УДК 004.056.53:004.946.5
DOI: 10.31673/2409-7292.2024.030008

Педченко Є. М., Іванченко І. С.

МЕТОД ОЦІНЮВАННЯ КІБЕРЗАХИЩЕНОСТІ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

У роботі розроблено метод на базі математичної моделі, що призначений для математичного обчислення оцінки стану кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. Для побудови методу оцінювання були використані результати розробки моделі, критерії оцінювання хмарних сервісів, а також варіанти відповідей, для яких визначено кількість балів за кожен варіант. Метод оцінювання складається з 11 етапів, де останнім є безпосередньо обчислення критичності хмарного сервісу. За результатами обчислень надається рекомендація щодо використання або не використання хмарного сервісу, що дозволяє приймати обґрунтовані рішення на основі отриманих даних. У статті також представлено обчислені максимально можливі кількості балів, які можуть бути отримані в межах оцінюваного хмарного сервісу. Цей метод може бути використаний під час розробки мережевого застосунку, що стане корисним інструментом для аудитора. Він допоможе оцінити стан захищеності використовуваного хмарного сервісу в компанії-замовника, а також перед придбанням чи використанням таких сервісів. Застосування даного методу дозволяє значно підвищити рівень обізнаності щодо потенційних ризиків, пов'язаних з використанням хмарних технологій, і забезпечити належний рівень кібербезпеки. Розроблений підхід може стати основою для подальших досліджень у сфері оцінки кіберзахищеності, сприяючи розвитку більш комплексних моделей та інструментів для аналізу ризиків у хмарних середовищах. Це, в свою чергу, сприятиме зростанню довіри до хмарних сервісів і їх безпеки в умовах сучасних інформаційних викликів.

Ключові слова: кібербезпека, інформаційна безпека, оцінка, математична модель, математичний метод, аудит, CSP, Cloud Service Provider, IaaS, PaaS, CaaS, FaaS, SaaS.

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 проблемамизабезечення кібербезпеки.

Формулювання проблеми

Ці компанії окреслюють головні проблеми, пов'язані з безпекою хмарних сервісів.

1. Неправильна конфігурація систем безпеки, що може призвести до витоку даних бізнесу за межі ресурсів хмарного сервісу.

2. Можливість несанкціонованого доступу до середовищ, розгорнутих на ресурсах постачальників хмарних сервісів, що підключені до Інтернету, через відсутність належних систем безпеки, контролю доступу, компрометацію облікових даних або некоректні налаштування.

3. Недостатній захист API-інтерфейсів, який дозволяє виконувати CLI запити до конфігурації хмарних сервісів без необхідності введення токену або логіна й пароля, надаючи зловмиснику повний контроль над сервісами.

4. Відсутність систем захисту від кібератак, що дає змогу зловмисникам здійснювати успішні запити до хмарних сервісів і втручатися в бізнес-процеси компаній.

В даному випадку, компанії із виробництва та постачання систем безпеки лише надають опис проблем з безпеки, з якими стикається бізнес, що користується послугами постачальників хмарних сервісів, але не надає можливість проведення аудиту систем безпеки таких хмарних сервісів, як: IaaS, CaaS, PaaS, FaaS та SaaS [5].

Аналіз літературних джерел

На сьогоднішній день більшість компаній та установ апелюють стандартом ISO 27001 [6], 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 [7].

Разом з тим, розпочинаючи з 2004 року на теренах інформаційної простору України та світу існують підходи щодо побудови моделей оцінки стану захищеності систем [8], які також проаналізовано в роботі [9], 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 та завдання дослідження

Основною метою даної статті є розробка методу оцінки кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури на основі розробленої моделі оцінювання хмарних сервісів.

Для досягнення даної мети необхідно розробити систему оцінювання для сформованих 120 запитань із готовими варіантами відповідей і рекомендацій, що описують перелік необхідних дій щодо удосконалення стану захищеності хмарних сервісів об’єктів інформаційної інфраструктури. Розроблена система оцінювання дозволить чітко прописати кількість балів, що є закріпленими за кожним із оцінюваних параметрів і містить різну кількість балів, що може бути отримана в рамках оцінювання різних типів хмарних сервісів.

Основна частина

Розроблений метод оцінювання хмарних сервісів ґрунтується на визначеному переліку запитань в моделі, що є основною для побудови системи оцінювання та визначення ступеня критичності кожного із оцінюваних хмарних сервісів.

Для проведення оцінювання для методу було затверджено фіксовані бали в проміжку від 0 до 5, де 5 – це максимальний бал оцінки, а 0 – мінімальний бал оцінки.

Шляхом визначення системи оцінювання методу було виділено 10 ключових етапів, що є критично важливими під час проведення оцінювання хмарних сервісів об’єктів інформаційної інфраструктури, які дозволяють визначити рівень захищеності модуля: опису загальної інформації про хмарний сервіс; обслуговування мережі; зберігання даних; обслуговування серверного обладнання; обслуговування системи віртуалізації; операційної системи; управління контейнерами; безперервної роботи сервісу; управління застосунками; обробки даних.

Вище описані модулі будуть використані для оцінювання стану кіберзахищеності наступних типів хмарних сервісів: 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) [10].

Нижче буде вказано всі визначені модулі оцінювання хмарних сервісів, що є описаними в моделі оцінювання і складаються з 10 параметрів, описаних вище, а також 1-го параметру, що містить рекомендації щодо покращення стану захищеності хмарних сервісів:

$CSP_1 = GP =$ **"*General Points module*"** – модуль для опису загальних положень постачальника хмарного сервісу;

$CSP_2 = N =$ "***Network module***" – модуль оцінки рівня захищеності мережі постачальника хмарного сервісу;

$CSP_3 = S =$ "***Storage module***" – модуль оцінки рівня захищеності накопичувачів (HDD/SSD/M2 etc);

$CSP_4 = SR =$ "***Server module***" – модуль оцінки захищеності серверного обладнання;

$CSP_5 = V =$ "***Virtualization module***" – модуль оцінки використовуваного середовища віртуалізації;

$CSP_6 = OS =$ "***Operation System module***" – модуль оцінки захищеності використовуваних операційних систем;

$CSP_7 = CT =$ "***Container Technology module***" – модуль оцінки захищеності вика управління контейнерами;

$CSP_8 = R =$ "***Runtime module***" – модуль оцінки систем моніторингу, щодо виявлення аномалій, вразливостей, системних подій тощо;

$CSP_9 = A =$ "***Application module***" – модуль оцінки захищеності програмного забезпечення, що постачається замовникам;

$CSP_{10} = D =$ "***Data module***" – модуль оцінки рівня захищеності даних, що обробляться системами постачальника хмарних сервісів [10];

$CSP_{11} = RE =$ "***Requirements' module***" – модуль формування рекомендацій по всі можливі варіанти вибору аудитора.

Розроблений метод буде базуватися на основних 11 етапах проведення оцінювання кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури.

Кожний із вище описаних параметрів залежить від типу хмарного сервісу, оцінювання якого проводиться, як це зображено в Таблиці 1.

Таблиця 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	$CSP_{11} = RE =$ "***Requirements' module***"	+	+	+	+	+

Етап 1 – отримання загальної інформації щодо оцінюваного хмарного сервісу.

На даному етапі заповнюється параметр **GP**, що наповнюється даними, які вводить клієнт перед проведенням оцінювання. На першому етапі оцінювання не застосовується, оскільки даний параметр є виключно інформативним. Наприклад, якщо аудитор оцінює тип

© Педченко, Є. М., & Іванченко, І. С. (2024). Метод оцінювання кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. Сучасний захист інформації, 3(59), 75–84. https://doi.org/10.31673/2409-7292.2024.030008.

хмарного сервісу – SaaS, з назвою «Cloud Service» і вказує, що хмарний сервісі не співпрацює з країнами-агресорами, то формула буде мати наступний вигляд:

$$\mathbf{CSP}_1 = \mathbf{GP} = \{SaaS, "Cloud\ Service", Hi\}, \quad (1)$$

Етап 2 – оцінка кіберзахищеності модуля обслуговування мережі.

На даному етапі використовуються значення параметру N та відбувається оцінювання стану захищеності мережевого модуля, що включає в себе перевірку системи на протидію DDoS атак, пропускну здатність мережі тощо. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

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

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

На базі критеріїв Етапу 2 – представимо, для яких варіантів відповідей – які бали методу оцінювання застосовуються: 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).

Аналогічно як для даного етапу, бали методу оцінювання будуть застосовуватися і для інших етапів оцінювання.

Етап 3 – оцінка кіберзахищеності модуля зберігання даних.

На даному етапі використовуються значення параметру $\boldsymbol{S}$ та відбувається оцінювання стану захищеності модуля зберігання даних, що опрацьовуються на хмарному сервісі, де оцінюється можливість відновлення даних, стійності масивів даних тощо . В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

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

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

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 4 – оцінка кіберзахищеності модуля обслуговування серверного обладнання.

На даному етапі використовуються значення параметру $\boldsymbol{SR}$ та відбувається оцінювання стану захищеності модуля обслуговування хмарного обладнання, що опрацьовуються на хмарному сервісі, де оцінюється здатність системи протидіяти фізичному впливу на обладнання тощо. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

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

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

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 5 – оцінка кіберзахищеності модуля обслуговування системи віртуалізації.

На даному етапі використовуються значення параметру $\boldsymbol{V}$ та відбувається оцінювання стану захищеності модуля забезпечення функціонування віртуального середовища хмарного провайдера, де оцінюється використана система віртуалізації, її ступінь захищеності тощо. В

даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

$$\begin{gathered}
\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\} \\
\{\{\{\{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}\}\} = \\
\{\{\{\{''5'',''4'',''3'',''2'',''1'',''0''\},\{''3'',''4'',''5'',''1'',''2'',''3'',''4'',''0''\},\{''5'',''0''\}\}, \\
\{\{''5'',''4'',''3'',''2'',''1'',''0''\},\{''3'',''4'',''5'',''1'',''2'',''3'',''4'',''0''\},\{''5'',''0''\}\}, \\
\{\{''5'',''4'',''3'',''2'',''1'',''0''\},\{''3'',''4'',''5'',''1'',''2'',''3'',''4'',''0''\},\{''5'',''0''\}\}, \\
\{\{''5'',''4'',''3'',''2'',''1'',''0''\},\{''3'',''4'',''5'',''1'',''2'',''3'',''4'',''0''\},\{''5'',''0''\}\}, \\
\{\{''5'',''4'',''3'',''2'',''1'',''0''\},\{''3'',''4'',''5'',''1'',''2'',''3'',''4'',''0''\},\{''5'',''0''\}\}, \\
\{\{''5'',''4'',''3'',''2'',''1'',''0''\},\{''3'',''4'',''5'',''1'',''2'',''3'',''4'',''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{5}$$

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 6 – оцінка кіберзахищеності модуля операційної системи.

На даному етапі використовуються значення параметру ***OS*** та відбувається оцінювання стану захищеності модуля забезпечення функціонування використовуваних операційних систем, де оцінюється вибрана операційна система на предмет захищеності. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

$$\begin{gathered}
\mathbf{CSP}_6 = \mathbf{OS} = \left\{ \bigcup_{j=1}^{11} \left\{ \bigcup_{k=1}^{m_{6j}} \left\{ \bigcup_{l=1}^{m_{6jk}} \left\{ \bigcup_{p=1}^{m_{6jkl}} OS_{jklp} \right\} \right\} \right\} \right\} = \\
\{\{OS_{11}, OS_{12}, OS_{13}, OS_{14}, OS_{15},\},
\end{gathered} \tag{6}$$

© Педченко, Є. М., & Іванченко, І. С. (2024). Метод оцінювання кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури. Сучасний захист інформації, 3(59), 75–84. https://doi.org/10.31673/2409-7292.2024.030008.

$$\{\{\{OS_{2111}, OS_{2112}\}\}, OS_{22}\}, \{OS_{31}, OS_{32}\}, \{OS_{41}, OS_{42}\},$$
$$\{OS_{51}, OS_{52}\}, \{OS_{61}, OS_{62}\}, \{OS_{71}, OS_{72}\}, \{OS_{81}, OS_{82}\},$$
$$\{OS_{91}, OS_{92}\}, \{OS_{101}, OS_{102}\}, \{OS_{111}, OS_{112}\}\} =$$
$$\{\{"5","3","2","1","0"\}, \{\{\{"5","0"\}\},"0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\},$$

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 7 – оцінка кіберзахищеності модуля управління контейнерами.

На даному етапі використовуються значення параметру ***CT*** та відбувається оцінювання стану захищеності модуля управління середовищем контейнеризації, що відповідає за оцінки захищеності всіх розгорнутих контейнерів на базі ресурсів хмарного провайдера. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

$$\mathbf{CSP_7} = \mathbf{CT} = \left\{ \bigcup_{j=1}^{10} \left\{ \bigcup_{k=1}^{m_{7j}} CT_{jk} \right\} \right\} =$$
$$\{\{CT_{11}, CT_{12}\}, \{CT_{21}, CT_{22}\}, \{CT_{31}, CT_{32}\}, \{CT_{41}, CT_{42}\},$$
$$\{CT_{51}, CT_{52}\}, \{CT_{61}, CT_{62}\}, \{CT_{71}, CT_{72}\}, \{CT_{81}, CT_{82}\},$$
$$\{CT_{91}, CT_{92}\}, \{CT_{101}, CT_{102}\}\} =$$
$$\{\{"5","3"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\},$$

(7)

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 8 – оцінка кіберзахищеності модуля безперервної роботи сервісу.

На даному етапі використовуються значення параметру ***R*** та відбувається оцінювання стану захищеності модуля забезпечення безперервності роботи сервісів хмарного провайдера з метою забезпечення їх максимальної доступності. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

$$\mathbf{CSP_8} = \mathbf{R} = \left\{ \bigcup_{j=1}^{13} \left\{ \bigcup_{k=1}^{m_{8j}} R_{jk} \right\} \right\} =$$
$$\{\{R_{11}, R_{12}\}, \{R_{21}, R_{22}\}, \{R_{31}, R_{32}\}, \{R_{41}, R_{42}\}, \{R_{51}, R_{52}\},$$
$$\{R_{61}, R_{62}\}, \{R_{71}, R_{72}\}, \{R_{81}, R_{82}\}, \{R_{91}, R_{92}\}, \{R_{101}, R_{102}\},$$
$$\{R_{111}, R_{112}\}, \{R_{121}, R_{122}\}, \{R_{131}, R_{132}\}\} =$$
$$\{\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\},$$
$$\{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}, \{"5","0"\}\},$$

(8)

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

© Педченко, Є. М., & Іванченко, І. С. (2024). Метод оцінювання кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. Сучасний захист інформації, 3(59), 75–84. https://doi.org/10.31673/2409-7292.2024.030008.

Етап 9 – оцінка кіберзахищеності модуля управління застосунками.

На даному етапі використовуються значення параметру ***A*** та відбувається оцінювання стану захищеності модуля забезпечення захищеності розгорнутого додатку-як-сервіс на ресурсах хмарного провайдера та з метою оцінки стану захищеності пропонованого застосунку та його спроможності протидіяти кібератакам. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

$$\begin{gathered}\mathbf{CSP_9} = \mathbf{A} = \left\{\bigcup_{j=1}^{10}\left\{\bigcup_{k=1}^{m_{9j}} A_{jk}\right\}\right\} = \\ \{\{A_{11}, A_{12}\},\{A_{21}, A_{22}\},\{A_{31}, A_{32}, A_{33}\},\{A_{41}, A_{42}\},\{A_{51}, A_{52}\}, \\ \{A_{61}, A_{62}\},\{A_{71}, A_{72}\},\{A_{81}, A_{82}\},\{A_{91}, A_{92}\},\{A_{101}, A_{102}\}\} = \\ \{\{"5","0"\},\{"5","0"\},\{"5","3","0"\},\{"5","0"\},\{"5","0"\}, \\ \{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\}\},\end{gathered} \tag{9}$$

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 10 – оцінка кіберзахищеності модуля обробки даних.

На даному етапі використовуються значення параметру ***D*** та відбувається оцінювання стану захищеності модуля обробки даних компанії на ресурсах хмарного провайдера, з метою виявлення потенційних джерел витоку інформації та необхідності їх закриття. В даному випадку, використовуючи метод оцінювання кіберзахищеності хмарних сервісів та критерії оцінювання даного параметру, формула буде мати наступний вигляд:

$$\begin{gathered}\mathbf{CSP_{10}} = \mathbf{D} = \left\{\bigcup_{j=1}^{12}\left\{\bigcup_{k=1}^{m_{10j}} D_{jk}\right\}\right\} = \\ \{\{D_{11}, D_{12}\},\{D_{21}, D_{22}\},\{D_{31}, D_{32}\},\{D_{41}, D_{42}\},\{D_{51}, D_{52}\}, \\ \{D_{61}, D_{62}\},\{D_{71}, D_{72}\},\{D_{81}, D_{82}\},\{D_{91}, D_{92}\},\{D_{101}, D_{102}\}, \\ \{D_{111}, D_{112}\},\{D_{121}, D_{122}\}\} = \\ \{\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\}, \\ \{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\},\{"5","0"\}\},\end{gathered} \tag{10}$$

де кожна із вказаних підмножин – є відповіддю на критерій оцінювання хмарного сервісу та має визначену кількість балів.

Етап 11 – обчислення результатів оцінювання.

На даному етапі відбувається фінальне обчислення результатів оцінювання модулів оцінки хмарних сервісів, та обчислюється за формулою:

$$\mathbf{CC} = \frac{\sum_{i=1}^{10}\mathbf{CSP_i}}{< CSP\ type\ selected >} * 100\%, \tag{11}$$

де: **CC –** коефіцієнт кіберзахищеності хмарних сервісів; $\sum_{i=1}^{10}\mathbf{CSP_i}$ – сума всіх обчислених балів

по кожному параметру оцінювання; $< CSP\ type\ selected >$ – підстановка максимальної кількості балів, що потенційно може отримати кожний із типів хмарних сервісів.

Для обчислення значення $\sum_{i=1}^{10} \mathbf{CSP_i}$ - використовується формула наступного вигляду, що передбачає обчислення суми балів, отриманих по всіх параметрах оцінювання:

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

Також, нижче представлені максимально-допустимі значення оцінки кіберзахищеності хмарних сервісів, що підставляються в формулу замість $< CSP\ type\ selected >$: 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.

Окрім вище вказаного підходу до обчислення коефіцієнту кіберзахищеності хмарних сервісів – вводиться нова змінна під назвою **RC**, що дозволить надати розуміння, як для системи, і для користувача інформацію, чи рекомендується до використання хмарного сервісу чи ні. В результаті, аудитору після завершення оцінювання кіберзахищеності хмарного сервісу надається один із нижче вказаних рекомендацій:

“Рекомендується до використання (**Recommended**)”. Застосовується, якщо значення змінної CC ставить від 1% до 25%;

“Можливе до використання (**Maybe**)”. Застосовується, якщо значення змінної CC ставить від 26% до 75%;

“Не рекомендується до використання (**No Recommended**)”. Застосовується, якщо значення змінної CC ставить від 76% до 100%.

В розрізі математичних обчислень, вище вказані рекомендації надаються відповідно до Таблиці 2.

Таблиця 2

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

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

Висновок

В рамках даної статті було розроблено метод на базі математичної моделі, що призначений для математичного обчислення оцінки стану кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. Для побудови методу оцінювання було використано результати розробки моделі, критерії оцінювання хмарних сервісів, а також варіанти відповідей для яких було визначено кількість балів за кожний варіант відповіді. Метод оцінювання складається з 11 етапів, де останній це безпосередньо обчислення критичності хмарного сервісу, за результатом якого надається рекомендація, щодо використання/не використання хмарного сервісу. Також, в даній статті представлено обчислені максимально-можливі кількості балів, що можуть бути отримані в межах оцінюваного хмарного сервісу. За рахунок описаного методу оцінювання кіберзахищеності хмарних сервісів досягнуто завершення опрацювання математичної моделі дослідження, для впровадження його в розроблений мережевий застосунок, що буде корисний аудиторам під час оцінки стану захищеності використовуваного хмарного сервісу в компанії-замовника чи перед придбанням/використанням.

Перелік посилань

1. Pedchenko, Y. Analysis of modern cloud services to ensure cybersecurity [Electronic resource] / Y. Pedchenko, Y. Ivanchenko, I. Ivanchenko, I. Lozova, D. Jancarczyk, P. Sawicki // Procedia Computer Science. – 2022. – Vol. 207. – P. 110-117. – Mode of access: https://www.sciencedirect.com/science/article/pii/S1877050922009164 (date of access: 17.08.2024). – Analysis of modern cloud services to ensure cybersecurity.

2. Cloud Security [Electronic resourse]: Proofpoint. – Mode of access: https://www.proofpoint.com/us/threat-reference/cloud-security (date of access: 15.08.2024). – Cloud Security.

3. What is Cyber Espionage? [Electronic resourse]: CrowdStrike. – Mode of access: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/ (date of access: 15.08.2024). – What is Cyber Espionage?

4. Top 15 Cloud Security Issues, Threats and Concerns [Electronic resourse]: Check Point. – Mode of access: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/ (date of access: 15.08.2024). — Top 15 Cloud Security Issues, Threats and Concerns.

5. All You Need to Know About Top 10 Security Issues in Cloud Computing [Electronic resource]: Veritis. – Mode of access: https://www.veritis.com/blog/top-10-security-issues-in-cloud-computing/ (date of access: 14.08.2024). – All You Need to Know About Top 10 Security Issues in Cloud Computing.

6. ISO/IEC 27001. Electronic resourse] Information security management systems. – Mode of access: https://www.iso.org/standard/27001 (date of access: 14.08.2024). – Information security, cybersecurity and privacy protection.

7. Morgan, T. P. Cloud Spending Curtailed, On Premises Spending Heading Into Recession [Electronic resource] / T.P. Morgan // TheNextPlatform. – Mode of access: https://www.nextplatform.com/2023/04/03/cloud-spending-curtailed-on-premises-spending-heading-into-recession/ (date of access: 20.08.2024). – Cloud Spending Curtailed, On Premises Spending Heading Into Recession.

8. Корченко, О. Г. Системи захисту інформації: Монографія. – К.: НАУ, 2004. – 264 с.

9. Потій, О. В., Шульга, В. П., Корченко, О. Г., Іванченко, Є. В., Бакалинський, О. О., Мялковський, Д. В, Верба, Д. В., Зубков, Д. А., Юдіна, Д. О. Модель системи характеристик даних для оцінювання стану кіберзахисту в Україні. Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України №4 (107), 2023 – С. 313-329.

10. Roger, S. IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS – What's the difference? [Electronic resource] / S. Roger // Medium. – Mode of access: https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference (date of access: 10.07.2024). – IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS – What's the difference?

Надійшла 27.08.2024