конфіденційної інформації, реалізація принципу нульової довіри (Zero Trust) на індивідуальному рівні тощо.

У цьому контексті культура безпеки не є лише похідною від технічної захищеності або нормативної відповідності – вона формується як організаційна компетенція, що дозволяє запобігати атакам, знижувати вразливість до маніпуляцій і підвищувати загальну стійкість системи. Її розвиток має здійснюватися як через впровадження чітко визначених процедур, так і через зміну підходів до управління, у яких людський чинник розглядається не як вразливість, а як ключовий об'єкт цілеспрямованого формування поведінки та навичок.

1. Security-first culture: defending against social engineering. URL: https://www.venzagroup.com/security-first-culture-defending-against-social-engineering (дата звернення: 24.04.2025)
2. Defending against social engineering: a proactive approach. URL: https://privacymatters.ubc.ca/news/defend-against-social-engineering (дата звернення: 24.04.2025)
3. 8 ways organisations prevent social engineering attacks. URL: https://blogs.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks (дата звернення: 24.04.2025)

Структурна модель системи оцінювання стану кіберзахисту хмарних сервісів

УДК 004.056.5

Євгенія Іванченко[1], Євгеній Педченко[2], Марі Петровська[3], Ігор Іванченко[4]
State University of Information and Communication Technologies,
[1]evivancenko@gmail.com
State Non-Commercial Company «State University «Kyiv Aviation Institute»,
[2]ympedchenko@gmail.com, [3]pmarisha2004@gmail.com,[4]igor-p-l@gmail.com

Оцінювання рівня інформаційної безпеки постачальників хмарних сервісів є актуальним завданням для будь-якої організації, що планує або вже здійснила міграцію своїх ресурсів до хмарних середовищ, проте не володіє повною інформацією щодо їхньої кіберзахищеності [1]. Дослідження провідних світових компаній, зокрема Proofpoint [2], CrowdStrike [3] та Check Point [4], підтверджують, що проблема забезпечення безпеки хмарних платформ має пріоритетне значення, а організації, які застосовують хмарні технології, постійно стикаються з низкою ризиків, загроз та викликів у сфері кібербезпеки.

На сьогоднішній день, виділяються такі ключові проблеми оцінювання стану кіберзахисту хмарних сервісів: невиявлені та невиправлені вразливості, проведення перевірки налаштувань відповідно до кращих практик та належна побудова відповідного рівня захищеності на всіх рівнях роботи хмарних сервісів. З огляду на зазначене, проблема оцінювання стану кіберзахисту хмарних сервісів є комплексною та потребує системного підходу, що враховує інтереси та відповідальність як користувачів, так і постачальників хмарних послуг. Важливим аспектом цього процесу є постійний моніторинг і

впровадження відповідних інструментів, спрямованих на ефективне управління ризиками й ідентифікацію потенційних вразливостей [5].

Метою даної роботи є розробка структурної моделі системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури.

Новизною є розроблена структурна модель системи оцінювання, яка за рахунок розроблених модулів оцінювання дозволяє оцінити стан кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури [6].

Структурна модель системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури зображена на Рис. 1 та складається з наступних компонентів:

- 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) [5].

Структурна модель оцінювання стану кіберзахисту хмарних сервісів працює за наступним алгоритмом:

1. Робота системи починається із запуску модуля МІО для ініціалізації оцінювання та формування підмножини CSP.
2. Наступний модуль МОЗД із базою БДЗЗ визначає тип сервісу (IaaS, PaaS, CaaS, FaaS, SaaS [7]) та параметри оцінювання.
3. Модуль МОМ разом із базою БДЗММ оцінює захищеність мережевого рівня.

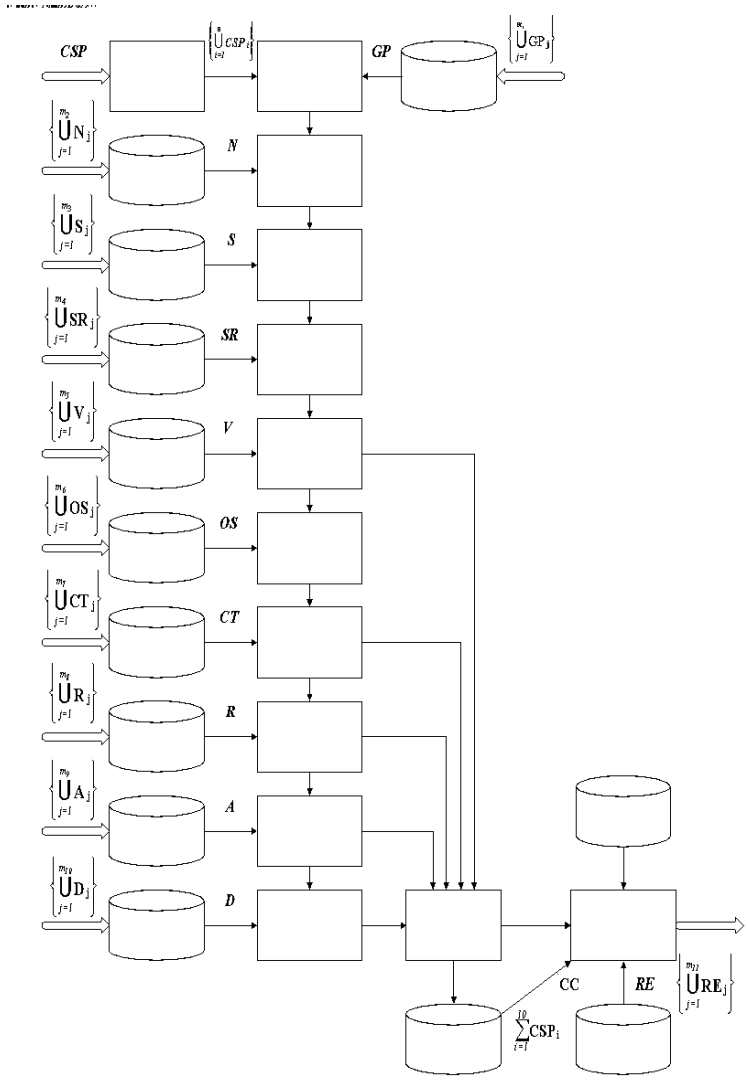

Рис. 1. Структурна модель системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури

4. Модуль МОЗіД із базою БДЗМЗД аналізує стан захисту середовища зберігання даних.

5. Модуль МОСО із базою БДЗСМ оцінює фізичну захищеність серверного обладнання.
6. Модуль МОСВ із базою БДЗМВ аналізує безпеку середовища віртуалізації VPC/VDS.
7. Модуль МООС з базою БДЗОС перевіряє захищеність підтримуваної операційної системи.
8. Модуль МОСК із базою БДЗМК здійснює оцінювання безпеки середовища контейнеризації.
9. Модуль МОБР з базою БДЗМБР визначає захищеність безперебійності роботи сервісу.
10. Модуль МОД з базою БДЗМД аналізує безпеку запропонованого хмарного застосунку.

Після завершення оцінки всіх параметрів запускається модуль МЗРОБД, який підраховує результати й записує їх у базу БДРО. Визначається загальна сума балів, обчислюється коефіцієнт СС та вводиться параметр **RC** для надання рекомендацій щодо подальшого використання сервісу у середовищі компанії.

В роботі представлено розроблену структурну модель системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури, що базується на запропонованих моделі та методі оцінювання стану кіберзахисту хмарних сервісів. Для побудови структурної моделі було використано 11 параметрів оцінювання, визначених у відповідній моделі оцінювання. Кожному етапу оцінювання відповідають методичні напрацювання, які передбачають виставлення балів за відповіді аудитора під час проведення оцінюваня стану кіберзахисту хмарного сервісу. У структурній моделі продемонстровано взаємодію параметрів оцінювання з відповідними базами даних. За результатами оцінювання здійснюється підрахунок набраних балів, після чого приймається рішення щодо доцільності використання хмарного сервісу в продуктивному середовищі компанії. Розроблену систему оцінювання в подальшому буде використано для розробки програмного застосунку оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

1. Cloud Adoption and Risk Report, *McAfee*. 2019, 14 p. URL: https://files.constantcontact.com/e4d8c81b001/d093e39a-1795-4f0b-928d-c5bb25a3a4b7.pdf
2. Stephen L. Cloud Security Posture Management (CSPM), *HyperGlance*. 2023. URL: https://www.hyperglance.com/blog/cloud-security-posture-management-cspm/
3. Shared responsibility in the cloud, *Microsoft*. 2024. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
4. ISO/IEC 27001. Information security management systems, *ISO*. 2022, 19 p. URL: https://www.iso.org/standard/27001
5. 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

6. Педченко Є.М. Іванченко І.С. Метод оцінювання кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. *Сучасний захист інформації*. 2024, Том 59, № 3, 75-84 с. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2999/2897

7. Roger S. IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS — What's the difference? *Medium*. 2021. URL: https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference

Інструменти динамічного аналізу шкідливого програмного забезпечення

УДК 621.395.7 (043.2)

Степан Івасьєв[1], Віталій Кобиця[2]

Західноукраїнський національний університет,

[1]isv@wunu.edu.ua, [2]kobutsia.v.v@gmail.com

Розвиток шкідливого програмного забезпечення зумовлений постійною кібервійною призводить до постійної необхідності в засобах динамічного та статичного аналізу ШПЗ. Важливим елементом є боротьба з засобами виявлення віртуальних машин та методами їх протидії, що застосовуються в ШПЗ для унеможливлення їх динамічного аналізу.

Поширеними інструментами для аналізу ШПЗ є відкриті засоби доступні онлайн такі, як VirusTotal, Joe Sandbox Cloud, Hybrid Analysis, Any.Run, Intezer Analyze.

Проте враховуючи широкий набір засобів боротьби з віртуальними машинами окрему увагу потрібно приділити налаштуванню власної віртуальної машини, для боротьби з методами виявлення віртуалізації.

Для ефективного динамічного аналізу шкідливого програмного забезпечення доцільно використовувати такі віртуальні машини, які здатні протидіяти методам виявлення віртуалізації, які активно застосовують зловмисники. З цією метою слід обирати рішення, що забезпечують гнучке налаштування, можливість маскування віртуального середовища та максимально наближені до умов реального комп'ютера. Процес динамічного аналізу програмного забезпечення можна представити у вигляді схеми, що на рис. 1.

Для динамічного аналізу досить часто використовують гіпервізори VMware Workstation або VMware ESXi. Ці платформи мають відносно низький рівень виявлення, оскільки дозволяють детально налаштувати параметри віртуальної машини. Завдяки цим можливостям VMware часто використовується для ручного або напівавтоматизованого аналізу зразків шкідливого ПЗ.

Ще одним поширеним рішенням є VirtualBox, який завдяки відкритому вихідному коду зручно модифікувати. Проте в базовому стані VirtualBox часто виявляється шкідливими програмами через типові драйвери, службові процеси та пристрої з характерними назвами. Щоб зменшити ймовірність детектування, слід вручну видалити ознаки віртуального середовища, змінити системні назви