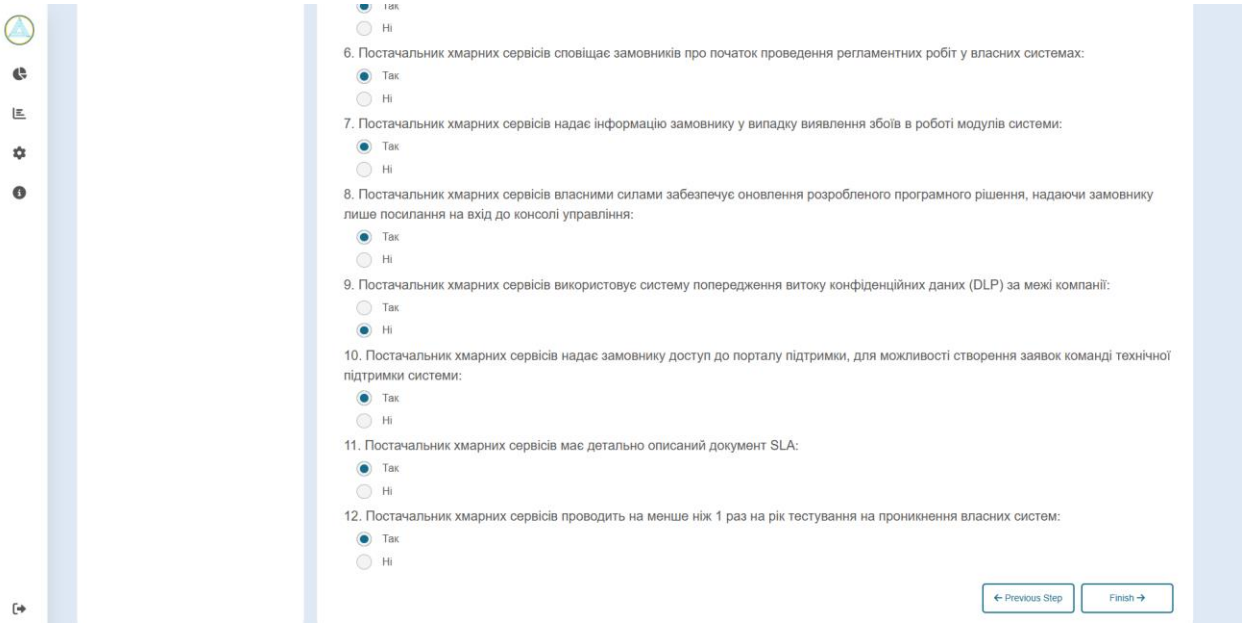
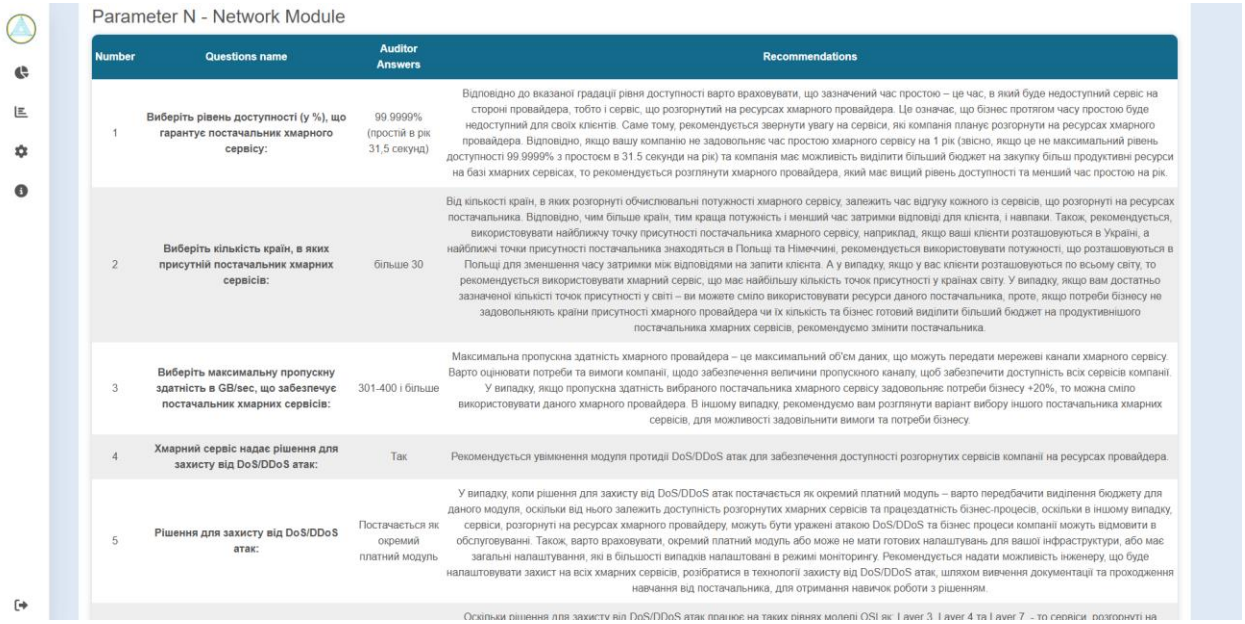


Рис. Б.22. Візуальне представлення переліку запитань для модуля оцінювання «Data Module»



Parameter N - Network Module

Number	Questions name	Auditor Answers	Recommendations
1	**Виберіть рівень доступності (у %), що гарантує постачальник хмарного сервісу:**	99.9999% (простій в рік 31,5 секунд)	Відповідно до вказаної градації рівня доступності варто враховувати, що зазначений час простою – це час, в який буде недоступний сервіс на стороні провайдера, тобто і сервіс, що розгорнутий на ресурсах хмарного провайдера. Це означає, що бізнес протягом часу простою буде недоступний для своїх клієнтів. Саме тому, рекомендується звернути увагу на сервіси, які компанія планує розгорнути на ресурсах хмарного провайдера. Відповідно, якщо вашу компанію не задовольняє час простою хмарного сервісу на 1 рік (звісно, якщо це не максимальний рівень доступності 99.9999% з простоєм в 31.5 секунди на рік) та компанія має можливість виділити більший бюджет на закупку більш продуктивні ресурси на базі хмарних сервісах, то рекомендується розглянути хмарного провайдера, який має вищий рівень доступності та менший час простою на рік.
2	**Виберіть кількість країн, в яких присутній постачальник хмарних сервісів:**	більше 30	Від кількості країн, в яких розгорнуті обчислювальні потужності хмарного сервісу, залежить час відгуку кожного із сервісів, що розгорнуті на ресурсах постачальника. Відповідно, чим більше країн, тим краща потужність і менший час затримки відповіді для клієнта, і навпаки. Також, рекомендується, використовувати найближчу точку присутності постачальника хмарного сервісу, наприклад, якщо ваші клієнти розташовуються в Україні, а найближчі точки присутності постачальника знаходяться в Польщі та Німеччині, рекомендується використовувати потужності, що розташовуються в Польщі для зменшення часу затримки між відповідями на запити клієнта. А у випадку, якщо у вас клієнти розташовуються по всьому світу, то рекомендується використовувати хмарний сервіс, що має найбільшу кількість точок присутності у країнах світу. У випадку, якщо вам достатньо зазначеної кількості точок присутності у світі – ви можете сміло використовувати ресурси даного постачальника, проте, якщо потреби бізнесу не задовольняють країни присутності хмарного провайдера чи їх кількість та бізнес готовий виділити більший бюджет на продуктивнішого постачальника хмарних сервісів, рекомендуємо змінити постачальника.
3	**Виберіть максимальну пропускну здатність в GB/sec, що забезпечує постачальник хмарних сервісів:**	301-400 і більше	Максимальна пропускна здатність хмарного провайдера – це максимальний об'єм даних, що можуть передати мережеві канали хмарного сервісу. Варто оцінювати потреби та вимоги компанії, щодо забезпечення величини пропускного каналу, щоб забезпечити доступність всіх сервісів компанії. У випадку, якщо пропускна здатність вибраного постачальника хмарного сервісу задовольняє потреби бізнесу +20%, то можна сміло використовувати даного хмарного провайдера. В іншому випадку, рекомендуємо вам розглянути варіант вибору іншого постачальника хмарних сервісів, для можливості задовільнити вимоги та потреби бізнесу.
4	**Хмарний сервіс надає рішення для захисту від DoS/DDoS атак:**	Так	Рекомендується увімкнення модуля протидії DoS/DDoS атак для забезпечення доступності розгорнутих сервісів компанії на ресурсах провайдера.
5	**Рішення для захисту від DoS/DDoS атак:**	Постачається як окремий платний модуль	У випадку, коли рішення для захисту від DoS/DDoS атак постачається як окремий платний модуль – варто передбачити виділення бюджету для даного модуля, оскільки від нього залежить доступність розгорнутих хмарних сервісів та працездатність бізнес-процесів, оскільки в іншому випадку, сервіси, розгорнуті на ресурсах хмарного провайдеру, можуть бути уражені атакою DoS/DDoS та бізнес процеси компанії можуть відмовити в обслуговуванні. Також, варто враховувати, окремий платний модуль або може не мати готових налаштувань для вашої інфраструктури, або має загальні налаштування, які в більшості випадків налаштовані в режимі моніторингу. Рекомендується надати можливість інженеру, що буде налаштовувати захист на всіх хмарних сервісів, розібратися в технології захисту від DoS/DDoS атак, шляхом вивчення документації та проходження навчання від постачальника, для отримання навичок роботи з рішенням.
6	**Виберіть рівні моделі OSI, на яких працює захист від DoS/DDoS атак:**	Layer 3, 4, 7	Оскільки рішення для захисту від DoS/DDoS атак працює на таких рівнях моделі OSI як: Layer 3, Layer 4 та Layer 7, - то сервіси, розгорнуті на ресурсах хмарного провайдера будуть мати захист від: GET Floods, Slow POST, Slowloris тощо (L7); DNS query flood, DNS UDP flood, SSL flood, SYN flood, Smurf DDoS, Ping-Of-Death тощо (L4); UDP flood, ICMP flood, ACK flood, Ping flood тощо (L3). Оскільки даний модуль захисту від DoS/DDoS атак має повноцінний набір захисту, рекомендуємо приділити увагу коректному налаштуванню даного сервісу відповідно під потреби та можливості бізнес процесів компанії, оскільки в іншому випадку, наявність широкого спектру налаштувань жодним чином не допоможе попередити атаки даного типу.
7	**Рішення для захисту від DoS/DDoS атак налаштовується:**	Замовником	Перед початком встановлення налаштувань, рекомендується надати час інженеру, що буде займатися налаштуванням захисту сервісів, розгорнутих на ресурсах хмарних сервісів, дослідити функціонал рішення із залученням інтегратора чи розробника. Додатково, рекомендується забезпечити навчання інженеру по роботі із даним рішенням, щоб навчити співробітника роботі із даним модулем захисту від DoS/DDoS атак.
8	**Рішення для захисту від DoS/DDoS атак забезпечується попередньо-налаштованими правилами:**	Так	У випадку, якщо попередньо-налаштовані правила – це лише шаблон, який можна змінювати, то варто внести зміни під функціональні можливості бізнес процесів, що функціонують на ресурсах хмарних сервісів, оскільки попередньо-налаштовані правила не у всіх випадках працює коректно і можуть провокувати false-positive спрацювання.
9	**Рішення для захисту від DoS/DDoS атак забезпечує можливість створення індивідуальних правил:**	Так	Рекомендується, перед створенням індивідуальних правил захисту від DoS/DDoS атак, скористатися дослідженням можливостей бізнес процесів, що розгорнуті на ресурсах хмарних сервісів для можливості побудови коректних правил захисту та зменшення false-positive спрацювань.
10	**Рішення для захисту від DoS/DDoS атак забезпечує можливість в реальному часі відслідковувати об'єм аномального трафіку:**	Так	В даному випадку, у випадку недостатньої видимості попередньо налаштованої аналітикою на стороні хмарного провайдера, рекомендується побудувати власні інформаційні панелі, або направити події на вашу SIEM систему, або скористатися рішенням, наприклад, Grafana, для можливості побудови індивідуальних інформаційних панелей для забезпечення кращої видимості подій та трафіку.»
11	**Рішення для захисту від DoS/DDoS атак забезпечує можливість встановлювати власні rate-контролі для окремих IP-адрес/FQDN:**	Так	Рекомендується, перед створенням індивідуальних rate-контролів захисту від DoS/DDoS атак, скористатися дослідженням можливостей бізнес процесів, що розгорнуті на ресурсах хмарних сервісів для можливості побудови коректних rate-контролів захисту та зменшення false-positive спрацювань та попередження блокування легітимних запитів користувачів сервісів.
12	**Рішення для захисту від DoS/DDoS атак забезпечує захист від UDP Flood атак:**	Так	Рекомендується увімкнути модуль захисту від UDP Flood атак.
13	**Рішення для захисту від DoS/DDoS атак забезпечує захист від TCP SYN Flood атак:**	Так	Рекомендується увімкнути модуль захисту від TCP SYN Flood атак.
14	**Рішення для захисту від DoS/DDoS атак забезпечує захист від DNS query Flood атак:**	Так	Рекомендується увімкнути модуль захисту від DNS query flood атак.

Рис. Б.23. Візуальне представлення переліку рекомендацій для модуля оцінювання «Network Module»

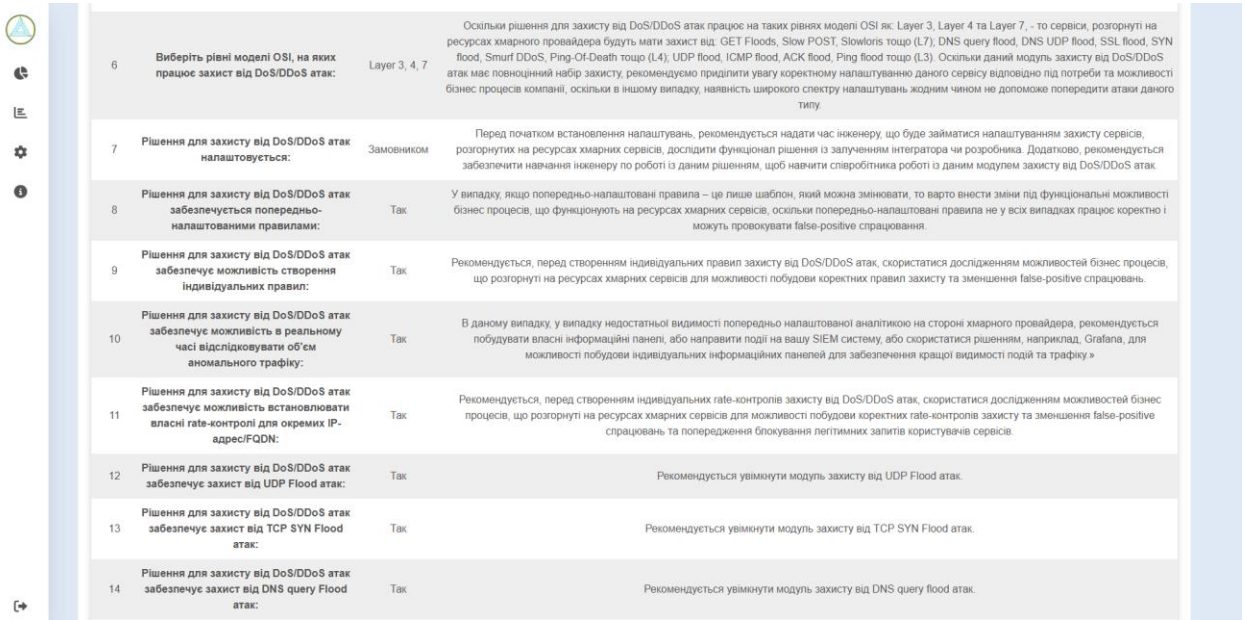


Рис. Б.24. Візуальне представлення переліку рекомендацій для модуля оцінювання «Network Module»

15	**Рішення для захисту від DoS/DDoS атак забезпечує захист від HTTP Flood атак:**	Так	Рекомендується увімкнути модуль захисту від HTTP flood атак.
16	**Хмарний сервіс забезпечує рішенням для управління DNS записами:**	Так	Для доцільності управління DNS записами, рекомендується скористатися можливістю управління DNS записами на рівні хмарного провайдера, як Primary зоною, за для можливості реалізації всіх бізнес-потреб, що вимагаються від сервісу управління DNS записами. Або скористатися можливістю використання даного сервісу, як Secondary зони, у випадку недоступності зміни Primary зони.
17	**Хмарний сервіс забезпечує захист DNSSEC для рішення DNS:**	Так	Незалежно від налаштувань DNS (як Primary чи Seocndary), рекомендується налаштувати захист DNSSEC для можливості захисту запитів на рівні DNS та перевірки цілісності та легітимності запитів, що передаються.
18	**Хмарний сервіс забезпечує можливість використання Load-Balancing для балансування навантаження між VPC/VPS серверами:**	Так	Рекомендується розгорнути копію критичних бізнес сервісів компанії та за допомогою вбудованого Load-Balancing модуля налаштувати балансування між декілька копіями ваших сервісів, для забезпечення роботи відмовостійкості розгорнутого сервісу. У випадку, якщо даний сервіс (LB) тарифікується окремо – варто розрахувати вартість та додати його до закупівлі для забезпечення відмовостійкого функціонування критичних бізнес процесів компанії.
19	**Хмарний сервіс забезпечує доступ до розгорнутих VPC/VPS серверів виключно з використанням безпечних методів передачі даних (SSH, SSL/TLS, IPSec, VPN):**	Так	Рекомендується налаштувати один із доступних варіантів доступу до VPC/VPS розгорнутих на ресурсах хмарних сервісів, для забезпечення безпечного підключення до віртуальних машин, що розгорнуті в мережі Інтернет. Також важливо налаштувати обмеження по IP-адресах, з яких буде відбуватися адміністративне підключення до віртуальних машин. Дані дії необхідно виконати для унеможливлювано нелегітимного доступу до віртуальних машин, що забезпечують функціонування критичних бізнес сервісів компанії замовника.
20	**Хмарний сервіс забезпечує можливість використання NBAD (Network Behavoir nomaly Detection) рішення для виявлення аномалій (Бот мереж, зловмисного трафіку, шкідливого програмного забезпечення тощо) в сегменті мережі:**	Так	Рекомендується увімкнути NBAD рішення для детального аналізу трафіку, що надходить до розгорнутих сервісів на ресурсах хмарного провайдера, з можливістю виявлення аномального трафіку, бот-мереж та попередження спроби компрометації бізнес сервісів компанії замовника. У випадку, якщо даний сервіс тарифікується окремо – рекомендується закласти в бюджет придбання даного сервісу.
21	**Хмарний сервіс забезпечує можливість використання IPS/IDS рішень:**	Так	Рекомендується увімкнути IPS/IDS рішення для виявлення та блокування аномальної поведінки в трафіку, що надходить до бізнес сервісів, щоб забезпечити безперебійне функціонування бізнес-процесів компанії замовника. У випадку, якщо даний сервіс тарифікується окремо – рекомендується закласти в бюджет придбання даного сервісу.
22	**Хмарний сервіс має вбудований мережевий екран (firewall) для контролю доступу до VPC/VPS серверів:**	Так	Рекомендується увімкнути вбудований Firewall на ресурсах постачальника хмарного сервісу для бізнес процесів компанії та визначити, для яких мереж/IP адрес буде доступний сервіс та які порти будуть доступні для підключення. Даний модуль необхідний, щоб унеможливити зловмисникам можливість підключення до інших сервісів, що функціонують на VPC/VPS та не мають бути доступними з публічної мережі Інтернет.

Parameter S - Storage Module

Рис. Б.25. Візуальне представлення переліку рекомендацій для модуля оцінювання «Network Module»

Додаток В. Лістинг захищеного мережевого застосунку

```
function loginEnco()
{
  var out = '';

  out += '<span class="spinner-border spinner-border-sm" role="status" aria-hidden="true"></span>';
  out += '<span class="sr-only"></span>';

  $('.btn-login').on('click', function (e)
  {
    // Add element of webpage
    $('.waiting').html(out);

    var inputL = document.getElementById("username").value;
    var inputP = document.getElementById("pwd").value;

    console.log(inputL);
    console.log(inputP);

document.getElementById("username").style.boxShadow = "0px 2px 0px 0px white";

document.getElementById("pwd").style.boxShadow = "0px 2px 0px 0px white";

document.getElementsByClassName("msg")[0].textContent ="Welcome back";

    if (inputL.trim() == '')
    {

document.getElementById("username").style.boxShadow = "0px 2px 0px 0px red";

document.getElementsByClassName("msg")[0].textContent ="Please, enter your username!";

      // delete element on webpage
      delete_element("spinner-border");
    }
    else if (inputP.trim() == '')
    {

document.getElementById("pwd").style.boxShadow = "0px 2px 0px 0px red";

document.getElementsByClassName("msg")[0].textContent ="Please, enter your password!";
```

```
    // delete element on webpage
    delete_element("spinner-border");
  }
  else {
    (async() => {
      const resL = await sha256(inputL);
      console.log(resL);

      // Send hash to server for check with user data
      $.post(
        "php/core.php",
        {
          "action" : "sub_L",
          "data"   :  resL
        },
        // Get Salt from server
        function (data_s)
        {
          data_s = JSON.parse(data_s);
          console.log(data_s);
          if (data_s == "Err_data")
          {

document.getElementsByClassName("msg")[0].textContent ="500 Error";

            // delete element on webpage
            delete_element("spinner-border");
          }
          else if (data_s == 'Err_user')
          {

document.getElementsByClassName("msg")[0].textContent ="Login or password incorrect!";

            // delete element on webpage
            delete_element("spinner-border");
          }
          else
          {
            if (data_s.length == 64)
            {
              (async() => {
                const resP = await sha256(inputP);
                console.log(resP);

                // Send login hash to server
                // Send sha256(sha256(password) + Salt)
                var inputPwdSalt = resP.concat(data_s);
                console.log(inputPwdSalt);
                (async() => {
```

```
            const hash = await
sha256(inputPwdSalt);
            console.log(hash);

            /// Send data Salt, login
hash and sha256(sha256(password) +
Salt) to server
            $.post(
              "php/core.php",
              {
                "action" : "sub_LP",
                "data"    : data_s,
                "data_hL" : resL,
                "data_hP" : hash
              },
              // Getting data from
server to authentication
              function (data_n)
              {
                data_n =
JSON.parse(data_n);
                console.log(data_n);

                if (data_s ==
"Err_data")
                {

document.getElementsByClassName(
"msg")[0].textContent ="500 Error";
                // delete element on
webpage

delete_element("spinner-border");
                }
                else if (data_s ==
'Err_user')
                {

document.getElementsByClassName(
"msg")[0].textContent ="Login or
password incorrect!";

                // delete element on
webpage

delete_element("spinner-border");
                }
                // Getting respond
from customer and write identifier to
cookies
                else
                {
                  var identLP =
data_n["_identity"];

console.log(identLP);


sessionStorage.setItem('_auth_query',
JSON.stringify(identLP));
```

```
                    var jArray =
data_n["_fold_main"];
                    jArray =
jArray.concat(data_n["_sepp"]);
                    jArray =
jArray.concat(data_n["_page"]);


                    console.log(jArray);


                    // delete element on
webpage

delete_element("spinner-border");



document.location.href = jArray;
                  }
                }
              );
             })();
           })();
         }
         else
         {

document.getElementsByClassName(
"msg")[0].textContent ="503 Error";


          // delete element on
webpage
          delete_element("waiting");
                }
              }
             }
            );
           })();
         }

         return false;
        });
       }


// Check auth token
function init() {
 var _id_ =
sessionStorage.getItem('_auth_query')
;
 console.log(_id_);
 load_console();


 if (_id_ == null)
 {
  window.location.href =
'../auth.html';
  return false;
 }
 else
 {
  _id_ = _id_.replace(/"/g, '');
```

```
    console.log(_id_);

    // Send user id to server
    $.post(
      "php/core.php",
      {
        "action" : "_check_user_data",
        "id"   : _id_
      },
      // Get data from server
      function (data)
      {
        data = JSON.parse(data);
        console.log(data);

        if (data == "Err_user")
        {
          window.location.href =
'../auth.html';
          return false;
        }
        else if (data == "Correct_user")
        {
          delete_element("sp-main");
          _top_info_user_();
        }
        else
        {
          window.location.href =
'../auth.html';
          return false;
        }
      }
    );
  }
}



// Get Assessment's List
function _get_list_of_assessments_()
{
  // Send user id to server
    $.post(
      "php/core.php",
      {
        "action" :
"_get_assessments_list"
      },
      // Get data from server
      function (data)
      {
        if (data == "\"List of
Assessments is empty\"")
        {
          console.log(data);
          delete_element("span_spin");

          var out = '';
```

```
        out += '<tr>';
         out += `<td
class="_no_elements_"
colspan="6">No Assessments. Please
click "+ Add New Assessment" to
complete assessment for your Cloud
Service Provider.</td>`;
        out += '</tr>';


        $('#_table_dash_').append(out);
      }
      else {
        let _assessment_list =
JSON.parse(data);
        console.log(_assessment_list);


        var out = '';


        for (var i = 0; i <
_assessment_list.length; i++) {
          out += `<tr
class="assessment_number_${i+1}">
`;
            out += `<td
class="_as_number_">${_assessment
_list[i][0]}</td>`;
            out += `<td
class="_as_name_">${_assessment_li
st[i][1]}</td>`;
            out += `<td
class="_as_csp_type_">${_assessmen
t_list[i][2]}</td>`;
            out += `<td
class="_as_score_">${_assessment_li
st[i][3]}</td>`;
            out += `<td
class="_as_mark_">`;
              if (_assessment_list[i][4] ==
'Recommended')
                out += `<i class="bi bi-
circle-fill green_status"></i>${' / ' +
_assessment_list[i][4]}`;
              else if
(_assessment_list[i][4] == 'Maybe')
                out += `<i class="bi bi-
circle-fill yellow_status"></i>${' / ' +
_assessment_list[i][4]}`;
              else if
(_assessment_list[i][4] == 'No
Recommended')
                out += `<i class="bi bi-
circle-fill red_status"></i>${' / ' +
_assessment_list[i][4]}`;
            out += `</td>`;
              out += `<td
class="_element_actions_">`;
            out += `<a href="#"
alt="Information about Assessment"
onclick="_popup_info_as_record(${'"
"+_assessment_list[i][5]+'"'});">`;
              out += '<i class="fa-solid
fa-circle-info"></i>';
            out += '</a>';
            out += `<a href="#"
alt="Assessment Report"
onclick="_popup_report_assessment(
${'"'+_assessment_list[i][5]+'"'},${'"
"+_assessment_list[i][1]+'"'});">`;
```

```
                out += '<i class="fa-solid fa-file"></i>';
                out += '</a>';
                out += `<a href="#" alt="Remove Assessment" onclick="_popup_confirmation_del_as_record(${""+_assessment_list[i][5]+""},${""+_assessment_list[i][1]+""});">`;
                out += '<i class="fa-solid fa-trash"></i>';
                out += '</a>';
              out += `</td>`;
            out += '</tr>';
          }

          delete_element("span_spin");

          $('#_table_dash_').append(out);
        }
      }
    );
}

// Info Assessment
function _popup_info_as_record(as_id) {
  $.post(
      "php/core.php",
      {
        "action"    : "_get_assessments_list_with_id",
        "unique_id" : as_id
      },
      // Get data from server
      function (data)
      {
        let _assessment_list = JSON.parse(data);
        console.log(_assessment_list);

        var out = '';

        out += '<div class="info-as">';
          out += '<div class="wrapper">';
            out += '<div class="head_popup">';
              out += `<h1 class="elastic_head">Information about selected assessment:</h1>`;
            out += '</div>';
            out += '<div class="information">';
              out += `<h3>Name: <span>${_assessment_list[0][1]}</span></h3>`;
              out += `<h3>Type: <span>${_assessment_list[0][2]}</span></h3>`;
              out += `<h3>Score: <span>${_assessment_list[0][3]}</span></h3>`;
```

```
            out += `<h3>Mark: <span>${_assessment_list[0][4]}</span></h3>`;

            out += `<h3 class="h3_id">ID: <span>${_assessment_list[0][5]}</span></h3>`;

            out += `<h3>Parameter score N: <span>${_assessment_list[0][6]}</span></h3>`;

            out += `<h3>Parameter score S: <span>${_assessment_list[0][7]}</span></h3>`;

            out += `<h3>Parameter score SR: <span>${_assessment_list[0][8]}</span></h3>`;

            out += `<h3>Parameter score V: <span>${_assessment_list[0][9]}</span></h3>`;

            out += `<h3>Parameter score OS: <span>${_assessment_list[0][10]}</span></h3>`;

            out += `<h3>Parameter score CT: <span>${_assessment_list[0][11]}</span></h3>`;

            out += `<h3>Parameter score R: <span>${_assessment_list[0][12]}</span></h3>`;

            out += `<h3>Parameter score A: <span>${_assessment_list[0][13]}</span></h3>`;

            out += `<h3>Parameter score D: <span>${_assessment_list[0][14]}</span></h3>`;

            out += '</div>';

            out += '<div class="buttons">';

            out += '<div class="close-button">';

            out += `<a href="#" class="close-info-assessment">Close`;

            out += '</a>';

            out += '</div>';

            out += '<div class="message">';

            out += '</div>';

            out += '</div>';

        out += '</div>';


        $('.popup-menu').append(out);


        $('.close-info-assessment').click(function(){

            delete_element('info-as');

        }

        );

    }

);
```

```
}



// 1-st Step in Assessment
function content() {
  var out = '';

  out += '<h1>New Assessment</h1>';
  out += '<div class="menu_assessment">';
  out += '</div>';

  $('._new_assessment_').html(out);

 /* out = '';

  out += '<tr class="span_spin">';
    out += `<td class="_no_elements_" colspan="5" style="border-radius: 0 0 10px 10px;">`;
      out += '<span class="sp-main spinner-border spinner-border-sm" role="waiting" aria-hidden="true"></span>';
    out += `</td>`;
  out += '</tr>';

  $('#_table_dash_').append(out);*/

  _add_info_for_new_assessment_();
}

// First Step in New Assessment
function _add_info_for_new_assessment_() {
  // Add content to page
  var out = '';

  out += '<div class="right-content">';
    out += '<div class="content-items">';
      out += '<h2>Cloud Service Provider Assessment</h2>';
      out += '<div class="step-assessment">';
      out += '</div>';
      out += '<div class="new-step-assessment">';
      out += '</div>';
    out += '</div>';
  out += '</div>';

  $('.menu_assessment').html(out);


  // Get 1-st Questions of Assessment
```

```
 let assessment_questions = new Array();


 $.post(
    "php/core.php",
    {
     "action" : "_get_1st_assessment_questions"
    },
    // Get data from server
    function (data)
    {
     data = JSON.parse(data);
     console.log(data);


     assessment_questions = data;


     /*Add data to console*/
     var out = '';


     out += '<h3 class="text-muted"><span>First Step</span> - Enter Information about your evaluated Cloud Service Provider</h3>';


     $('.step-assessment').html(out);


     var out = '';


      out += '<div class="step-questions">';

       out += '<div class="first-assessment-questions">';

         out += '<div class="container-questions">';

           var counter = 1;

           for (var i = 0; i < assessment_questions.length; i++)
           {
            var counter_j = 1;
            if (assessment_questions[i][2] !== 'undefined' && assessment_questions[i][2] !== null)
            {
             out += '<div class="first-level-questions">';
              out += '<fieldset>';
               out += `<legend>${assessment_questions[i][0]}. ${assessment_questions[i][1]}</legend>`;
                for (var j = 2; j < 10; j++) // 9 - maximum answers for all questions
                {
                 if (assessment_questions[i][j] !== 'undefined' && assessment_questions[i][j] !== null)
                 {
                  out += '<div>';
```

```
                    out += `<input type="radio" id="${counter}-${counter_j}-answer" name="${i+1}-answers" value="${counter}-${counter_j}-answer" />`;
                    out += `<label for="${counter}-${counter_j}-answer">${assessment_questions[i][j]}</label>`;
                    out += '</div>';
                }
                counter_j++;
            }
            out += '</fieldset>';
        out += '</div>';
    }
    else
    {
        out += '<div class="first-level-questions">';
            out += '<fieldset>';
                out += `<legend>${assessment_questions[i][0]}. ${assessment_questions[i][1]}</legend>`;
                out += '<div>';
                out += '<input type="csp-name" placeholder="Name of Cloud Service Provider" class="csp-name" id="csp-name" required>';
                out += '</div>';
            out += '</fieldset>';
        out += '</div>';
    }
    counter++;
}
out += '</div>';
out += '</div>';
out += '</div>';
out += '<div class="step-buttons">';
    out += `<a href="#" class="next-step-second-page" onclick="next_step_second_page(${assessment_questions.length});">`;
        out += '<span class="item">Next Step </span>';
        out += '<i class="fa-solid fa-arrow-right"></i>';
    out += '</a>';
out += '</div>';

$('.new-step-assessment').html(out);

/*Get Elements from SessionStorage*/
let first_attribute_id = JSON.parse(sessionStorage.getItem('first_attribute_id'));
```

```
        let _csp_name_ =
JSON.parse(sessionStorage.getItem('_
csp_name_'));
        console.log(first_attribute_id);


        if (first_attribute_id !== null)
        {
          for (var i = 0; i <
first_attribute_id.length; i++)
          {
            if (first_attribute_id[i] !==
null)
            {
              var element =
document.getElementById(first_attrib
ute_id[i]);


              if
(element.getAttribute("type") ===
"radio")
              {

document.getElementById(first_attrib
ute_id[i]).checked = true;
              }
               else {

document.getElementById(first_attrib
ute_id[i]).value = _csp_name_;
              }
            }
          }
        }
      }
    }
  );
}


 function findElementByText(tag,
text) {
    // Находим все элементы с
указанным тегом
    const elements =
document.querySelectorAll(tag);
    // Перебираем все элементы и
ищем тот, у которого текстовое
содержимое соответствует
заданному
    for (let element of elements) {
        if (element.innerHTML == text)
{
            return element;
        }
    }
    return null; // Если элемент не
найден, возвращаем null
}


// Processing data from First Step,
Save data to Temporary Storage in
Browser and go to Second Step
function
next_step_second_page(as_length) {
  let first_step_result = new Array();
```

```
  let first_step_result_id = new
Array(); // need for save attribute
name


  for (var i = 0; i < as_length; i++)
  {
    var getSelectedValue =
document.querySelector(`input[name
="${i+1}-answers"]:checked`); // get
data from radio button


    if (getSelectedValue == null) //
need for get data from input element
    {
      getSelectedValue =
document.getElementById("csp-
name"); // Get data from input
element


first_step_result.push(getSelectedVal
ue.value); // add element to Array


console.log(getSelectedValue.value);


      // Save Attributes
      first_step_result_id.push("csp-
name");
    }
    else
    {
first_step_result.push(getSelectedVal
ue.labels[0].innerHTML); // add
element to Array


console.log(getSelectedValue.labels[0
].innerHTML);


console.log(getSelectedValue.labels[0
].getAttribute("for"));


      // Save Attributes

first_step_result_id.push(getSelected
Value.labels[0].getAttribute("for"));
    }
  }


  // Result Output
  console.log(first_step_result);
  console.log(first_step_result_id);


  // Set data from first_step_result
Array to SessionStorage
  sessionStorage.setItem('_csp_type_',
JSON.stringify(first_step_result[0]));

sessionStorage.setItem('_csp_name_',
JSON.stringify(first_step_result[1]));
```

```
sessionStorage.setItem('_csp_working_with_disrupted_area_', JSON.stringify(first_step_result[2]));

sessionStorage.setItem('first_attribute', JSON.stringify(first_step_result));

sessionStorage.setItem('first_attribute_id', JSON.stringify(first_step_result_id));



_network_module_for_new_assessment_();
}




/*Recommendations N*/
async function _get_recommendations_for_parameter_N_(parameter) {
  // unique_id of Assessment
  let unique_id = JSON.parse(localStorage.getItem('unique_id'));


  /*data N*/
  // Повертаємо проміс, обгортаючи $.post
  return new Promise((resolve, reject) => {
    $.post(
      "php/core.php",
      {
        "action"    : "_get_recomendations_parameter_n_",
        "unique_id" : unique_id,
        "parameter" : parameter
      },
      // Get data from server
      function (data)
      {
        //data = JSON.parse(data);
        //console.log(data);
        //return data;
        try {
          data = JSON.parse(data);
          //console.log(data); // Лог для перевірки
          resolve(data);     // Повертаємо дані через resolve, щоб завершити проміс
        } catch (error) {
          reject(error);     // Якщо виникла помилка при парсингу, відхиляємо проміс
        }
      }
    ).fail(reject);
  });
}
```

```
/*Processing data Parameters for getting recommendations*/
function _processing_parameters_ (assessment, results, recommendations) {
  const count = assessment.length;
  console.log(count);

  // рекомендації
  let recommendations_for_answers = new Array();

  /*Знаходимо відповідь користувача. У питаннях знаходимо розташування відповіді та по номеру відповіді - знаходимо рекомендацію*/
  let q_counter = 0;

  for (var i = 2; i < count+2; i++)
  {
    let user_answer = results[0][i]; // Взяли відповідь користувача
    console.log(user_answer);

    for (var j = 3; j < 11; j++) // Ініціалізували процес перебору відповідей користувача із загальною кількістю запитань
    {
      let temp_number = 0;

      if (user_answer == assessment[q_counter][j]) // пошук співпадіння
      {
        temp_number = j; // знайшли порядковий номерспівпадіння

recommendations_for_answers.push(recommendations[q_counter][temp_number]);

console.log(recommendations[q_counter][temp_number]); // вивели на екран рекомендацію
      }

    }

    q_counter++;
  }

  return recommendations_for_answers;
}
```

Додаток Г. Акт впровадження

SDIGITAL

ТОВ "СІТОН ДІДЖИТАЛ"
вул. Гарматна, 4, 4-й поверх, офіс 4,
Київ, Україна, 03067
+380 44 239 99 99
info@seeton.digital

ЗАТВЕРДЖУЮ
Директор товариства з обмеженою відповідальністю «СІТОН ДІДЖИТАЛ»
_____ **Дмитро НІКІТЮК**
(підпис)
"03" 12 2024 року
М.П.

АКТ

Комісія у складі:
голови – директор, Нікітюк Дмитро Вікторович;
членів комісії: – заступник керівника відділу систем інформаційної безпеки, Коровайченко Юрій Юрійович
– провідний фахівець з інформаційної безпеки, Костіна Єлизавета Василівна.

цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри Кібербезпеки державного некомерційного підприємства «Державний університет «Київський авіаційний інститут».

Педченка Євгенія Максимовича

на тему: "Методи та моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури"
на здобуття ступеня доктора філософії за спеціальністю **125 «Кібербезпека»**
впроваджені в діяльності **товариства з обмеженою відповідальністю «СІТОН ДІДЖИТАЛ».**

Зокрема, під час підготовки програмного продукту для оцінювання кіберзахищеності хмарних сервісів, орієнтованого на компанії та державні структури України використано аналітичні та практичні матеріали дисертаційної роботи Педченка Євгенія Максимовича, які описують метод проведення оцінювання стану кіберзахисту хмарних сервісів, надають деталізовану структурну модель оцінювання, забезпечують алгоритмічним програмним забезпечення для впровадження розробленого підходу оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури в розроблюваний веб-програмний застосунок компанії.

Голова комісії	Директор	(підпис) Дмитро НІКІТЮК
Члени комісії	Заступник керівника відділу систем інформаційної безпеки	(підпис) Юрій КОРОВАЙЧЕНКО
	Провідний фахівець з інформаційної безпеки	(підпис) Єлизавета КОСТІНА

Рис. Г.1. Акт впровадження результатів дисертаційної роботи в компанії ТОВ «СІТОН ДІДЖИТАЛ» під час розробки програмного забезпечення оцінювання стану кіберзахисту хмарних сервісів