КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.505515
УДК 004.056.5

Іванченко Ігор Сергійович
к.т.н., доцент кафедри Технічного захисту інформації
місце роботи: Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0003-3415-9039
ihor.ivanchenko@npp.nau.edu.ua

Педченко Євгеній Максимович
аспірант, асистент кафедри Кібербезпеки
місце роботи: Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0001-8436-5792
pedchenko.ievhenii@npp.nau.edu.ua

СТРУКТУРНА МОДЕЛЬ СИСТЕМИ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. Під час даного дослідження продемонстровано структурну модель системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури, що має на меті застосування для оцінки всіх публічних хмарних сервісів. Розроблено структурну модель системи оцінювання кібербезпеки хмарних сервісів, що складається з 11 параметрів оцінки модулів, а саме: мережевого, збереження даних, серверного, віртуалізації, операційної системи, контейнеризації, безперервної роботи, додатків та обробки даних. Для розробленої структурної моделі системи оцінювання представлено всі модулі, що є задіяними під час оцінки використовуваного хмарного сервісу, а також представлено формули обчислення кожного із 1 параметрів оцінки, що є задіяними вданій системі. Для розробленої структурної моделі системи оцінювання розроблено схематичне зображення, яке демонструє залежність усіх компонентів системи та використаних параметрів оцінювання хмарних сервісів, а також представлено взаємодію з базою даних, що розміщує всю інформацію про питання, відповіді, рекомендації та проведені оцінки аудитором. Додатково на схемі можна побачити процес запису результатів оцінювання до бази даних. Представлено візуалізацію результатів проведеної оцінки шляхом формування окремої веб-сторінки, дані для якої беруться із таблиць бази даних, що містять результати проведеної оцінки та відбувається представлення рекомендації, щодо можливості використання чи не використання хмарного сервісу в продуктивному середовищі компанії на основі отриманих балів по результатам оцінювання 11 модулів. Додатково, представлена можливість вивантаження результатів оцінювання в окремий звіт, що може бути представлений керівництву компанії для прийняття фінального рішення. Тому, в даній роботі описано використані модулів та баз даних для побудови структурованої моделі системи оцінювання, а також алгоритм оцінювання кіберзахищеності хмарного сервісу та надання фінального висновку, щодо рекомендації використання чи невикористання оцінюваного хмарного сервісу.

Ключові слова: кібербезпека; модель; метод; система; аудит; провайдер хмарних сервісів

ВСТУП

Оцінка безпеки постачальників хмарних сервісів є важливим питанням для будь-якого бізнесу, який планує або вже здійснив міграцію своїх сервісів до хмарних провайдерів, не маючи повного уявлення про рівень їхньої кіберзахищеності. [1] Відповідно до досліджень провідних світових компаній, таких як Proofpoint [2], CrowdStrike [3] та Check Point [4], проблема захисту хмарних середовищ є ключовою, і

будь-яка організація, що використовує хмару, зіштовхується з ризиками, загрозами та проблемами забезпечення кібербезпеки.

Постановка проблеми. Проблема оцінювання кібербезпеки хмарних сервісів стає все більш актуальною, оскільки зростає залежність компаній від хмарних обчислювальних потужностей та сервісів для зберігання і обробки даних.

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

1. **Загрози кібербезпеці та невиправлені вразливості:** Попри розширені механізми захисту, хмарні сервіси можуть бути вразливими до різних видів атак, включаючи DDoS, атаки на порушення захищеності даних та експлуатацію вразливостей через некоректні налаштування безпеки. Дослідження компанії McAfee показало [5], що понад 90% підприємств мають недостатній контроль над своїми даними в хмарі, що підвищує ризики несанкціонованого доступ до комерційних даних.
2. **Оцінка безпеки користувацьких конфігурацій:** Невірно налаштовані сервіси та помилки в конфігурації веб-серверів, сервісів є одними з основних джерел вразливостей. У звіті компанії Gartner зазначено [6], що до 2025 року 99% інцидентів безпеки у хмарі будуть спричинені помилками користувачів, а не провайдерами хмарних послуг.
3. **Відповідальність за організації кібербезпеки:** Хмарні провайдери часто використовують модель відповідальності "shared responsibility" [7], де частина обов'язків за організацію кібербезпеки лежить на користувачах. Наприклад, Microsoft Azure чітко розмежовує відповідальність за інфраструктуру, яку вони захищають, і відповідальність користувачів за захист даних та додатків, розміщених у хмарі.

Саме тому, проблема оцінювання кіберзахищеності хмарних сервісів є багатогранною і вимагає комплексного підходу як з боку користувачів, так і хмарних провайдерів. Важливим є постійний моніторинг і використання відповідних інструментів для управління ризиками та вразливостями.

Аналіз останніх досліджень і публікацій. На сьогоднішній день більшість компаній та установ апелюють стандартом ISO 27001 [8], який вказує, які мають бути впроваджені підходи ля побудови інформаційної безпеки, але ніяк не надаючи чіткого плану дій для побудови захищеної мережі компанії чи установи, що є суттєвим недоліком даного стандарту. Також, потрібно враховувати, що даний стандарт націлений на побудову інформаційної безпеки саме для Private мережі, а не хмарних сервісів чи систем, що опубліковані в загально-доступній мережі Інтернет [9].

Разом з тим, розпочинаючи з 2004 року на теренах інформаційної простору України та світу існують підходи щодо побудови моделей оцінки стану захищеності систем [10], які також проаналізовано в роботі [11], що направлені на оцінку ризиків інформаційної безпеки компонентів інформаційно-комунікаційних систем та на виявлення аномалій в кіберпросторі, що направлені на оцінку можливостей протидії інформаційних систем відомим кіберзагрозам та інцидентам. Проте всі вище перераховані методи, стандарти та підходи націлені саме на надання рекомендацій, як потрібно проводити оцінку кіберзагроз, проте не націлені на чітке виявлення проблематика в замовника чи сервісу та не надають чітких рекомендацій для усунення виявленого недоліку в кібербезпеці компанії чи установи, а також не надають можливості та засоби оцінки хмарних сервісів на предмет їх захищеності та можливості протидії кіберзагрозам.

Саме тому питання оцінювання кіберзахищеності постачальників хмарних сервісів є вкрай актуальним на сьогоднішній день. Існує дефіцит детальної інформації про рівень захищеності пропонованих послуг, що призводить до невпевненості в тому, чи є

корпоративні дані, розміщені на ресурсах постачальника хмарних сервісів, надійно захищеними, чи ні.

Мета статті. Метою роботи є розробка структурної моделі системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури на основі розроблених моделі та методу оцінювання хмарних сервісів.

Для досягнення даної мети необхідно розробити структурну модель системи оцінювання на основі розроблених моделі та методу оцінювання хмарних сервісів, що включає в себе всі 11 кроків оцінювання хмарних сервісів [12]. Розроблена структурна модель системи оцінювання дозволить нам чітко визначити основні модулі програмного забезпечення, послідовність виконання оцінювання модулів хмарних сервісів та надати аудитору результат оцінювання у зручному вигляді на розробленому веб-додатку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Структурна модель системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури зображена на Рисунку 1 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).

Початок роботи системи розпочинається із запуску модуля МІО, що ініціює запуск нового оцінювання, що запускає створення підмножини CSP, що визначається формулою:,

$$\boldsymbol{CSP} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{CSP}_i \right\} = \left\{ \boldsymbol{CSP}_1, \boldsymbol{CSP}_2, \boldsymbol{CSP}_3, ..., \boldsymbol{CSP}_7, ..., \boldsymbol{CSP}_{11} \right\} \quad (1)$$

де $\boldsymbol{CSP}_i \subseteq \boldsymbol{CSP}$ $(i = \overline{1,n})$ – кореневий компонент системи характеристик, що представляє *i*-й номер параметра оцінки, а *n* – представляє кількість параметрів оцінки.

Після ініціалізації оцінювання, запускається новий модуль МОЗД, що працює в парі з Базою БДЗЗ, який дозволяє визначити тип оцінюваного хмарного сервісу (IaaS, PaaS, CaasS, FaaS чи SaaS [9]) та визначити, які з параметрів підмножини CSP будуть задіяні для проведення оцінювання хмарного сервісу. Модуль ініціалізує параметр **GP**, що визначається формулою:

$$\mathbf{GP} = \left\{ \bigcup_{j=1}^{m_1} \mathbf{GP}_j \right\} = \left\{ \mathbf{GP}_1, \mathbf{GP}_2 ..., \mathbf{GP}_{m_1} \right\}, \quad (2)$$

де $\mathbf{GP_j} \subseteq \mathbf{GP}$ $(j = \overline{1,m_1})$ – j-й перший лінійний параметр призначений для оцінювання загальних компонентів, а m_1 – кількість запитань. За результатами даного оцінювання, визначається тип хмарного сервісу та кількість параметрів оцінки, що є різники для кожного із оцінюваних типів хмарних сервісів. В нашому випадку представимо тип хмарного сервісу – **SaaS**, до якого застосовуються всі параметри оцінювання.

Після визначення типу хмарного сервісу, запускається новий модуль МОМ, що працює з Базою БДЗММ, який дозволяє оцінити стан захищеності мережі, в якій працює хмарний сервіс. Модуль ініціалізує параметр **N**, що визначається формулою:

$$\mathbf{N} = \left\{ \bigcup_{j=1}^{m_2} \mathbf{N}_j \right\} = \left\{ \mathbf{N}_1, \mathbf{N}_2 ..., \mathbf{N}_{m_2} \right\}, \quad (3)$$

де: $\mathbf{N_j} \subseteq \mathbf{N}$ $(j = \overline{1,m_2})$ – j-й другий лінійний параметр призначений для оцінювання стану захищеності мережі хмарного сервісу, а m_2 –кількість запитань.

Після оцінки стану захищеності мережевого рівня, запускається новий модуль МОЗіД, що працює з Базою БДЗМЗД, який дозволяє оцінити стан захищеності середовища зберігання даних на ресурсах хмарного сервісу. Модуль ініціалізує параметр **S**, що визначається формулою:

$$\mathbf{S} = \left\{ \bigcup_{j=1}^{m_3} \mathbf{S}_j \right\} = \left\{ \mathbf{S}_1, \mathbf{S}_2 ..., \mathbf{S}_{m_3} \right\}, \quad (4)$$

де: $\mathbf{S_j} \subseteq \mathbf{S}$ $(j = \overline{1,m_3})$ – j-й третій лінійний параметр призначений для оцінювання стану захищеності середовища зберігання даних, а m_3 – кількість запитань.

Після оцінки стану захищеності середовища зберігання даних, запускається новий модуль МОСО, що працює з Базою БДЗСМ, який дозволяє оцінити стан захищеності

середовища фізичного розташування серверного обладнання, що використовується для забезпечення роботи хмарного сервісу. Модуль ініціалізує параметр **SR**, що визначається формулою:

$$\mathbf{SR} = \left\{ \bigcup_{j=1}^{m_4} \mathbf{SR_j} \right\} = \left\{ \mathbf{SR_1}, \mathbf{SR_2} \ldots, \mathbf{SR_{m_4}} \right\}, \quad (5)$$

де: $\mathbf{SR_j} \subseteq \mathbf{SR}$ $(j = \overline{1, m_4})$ – j-й четвертий лінійний параметр призначений для оцінювання стану захищеності середовища фізичного розташування серверного обладнання, а m_4 – кількість запитань.

Після оцінки стану захищеності середовища фізичного розташування серверного обладнання, запускається новий модуль МОСВ, що працює з Базою БДЗМВ, який дозволяє оцінити стан захищеності середовища віртуалізації, що забезпечує роботу для VPC/VDS серверів хмарного сервісу. Модуль ініціалізує параметр **V**, що визначається формулою:

$$\mathbf{V} = \left\{ \bigcup_{j=1}^{m_5} \mathbf{V_j} \right\} = \left\{ \mathbf{V_1}, \mathbf{V_2} \ldots, \mathbf{V_{m_5}} \right\}, \quad (6)$$

де: $\mathbf{V_j} \subseteq \mathbf{V}$ $(j = \overline{1, m_5})$ – j-й п’ятий лінійний параметр призначений для оцінювання стану захищеності середовища віртуалізації, а m_5 – кількість запитань.

Після оцінки стану захищеності середовища віртуалізації, запускається новий модуль МООС, що працює з Базою БДЗОС, який дозволяє оцінити стан захищеності підтримуваної операційної системи, що пропонується до використання замовникам на базі хмарного сервісу. Модуль ініціалізує параметр **OS**, що визначається формулою:

$$\mathbf{OS} = \left\{ \bigcup_{j=1}^{m_6} \mathbf{OS_j} \right\} = \left\{ \mathbf{OS_1}, \mathbf{OS_2} \ldots, \mathbf{OS_{m_6}} \right\}, \quad (7)$$

де: $\mathbf{OS_j} \subseteq \mathbf{OS}$ $(j = \overline{1, m_6})$ – j-й шостий лінійний параметр призначений для оцінювання стану захищеності операційної системи, а m_6 –кількість запитань.

Після оцінки стану захищеності операційної системи, запускається новий модуль МОСК, що працює з Базою БДЗМК, який дозволяє оцінити стан захищеності середовище розгортання контейнерів. Модуль ініціалізує параметр **CT**, що визначається формулою:

$$\mathbf{CT} = \left\{ \bigcup_{j=1}^{m_7} \mathbf{CT_j} \right\} = \left\{ \mathbf{CT_1}, \mathbf{CT_2} \ldots, \mathbf{CT_{m_7}} \right\}, \quad (8)$$

де: $\mathbf{CT_j} \subseteq \mathbf{CT}$ $(j = \overline{1, m_7})$ – j-й сьомий лінійний параметр призначений для оцінювання стану захищеності середовища контейнеризації, а m_7 – кількість запитань.

Після оцінки стану захищеності середовища контейнеризації, запускається новий модуль МОБР, що працює з Базою БДЗМБР, який дозволяє оцінити стан захищеності безперебійної роботи всіх компонентів хмарного сервісу для надання сервісу замовникам. Модуль ініціалізує параметр **R**, що визначається формулою:

$$\mathbf{R} = \left\{ \bigcup_{j=1}^{m_8} \mathbf{R_j} \right\} = \left\{ \mathbf{R_1}, \mathbf{R_2} \ldots, \mathbf{R_{m_8}} \right\}, \tag{9}$$

де: $\mathbf{R_j} \subseteq \mathbf{R}$ $(j = \overline{1, m_8})$ – j-й восьмий лінійний параметр призначений для оцінювання стану захищеності середовища безперервної роботи, а m_8 – кількість запитань.

Після оцінки стану захищеності середовища безперервної роботи, запускається новий модуль МОД, що працює з Базою БДЗМД, який дозволяє оцінити стан захищеності пропонованого хмарного застосунку на базі хмарного сервісу. Модуль ініціалізує параметр **A**, що визначається формулою:

$$\mathbf{A} = \left\{ \bigcup_{j=1}^{m_9} \mathbf{A_j} \right\} = \left\{ \mathbf{A_1}, \mathbf{A_2} \ldots, \mathbf{A_{m_9}} \right\}, \tag{10}$$

де: $\mathbf{A_j} \subseteq \mathbf{A}$ $(j = \overline{1, m_9})$ – j-й дев'ятий лінійний параметр призначений для оцінювання стану захищеності хмарного застосунку, а m_9 – кількість запитань.

Після оцінки стану захищеності хмарного застосунку, запускається новий модуль МООД, що працює з Базою БДЗМОД, який дозволяє оцінити стан захищеності середовища обробки даних на ресурсах хмарного сервісу. Модуль ініціалізує параметр **D**, що визначається формулою:

$$\mathbf{D} = \left\{ \bigcup_{j=1}^{m_{10}} \mathbf{D_j} \right\} = \left\{ \mathbf{D_1}, \mathbf{D_2} \ldots, \mathbf{D_{m_{10}}} \right\}, \tag{11}$$

де: $\mathbf{D_j} \subseteq \mathbf{D}$ $(j = \overline{1, m_{10}})$ – j-й десятий лінійний параметр призначений для оцінювання стану захищеності середовища обробки даних, а m_{10} – кількість запитань.

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.

Перед початком оцінювання визначається тип хмарного сервісу та кількість максимально можливих балів. В нашому випадку, тип **SaaS** має максимально **615** балів.

Потім вираховується сума всіх набраних балів по 10 параметрам оцінки підмножини CSP за формулою:

$$\begin{gathered} \sum_{i=1}^{10} \mathbf{CSP_i} = \mathbf{CSP_1} + \mathbf{CSP_2} + \mathbf{CSP_3} + \mathbf{CSP_4} + \mathbf{CSP_5} + \\ \mathbf{CSP_6} + \mathbf{CSP_7} + \mathbf{CSP_8} + \mathbf{CSP_9} + \mathbf{CSP_{10}} = \\ \mathbf{GP} + \mathbf{N} + \mathbf{S} + \mathbf{SR} + \mathbf{V} + \mathbf{OS} + \mathbf{CT} + \mathbf{R} + \mathbf{A} + \mathbf{D} \end{gathered} \tag{12}$$

де: $\mathbf{CSP_i} \subseteq \mathbf{CSP}$ $(i = \overline{1,10})$ – сума всіх набраних балів.

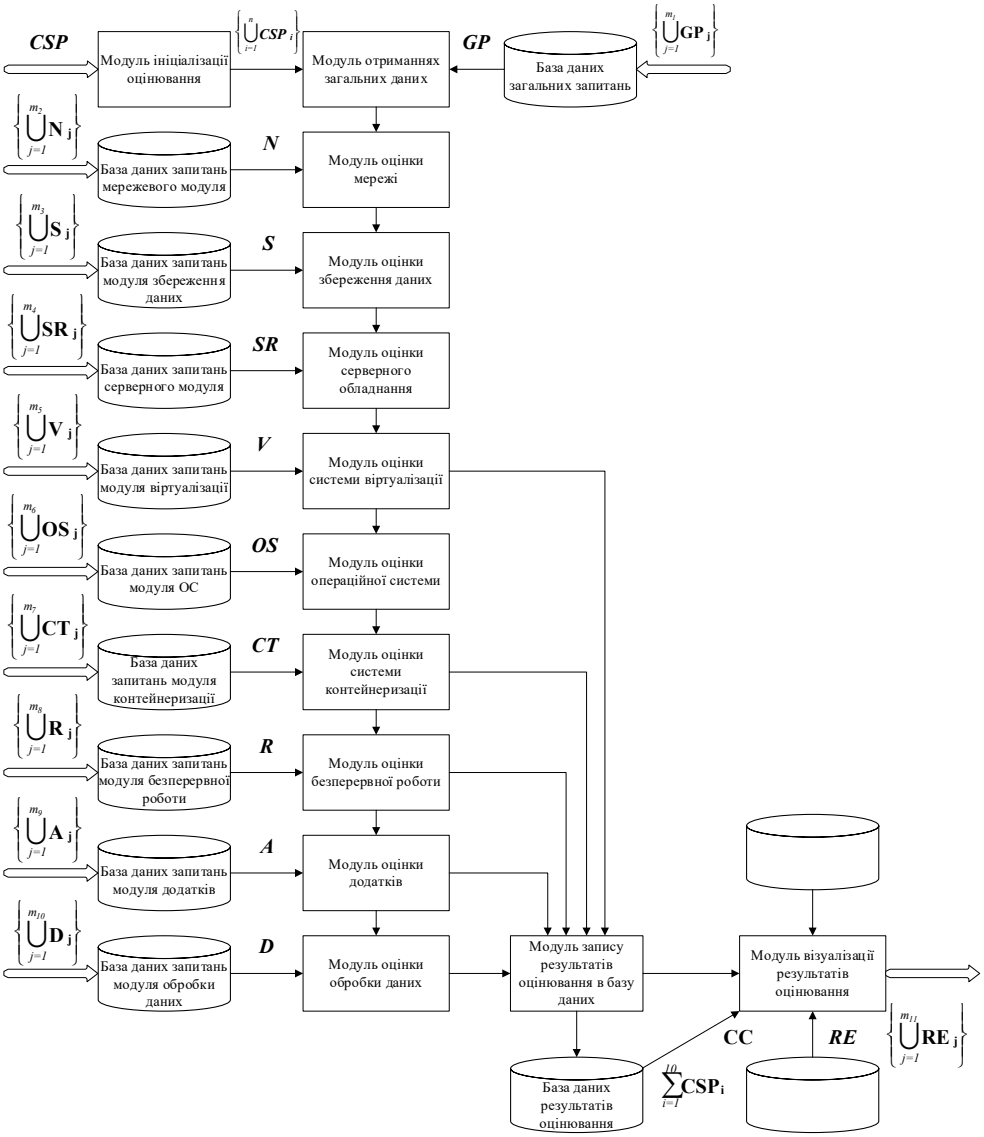

Рис. 1. Розроблена Структурна Модель Системи Оцінювання Кібербезпеки Хмарних Сервісів Об'єктів Інформаційної Інфраструктури

За результатами знаходження суми всіх балів, запускається етап обчислення коефіцієнту **CC**, що обчислюється за наступною формулою:

$$\mathbf{CC} = \frac{\sum_{i=1}^{10} \mathbf{CSP_i}}{< CSP\ type\ selected >} * 100\%, \tag{13}$$

де: $\sum_{i=1}^{10} \mathbf{CSP_i}$ – сума всіх обчислених балів, $< CSP\ type\ selected >$ – максимальна кількість балів по типу хмарному сервісу (SaaS=615).

І на останньому етапі оцінювання, вводиться новий параметр **RC**, що визначає ступінь рекомендації до використання в продуктивному середовищі оцінюваного хмарного сервісу.

Після запису результатів оцінювання в базу БДРО, запускається новий модуль МВРО, що отримує дані з таких Баз: БДРО, БДР та БДЕЗ, - та формує комплексний звіт за результатами проведеного оцінювання хмарного сервісу типу SaaS, на 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.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В даній роботі розроблено структурну систему моделі оцінювання кіберзахищеності хмарних сервісів об'єктів критичної інфраструктури керуючись розробленими моделлю та методом оцінювання кіберзахищеності хмарних сервісів. Для побудови основних кроків структурної моделі було використано 11 параметрів оцінювання хмарних сервісів, що були описані в моделі оцінювання хмарних сервісів. Для кожного із етапів оцінювання було присвоєно напрацювання із розробленого методу оцінювання хмарних сервісів, що включають в себе виставлення визначеної кількості балів за кожну відповідь аудитора на запитання щодо оцінки стану кіберахищеності хмарних сервісів. На структурній моделі показано, як кожний із параметрів оцінки взаємодіє із базою даних. Після проведення оцінки, розпочинається процес підрахунку отриманих балів відповідно до сформованих формул, за результатами якого надається рішення щодо рекомендації/не рекомендації використання хмарного сервісу. Також, продемонстровано процес формування звіту аудитору за результатами проведеної оцінки. Розроблена структурна модель системи оцінювання може бути використана для оцінки провідних та популярних хмарних сервісів з метою визначення їх кіберзахищеності із наданням рекомендації, щодо використання чи невикористання оцінюваного хмарного сервісу на основі результатів розробленої системи оцінювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pedchenko, Y., et al. (2022). Analysis of modern cloud services to ensure cybersecurity. *Procedia Computer Science, 207*, 110–117. https://doi.org/10.1016/j.procs.2022.09.043
2. Proofpoint. (n.d.). What is cloud security? - Issues & threats. Proofpoint. Retrieved September 20, 2024, from https://www.proofpoint.com/us/threat-reference/cloud-security
3. CrowdStrike. (n.d.). What is cyber espionage? CrowdStrike. Retrieved September 20, 2024, from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/
4. Checkpoint. (n.d.). Top 15 cloud security issues, threats and concerns. Checkpoint. Retrieved September 20, 2024, from https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
5. McAfee. (n.d.). Cloud adoption and risk report. Retrieved September 20, 2024, from https://files.constantcontact.com/e4d8c81b001/d093e39a-1795-4f0b-928d-c5bb25a3a4b7.pdf
6. Hyperglance. (n.d.). Cloud security posture management (CSPM). Hyperglance. Retrieved September 21, 2024, from https://www.hyperglance.com/blog/cloud-security-posture-management-cspm/
7. Microsoft. (n.d.). Shared responsibility in the cloud - Microsoft Azure. Microsoft Learn. Retrieved September 22, 2024, from https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
8. ISO. (2022). *ISO/IEC 27001:2022*. Retrieved September 21, 2024, from https://www.iso.org/standard/27001

9. The Next Platform. (2023, April 3). Cloud spending curtailed, on premises spending heading into recession. Retrieved September 23, 2024, from https://www.nextplatform.com/2023/04/03/cloud-spending-curtailed-on-premises-spending-heading-into-recession/
10. Korchenko, O. (2004). *Information protection systems* (Monograph). Kyiv: NAU.
11. Potii, O., et al. (2023). Model of the system of data characteristics for assessing the state of cyber protection in Ukraine. *Collection of scientific works of the Central Research Institute of the Armed Forces of Ukraine, 107*(4), 313–329.
12. Pedchenko, Y., & Ivanchenko, I. (2024). The method of assessing the cyber security of cloud services of information infrastructure objects. *Modern Information Security, 59*(3), 75–89. https://doi.org/10.31673/2409-7292.2024.030008
13. Stample. (n.d.). IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS – What's the difference? Retrieved September 29, 2024, from https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Ihor S. Ivanchenko
Candidate of Technical Sciences, Associate Professor of Technical Information Protection Department
Work place: National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-3415-9039
ihor.ivanchenko@npp.nau.edu.ua

Yevhenii M. Pedchenko
Postgraduate Student, Assistant of Cybersecurity Department
Work place: National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0001-8436-5792
pedchenko.ievhenii@npp.nau.edu.ua

STRUCTURAL MODEL OF THE CYBERSECURITY ASSESSMENT SYSTEM OF CLOUD SERVICES OF INFORMATION INFRASTRUCTURE OBJECTS

Abstract. During this investigation, a structural model of the system for evaluating the cyber security of cloud services of information infrastructure objects will demonstrate, which is intended to be used for the evaluation of all public cloud services. A structural model of the cyber security evaluation system of cloud services has been developed, consisting of 11 module evaluation parameters, namely: network, data storage, server, virtualization, operating system, containerization, continuous operation, applications and data processing. For the developed a structural model of the evaluation system, all the modules involved in the evaluation of the used cloud service are presented, as well as the formulas for calculating each of the 1 evaluation parameters involved in a successful system are presented. For the developed a structural model of the evaluation system, a schematic image has been developed that demonstrates the dependence of all system components and the used evaluation parameters of cloud services, as well as interaction with the database, which places all information about questions, answers, recommendations, and evaluations made by the auditor, is presented. In addition, the schematic image shows the process of recording the evaluation results to the database. The visualization of the results of the conducted assessment is presented by generating a separate web page, the data for which is taken from the database tables containing the results of the conducted assessment and a recommendation is presented regarding the possibility of using or not using the cloud service in the productive environment of the company based on the points obtained from the assessment results 11 modules. Additionally, it is possible to download the evaluation results into a separate report that can be presented to the company's management for a final decision. So, this work describes the modules and databases used to build a structured model of the evaluation system, as well as the algorithm for evaluating the cyber security of a cloud service and providing a final conclusion regarding the recommendation to use or not use the evaluated cloud service.

Keywords: cybersecurity; model; method; system; audit; cloud service provider.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Pedchenko, Y., et al. (2022). Analysis of modern cloud services to ensure cybersecurity. *Procedia Computer Science, 207*, 110–117. https://doi.org/10.1016/j.procs.2022.09.043
2. Proofpoint. (n.d.). What is cloud security? - Issues & threats. Proofpoint. Retrieved September 20, 2024, from https://www.proofpoint.com/us/threat-reference/cloud-security
3. CrowdStrike. (n.d.). What is cyber espionage? CrowdStrike. Retrieved September 20, 2024, from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/
4. Checkpoint. (n.d.). Top 15 cloud security issues, threats and concerns. Checkpoint. Retrieved September 20, 2024, from https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
5. McAfee. (n.d.). Cloud adoption and risk report. Retrieved September 20, 2024, from https://files.constantcontact.com/e4d8c81b001/d093e39a-1795-4f0b-928d-c5bb25a3a4b7.pdf

6. Hyperglance. (n.d.). Cloud security posture management (CSPM). Hyperglance. Retrieved September 21, 2024, from https://www.hyperglance.com/blog/cloud-security-posture-management-cspm/
7. Microsoft. (n.d.). Shared responsibility in the cloud - Microsoft Azure. Microsoft Learn. Retrieved September 22, 2024, from https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
8. ISO. (2022). *ISO/IEC 27001:2022*. Retrieved September 21, 2024, from https://www.iso.org/standard/27001
9. The Next Platform. (2023, April 3). Cloud spending curtailed, on premises spending heading into recession. Retrieved September 23, 2024, from https://www.nextplatform.com/2023/04/03/cloud-spending-curtailed-on-premises-spending-heading-into-recession/
10. Korchenko, O. (2004). *Information protection systems* (Monograph). Kyiv: NAU.
11. Potii, O., et al. (2023). Model of the system of data characteristics for assessing the state of cyber protection in Ukraine. *Collection of scientific works of the Central Research Institute of the Armed Forces of Ukraine, 107*(4), 313–329.
12. Pedchenko, Y., & Ivanchenko, I. (2024). The method of assessing the cyber security of cloud services of information infrastructure objects. *Modern Information Security, 59*(3), 75–89. https://doi.org/10.31673/2409-7292.2024.030008
13. Stample. (n.d.). IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS – What's the difference? Retrieved September 29, 2024, from https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference