DOI: 10.18372/2225-5036.30.19240

АНАЛІЗ МОДЕЛЕЙ ТА МЕТОДІВ ОЦІНЮВАННЯ СТАНУ КІБЕРЗАХИЩЕНОСТІ ХМАРНИХ СЕРВІСІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Ігор Іванченко, Євгеній Педченко

Національний авіаційний університет, Україна

ІВАНЧЕНКО Ігор Сергійович, к.т.н., доцент
Рік та місце народження: 1987 рік, м. Бердянськ, Запорізька обл., Україна.
Освіта: Національний авіаційний університет, 2015 рік.
Посада: доцент кафедри технічного захисту інформації з 2024 року.
Наукові інтереси: інформаційна та авіаційна безпека, методи і моделі управління доступом, оцінка ризиків та стану безпеки, побудова комплексних систем захисту інформації, безпека хмарних сервісів, кібербезпека.
Публікації: понад 50 друкованих наукових праць, серед яких колективів монографії, посібники, лабораторні практикуми, статті у вітчизняних та міжнародних фахових виданнях, навчально-методичні комплекси дисциплін, матеріали і тези доповідей на конференціях, патенти та авторські свідоцтва на комп'ютерні програми.
E-mail: ihor.ivanchenko@npp.nau.edu.ua.
Orcid ID: 0000-0003-3415-9039.

ПЕДЧЕНКО Євгеній Максимович, аспірант
Рік та місце народження: 1998 рік, смт. Чорнухи, Полтавська обл., Україна.
Освіта: Національний авіаційний університет, 2020 рік.
Посада: асистент кафедри кібербезпеки з 2024 року.
Наукові інтереси: захист персональних даних, оцінювання кіберзахищеності хмарних сервісів, безпека хмарних сервісів, кібербезпека.
Публікації: більше 15 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях та авторські свідоцтва.
E-mail: pedchenko.ievhenii@npp.nau.edu.ua.
Orcid ID: 0000-0001-8436-5792.

Анотація. *Дана стаття описує аналіз існуючих стандартів у сфері Кібербезпеки, що націлені на надання вимог до функціонування інформаційного середовища компаній. Під час розгляду статі буде представлено опис хмарних сервісів, їх типів, а також структурну модель кожного із обраних типів. На основі аналізу структурних моделей типів хмарних сервісів буде визначено основні критерії оцінки. Для оцінки відповідності стандартів у сфері Кібербезпеки визначених критеріїв оцінки, буде проведено їх порівняльний аналіз із застосуванням даних критеріїв.*

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

Постановка проблеми

Розпочинаючи з 50 років минулого століття, з'явилося перше поняття мережі, що об'єднувала в собі декілька обчислювальних пристроїв, що мали можливість обмінюватися даними без використання зовнішніх пристроїв [1]. Саме з цього моменту бере свій початок термін мережа, яку ми активно використовуємо для наших потреб.

Йшов час та з кінця 1990-х і початку 2000-х років, з'явилося поняття хмарний сервіс саме в тому розумінні, яке ми знаємо сьогодні. Один із перших засновників сучасного хмарного сервісу є компанія Amazon, яка започаткувала даний тренд і дала поштовх у розвитку хмарних сервісів іншими компаніями, таким як, Microsoft, Google, тощо [2].

Але в період зародження хмарних сервісів, компанії ще не задумувалися про забезпечення кіберзахисту своїх сервісів чи даних, що обробляються на ресурсах хмарних севірсів, тому випускали програмне забезпечення, що мало вразливості, обхідні шляхи та навіть застосовувався протокол передачі даних HTTP замість HTTPS, хоча другий з'явився ще у 1995 році [3].

Але, так як час йшов, рішення розвивалися, як і зацікавленість зловмисників до отримання доступу до даних, у постачальників хмарних сервісів виникала потреба в розробці засобів захисту даних, сервісів, і т.д., з метою від зловмисників. Щоб дізнатися про типи атак, що стосуються саме хмарних сервісів, рекомендуємо звернутися до [4].

Як і у зловмисників збільшувався інтерес до хмарних сервісів, так і у регуляторів та компаній, зростав інтерес, і в 2011 році на базі Національного інституту Стандартизації та Технологій (NIST – National

Institute of Standards and Technology) було створено п'ять основних характеристик, яким повинні відповідати всі існуючі хмарні сервіси:

- надання можливості замовникам самостійно обслуговувати хмарні ресурси;
- відсутність обмежень до мережі Інтернет;
- можливість виділення фізичних ресурсів;
- забезпечення гнучкого управління виділеними ресурсами;
- надання можливості замовникам самостійно визначати необхідну кількість фізичних ресурсів [5].

Вперше в період з 2013 по 2016 роки група дослідників намагалася висунути свої рекомендації щодо покращення засобів захисту хмарних сервісів, проте бізнес, як і, безпосередньо, хмарні провайдери, такі як AWS, Azure не підтримали ідею дослідників, аргументуючи тим, що незважаючи на кібератаки, система продовжує безперебійно працювати та виконувати бізнес-процеси, приносячи прибуток без додаткових витрат.

Аналіз останніх досліджень і публікацій

На сьогодні для оцінювання стану захищеності хмарних сервісів використовуються такі стандарти/регламенти, як HIPAA, PCI DSS, SOC 2, ISO 27001, NIST 80-145. Проте жоден із цих стандартів не описує чітко вимоги до захищеності всіх компонентів хмарних сервісів, покриваючи їх лише частково, як, наприклад, стандарт ISO 27001 – стосується тільки наземної частини функціонування хмарних сервісів. Саме тому актуальним на даний момент питанням є порівняння можливостей міжнародних стандартів для побудови захищеного та стійкого функціонування хмарних сервісів з можливістю забезпечення безпеки даних компаній замовників, які передають на опрацювання власні конфіденційні дані на ресурси хмарного провайдера.

Мета та постановка завдання

Метою даної роботи є визначення ключових критеріїв оцінювання хмарних сервісів та проведення порівняння існуючих стандартів відповідно до сформованих критеріїв оцінювання.

Для досягнення поставленої мети, нам необхідно:

1. Обрати типи хмарних сервісів, що використовуються по всьому світу.
2. Сформувати основні критерії оцінювання, що передбачатимуть оцінку стану кіберзахищеності обраних типів хмарних сервісів.
3. Провести порівняння існуючих стандартів оцінювання хмарних сервісів відповідно до визначених критеріїв оцінювання.

Виклад основного матеріалу дослідження

1. Типи хмарних сервісів

Керуючись даними, що описані в [4], візьмемо до опрацювання такі типи хмарних сервісів, як:

- IaaS (Infrastructure-as-a-Service) – сервіс, що надається бізнесу у вигляді хмарних обчислень, сховища, мережі та системи віртуалізації. В межах даного сервісу бізнес не займається підтримкою серверної частини, а відповідає лише за операційну систему, програмне забезпечення, віртуальні машини, дані, сервіси, тощо. [6]
- PaaS (Platform-as-a-Service) – сервіс, у рамках якого провайдер забезпечує керування апаратними та програмними ресурсами, що стосуються саме розробки програмного забезпечення в хмарі. У цьому випадку бізнес повинен самостійно писати власне програмне забезпечення та розгортати додаткові програми, проте саме середовище для розгортання та управління підтримується постачальником хмарного сервісу [6];
- CaaS (Containers-as-a-Service) – сервіс, що надає бізнесу можливість керування всіма апаратними та програмними ресурсами для розробки власного програмного забезпечення за допомогою використання контейнерів. В рамках використання даного сервісу, командам із розробки замовника надається можливість налагоджувати власну інфраструктуру чи платформу для управління контейнерами та програмним забезпеченням [6];
- FaaS (Function-as-a-Service) – сервіс, у рамках якого постачальник хмарних сервісів бере на себе відповідальність за налаштування та підтримки середовищ розробки програмного забезпечення. З іншого боку, бізнес-замовнику необхідно буде лише скористатися розгорнутим програмним забезпеченням та писати свою власну розробку [7];
- SaaS (Software-as-a-Service) – сервіс, у рамках якого бізнес-замовнику надається доступ вже до готового програмного засобу, де постачальник хмарних сервісів самостійно робить такі речі, як оновлення програмного забезпечення, впровадження нового функціоналу, оновлення операційної системи, тощо. Тобто даний сервіс передбачає, що замовник може підключитися до консолі управління і відразу використовувати сервіс [6].

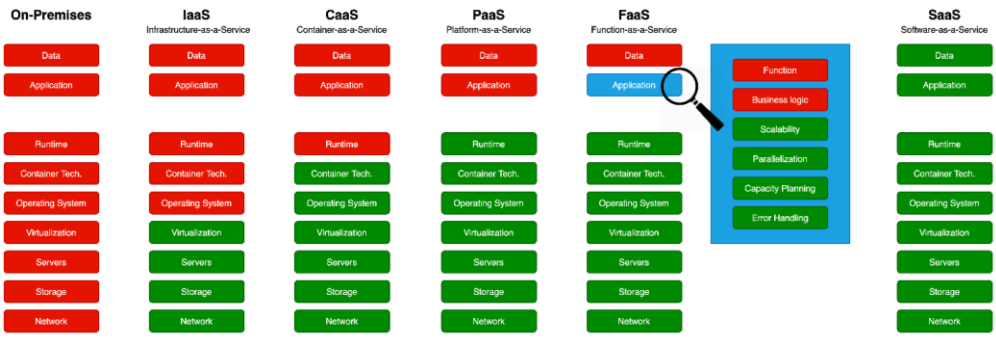

Рис. 1. Схема зображення зон відповідальності по кожному модулю взаємодії в розрізі різних типів хмарних сервісів

Для можливості наочно оцінити рівні залученості замовника та постачальника хмарного сервісу, рекомендуємо вам звернути увагу на рисунок (рис. 1) [8], що демонструє основні модулі, які представлені в

основі кожного типу хмарного сервісу та кольорами представлено, хто є відповідальним за кожний із модулів. Наприклад, «Зеленим» кольором позначено зону відповідальності постачальника хмарного сервісу, а «Червоним» - зону відповідальності бізнес-замовника.

Для того, щоб оцінити доцільність проведення даного дослідження варто поглянути на ринок хмарних сервісів. Щорічно частка хмарних сервісів у світі зростає, де навіть в період з 2022 року по 2024 роки, компанії України провели міграцію власних сервісів, обчислень, процес на ресурси хмарних провайдерів. Саме тому безпека хмарних сервісів та обробка даних на них є критично важливим питання, оскільки завдяки своєчасному виявленню прогалин в організації кібербезпеки хмарних сервісів можна попередити багатомільйонні збитки та репутаційні втрати компаній. Відповідно до рейтингу від компанії Gartner Magic Quadrant [9], до Топ-5 найпопулярніших хмарних провайдерів можна віднести: Amazon Web Services, Microsoft, Google, IBM та Alibaba Cloud (рис. 2).

Рис. 2. Рейтинг постачальників хмарних сервісів за версією компанії Gartner Magic Quadrant за 2024 рік

2. Основні критерії оцінювання

Оцінювання кіберзахищеності хмарних сервісів – це важливий процес у сучасному світі, оскільки від рівня захищеності залежить репутація компанії, цілісність та доступність конфіденційних даних, а також здатність замовникам бути впевненими, що їх персональні дані ніяким чином не будуть передані за межі обчислювальних систем. Додатково до захисту даних – це також відповідність частині положень Регламенту GDPR, щодо правил обробки персональних даних, у випадку, якщо діяльність постачальника хмарного сервісу ведеться на території Європейського Союзу. З основними кіберзагрозами, що стосуються хмарних сервісів, можна ознайомитися в [4].

Задля формування основних критеріїв оцінювання визначених типів хмарних сервісів у попередньому розділі, повертаємося до рисунку 1, де зображено 9 модулів, що відповідають за роботу кожного хмарного сервісу, а саме: Network module, Storage module, Servers module, Virtualization module, Operation System module, Container Technology module, Runtime module, Application module та Data module.

Детальний опис взаємодії кожного із вище вказаних модулів можна отримати в статті [10].

В основу наших існуючих критеріїв оцінювання, закладемо кожний із вище вказаних модулів, як ключовий критерій, що відповідає за частину функціонування хмарного сервісу. Перш ніж приступимо до формування критеріїв оцінювання стандартів, опишемо кожний із критеріїв.

1.Network module – модуль управління мережевими налаштуваннями, що передбачає оцінку стану захищеності хмарного сервісу від DDoS атак, сканування та виявлення вразливостей хмарного сервісу, тобто захист хмарного сервісу на рівні L3/L4 моделі OSI.

2.Storage module – модуль управління дисковим простором, що відповідає за оцінку можливостей хмарного сервісу, щодо побудови відмовостійких RAID масивів даних та здатність швидко відновлювати працездатність сервісу у випадку виникнення збою.

3.Servers module – модуль управління серверним обладнанням, що оцінює фізичний рівень доступу до серверного обладнання хмарного провайдера.

4.Virtualization module – модуль управління системи віртуалізації, що оцінює тип використовуваної системи віртуалізації, її налаштування та здатність протидії кібератакам.

5.Operation System module – модуль управління операційною системою, що оцінює, які налаштування встановлено на попередньо розгорнутих операційних системах, що підтримуються постачальником хмарного сервісу з метою виявлення недоліків та їх усунення.

6.Container Technology module – модуль управління системи контейнеризації, що визначає тип системи контейнеризації, місце зберігання контейнерів, середовище управління та її здатність протидіяти кібератакам.

7.Runtime module – модуль управління доступність сервісу, що відповідає за оцінку можливості системи працювати безперебійно навіть у випадку напливу кібератак, DDoS та ресурси хмарного сервісу.

8.Application module – модуль управління розгорнутими додатками на базі операційної системи чи контейнеру, що відповідає за оцінку стану захищеності розгорнутого додатку, що надається компаніям-замовникам як сервіс з метою виявлення прогалин захищеності додатку та їх виправлення.

9.Data module – модуль управління даними, що генеруються розгорнутими додатками, відповідає за перевірку стану захищеності даних при їх обробці на орендованих віртуальних середовищах провайдера хмарних сервісів.

Враховуючи, що загальними назвами модулів оцінювання – оцінка існуючих стандартів навряд чи буде об'єктивною, тому для коректної оцінки існуючих стандартів на ринку України, сформуємо 22 ключових позиції, яким мають відповідати стандарти. Важливою умовою відповідності кожному із нижче сформованих пунктів, є наявність рекомендації, щодо покращення кіберзахищеності оцінюваної частини

сервісів хмарного провайдера. Перелік 22 критеріїв оцінки передбачає наявність 2-х, 3-х або 4-х ключових позицій по кожному із описаних вище модулів оцінки, яким мають відповідати хмарні сервіси та стандарти. До критеріїв оцінки стандартів з кібербезпеки можна віднести:

- Network module:
- Оцінка можливості протидії DoS/DDoS атакам, на L3/L4/L7 рівнях моделі OSI.
- Оцінка можливості використання Load-BalancingдлябалансуванняnавантаженняміждекількомаVPC/VDS серверами.
- Storage module:
- Оцінювання можливості реплікації, створення резервних копій та клонування розгорнутих віртуальних машин.
- Оцінка можливості шифрування дискового простору та управління ключами шифрування.
- Servers module:
- Оцінка фізичної доступності до Центру обробки даних постачальника хмарних сервісів.
- Оцінка використовуваного в постачальника хмарного сервісу міжмережевого екрану та систем виявлення та попередження вторгнень.
- Virtualization module:
- Оцінка використовуваної системи віртуалізації та проведення аудиту її безпекових налаштувань.
- Оцінка можливостей системи віртуалізації з точки зору кібербезпеки.
- Оцінка системи авторизації в систему віртуалізації із використанням 2FA/MFA.
- Operation System module:
- Оцінка можливостей налаштування та генерації сповіщень системою під час виявлення певної події.
- Оцінка рівня доступу до кібербезпекових налаштувань операційної системи, якою управляє постачальник хмарного сервісу.
- Перевірка регулярності проведення оновлень операційної системи та її компонентів.
- Оцінка впровадженої політики пошуку вразливостей у підтримуваних операційних системах.
- Container Technology module:
- Оцінка рівня доступності контейнерів із різних середовищ, виділених під різних замовників.
- Перевірка послідовності дій при виявленні аномальної активності на базі розгорнутого контейнера чи кластера контейнерів.
- Runtime module:
- Оцінка рівня логування, що застосовується до підтримуваного програмного продукту.
- Оцінка впровадженої політики та системи управління вразливостями.
- Перевірка процесу проведення перевірки на вразливості відкритого коду програмного продукту, як на стадії розробки, так і під час використання.
- Application module:
- Оцінка проведення навчання по кібербезпеці співробітникам постачальника хмарних сервісів.
- Перевірка процедури підтримки власного програмного забезпечення шляхом випуску оновлень із виправленими недоліками та покращеними кібербезпековими функціями.
- Data module:
- Оцінка можливості проведення класифікації даних та їх типів, що обробляються на ресурсах постачальника хмарного сервісу.
- Перевірка можливості доступу до даних сторонніми особами, що обробляються на ресурсах постачальника хмарного сервісу.

Завдяки визначеним 22-м критеріям оцінки існуючих на сьогоднішній день стандартів та регламентів щодо забезпечення кібербезпеки, ми маємо можливість перевірити їх відповідність для використовуваних хмарних сервісів до кожного із модулів хмарного сервісу. Враховуючи результати даної оцінки, ми зможемо зрозуміти рівень відповідності стандарту чи регламенту до забезпечення кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури та за рахунок оцінки будемо мати змогу розглянути варіант актуальності розробки власної системи оцінювання хмарних сервісів на предмет їх кіберзахищеності, криптостійкості, відмовостійкості та здатності активно протидіяти кібератакам.

3. Порівняння існуючих стандартів

Для проведення порівняння було вибрано такі міжнародні стандарти та регламенти, а саме:

1.HIPAA,
2.PCI DSS,
3.SOC 2,
4.ISO 27001,
5.NIST 80-145,
6.GDPR.

Перед тим як проводити порівняння можливостей кожного із визначених стандартів, представимо короткий опис кожного із них, щоб надати інформацію про їх можливості та методи оцінки захищеності інформаційних систем.

Першим стандартом виступає HIPAA. HIPAA (Health Insurance Portability and Accountability Act) – це стандарт розроблений у США, що регулює процес захисту конфіденційної медичної інформації пацієнтів. Даний стандарт націлений на надання вимог до забезпечення конфіденційності, безпеки та передачі медичних даних. HIPAA впливає на декілька основних компонентів мережі компанії, які пов'язані з обробкою, зберіганням та передачею медичної інформації. Також стандарт надає опис положень з метою забезпечення відповідності встановленим вимогам безпеки та конфіденційності.

Компоненти мережі, на які впливає HIPAA:

1) сервери та сховища даних.
2) мережеві пристрої (роутери, комутатори, міжмережеві екрани).
3) VPN та шифрування каналів обміну інформацією.
4) IAM системи та контролю доступу.
5) пристрої кінцевих користувачів (робочі станції, мобільні пристрої).
6) системи резервного копіювання та відновлення даних.
7) системи антивірусного захисту.
8) системи аудиту та моніторингу подій.

Варто зауважити, що даний стандарт описує виключно вимоги до обробки медичних даних, проте не розповсюджується на інші типи даних.

Важливо розуміти, що стандарт HIPAA не надає конкретних технічних рекомендацій або інструкцій для забезпечення захисту медичних даних. Але стандарт націлений на формулювання загальних вимог, в рамках яких бізнес має працювати при обробці та захисту медичної інформації. [11]

Другий стандарт – PCI DSS. PCI DSS (Payment Card Industry Data Security Standard) – це стандарт, що розроблений для захисту даних платіжних карток. Він зобов'язує бізнеси, які зберігають, обробляють або передають інформацію про платіжні картки, дотримуватися вимог стандарту вимог для забезпечення конфіденційності та цілісності платіжних даних.

Компоненти мережі, на які впливає PCI DSS:

1) Системи обробки транзакцій.
2) Мережеві пристрої.
3) IAM системи та контролю доступу.
4) Пристрої кінцевих користувачів (робочі станції, мобільні пристрої).
5) Системи аудиту та моніторингу подій.

Варто зауважити, що даний стандарт описує виключно вимоги до обробки платіжних даних, проте не розповсюджується на інші типи даних.

На відміну від HIPAA, PCI DSS надає декілька конкретних технічних вимог і рекомендації для захисту даних платіжних карток. Наприклад:

- **Шифрування**: Використання протоколів TLS або IPsec для захисту даних при передачі.
- **Контроль доступу**: Використання рольової моделі доступу та визначених привілеїв доступу.
- **Сегментація мережі**: Розподіл мережі на логічні сегментовані частини для обмеження прямого доступу до критичних систем.[12]

Третій стандарт – SOC 2. SOC 2 (Service Organization Control 2) – це стандарт, що призначений для регулювання політик та процедур безпеки організацій, які обробляють дані власних клієнтів у хмарних сервісах або надають IT-послуги. SOC 2 оцінює, як компанія дотримується принципів безпеки, конфіденційності, доступності та цілісності даних.

Компоненти мережі, на які впливає SOC 2:

1) Сервери та сховища даних.
2) Мережеві пристрої (роутери, комутатори, міжмережеві екрани).
3) IAM системи та контролю доступу.
4) Пристрої кінцевих користувачів (робочі станції, мобільні пристрої).
5) Системи аудиту та моніторингу подій.

SOC 2, на відміну від PCI DSS, не надає конкретних технічних рекомендацій. Він більше орієнтований на оцінку того, як компанії впроваджують та дотримуються власних політик безпеки. Однак стандарт висуває загальні вимоги щодо безпеки, конфіденційності та цілісності даних, дозволяючи компаніям вибирати відповідні засоби для їх досягнення. [13]

Четвертий стандарт – ISO 27001. ISO/IEC 27001 – це міжнародний стандарт для управління інформаційною безпекою в компанії, що визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Метою ISO 27001 є забезпечення конфіденційності, цілісності та доступності інформації в організаціях шляхом впровадження комплексних заходів захисту, як фізичного, так і віртуального.

Компоненти мережі, на які впливає ISO 27001:

1) сервери та сховища даних.
2) мережеві пристрої (роутери, комутатори, міжмережеві екрани);
3) IAM системи та контролю доступу;
4) проведення сканування мережі та виявлення загроз;
5) пристрої кінцевих користувачів (робочі станції, мобільні пристрої).

Варто зауважити, що даний стандарт описує виключно вимоги до наземних обчислювальних потужностей бізнесу. В даному випадку використаємо в якості порівняння даних стандарт для оцінки фізичних та віртуальних складових хмарного сервісу.

Стандарт ISO 27001 надає конкретні вимоги для впровадження системи управління інформаційною безпекою (СУІБ), але він також залишає організаціям можливість самостійно вибирати заходи безпеки, виходячи з їхнього масштабу, типу діяльності та оцінки ризиків.

Основні рекомендації ISO 27001:

- управління ризиками: організація повинна провести оцінку ризиків, виявити потенційні загрози і вразливості та розробити плани мінімізації виявлених ризиків;
- впровадження контролю доступу: важливо впровадити системи, які забезпечують обмеження доступу до критичних даних і систем тільки для уповноважених користувачів;
- планування безперервності бізнесу: організація повинна мати плани для забезпечення безперервності бізнес-процесів у разі інцидентів, таких як збої в роботі критичних систем або при виникненні атаки/компрометації даних;
- постійне вдосконалення: одна з ключових вимог ISO 27001 – це постійний моніторинг, аналіз і вдосконалення системи управління інформаційною безпекою [14].

П'ятий стандарт – NIST 80-145. NIST SP 800-145 (National Institute of Standards and Technology Special Publication 800-145) – це один із стандартів компанії NIST, що надає визначення терміну хмарних обчислень і описує основні моделі використовуваних хмарних сервісів із варіантами їх розгортання. Даний документ розроблений для стандартизації концепцій, пов'язаних із використанням хмарних обчислень, щоб допомогти бізнесу краще розуміти, як використовувати хмарні технології задля покращення власних процесів і безпеки.

Компоненти мережі, на які впливає NIST SP 800-145:

1) хмарні платформи та інфраструктура;
2) мережеві пристрої (роутери, комутатори, міжмережеві екрани);
3) системи зберігання даних;
4) IAM системи та контролю доступу.

NIST SP 800-145 не містить визначених технічних рекомендацій щодо впровадження хмарних сервісів, проте надає визначення та описує основні концепції хмарних обчислень. Ці визначення можуть використовуватися як основа для розробки більш детальних

політик і процедур щодо використання хмарних технологій у межах бізнесу.

Основні рекомендації NIST SP 800-145:

• визначення моделі хмарних обчислень: бізнес має вибрати відповідну модель хмарних обчислень (IaaS, PaaS або SaaS) залежно від власних потреб і рівня контролю, який потрібно зберегти;

• вибір моделі розгортання: потрібно вибрати найбільш підходящий тип хмари (Public, Private, Hybrid або Community) залежно від вимог до безпеки бізнесу та конфіденційності даних, що передбачені внутрішніми політиками безпеки;

• управління доступом і ресурсами: бізнесу рекомендується розробити політики для контролю доступу до хмарних сервісів і моніторингу використання ресурсів хмарного провайдера. [5]

Шостий стандарт – Регламент GDPR. GDPR (General Data Protection Regulation) – це Регламент ЄС, що регулює обробку та захист персональних даних фізичних осіб.

Він був прийнятий для посилення контролю над даними користувачів і забезпечення їх конфіденційності. GDPR застосовується до всіх організацій, які обробляють дані громадян ЄС, незалежно від їх розташування по світу.

Компоненти мережі, на які впливає GDPR:

1) сервери та бази даних;
2) мережеві пристрої (роутери, комутатори, міжмережеві екрани);
3) IAM системи та контролю доступу;
4) системи резервного копіювання та відновлення даних;
5) системи аудиту та моніторингу подій.

Варто зауважити, що даний Регламент розповсюджується тільки на країни ЄС та громадян ЄС та у випадку, якщо ваш бізнес знаходиться за межами ЄС і ви не обробляєте дані громадян ЄС, то положення даного стандарту не діють.

GDPR не надає чітких технічних інструкцій або рекомендацій для впровадження заходів безпеки. Натомість він встановлює загальні принципи та вимоги, яких бізнес має дотримуватися, залишаючи їм свободу вибору підходів і технологій для досягнення відповідності положенням даного Регламенту.

Основні рекомендації Регламенту GDPR:

• отримання згоди на обробку власних персональних даних;

• впровадження заходів захисту: бізнесу рекомендується впроваджувати такі заходи, як шифрування, контроль доступу, багатофакторна автентифікація для захисту персональних даних клієнтів;

• формування оповіщень про порушення відповідальні органи: рекомендується створити чіткі процедури для виявлення порушень безпеки і швидкого оповіщення про них наглядових органів та суб'єктів даних;

• оцінка ризиків: бізнес проводить оцінку ризиків, пов'язаних із обробкою персональних даних, і вживати відповідних заходів для зниження рівня впливу даних ризиків.[15]

Завдяки наданню коротких відомостей щодо оцінюваних стандартів та безпеки є можливість оцінити їх відповідність до розроблених критеріїв оцінювання, що будуть представлені (табл. 1).

Таблиця 1

Порівняння існуючих стандартів оцінювання хмарних сервісів відповідно до визначених критеріїв оцінювання

Модуль	**Назва оцінки**	**Оцінювані стандарти та Регламенти**					
		HIPAA	**PCI-DSS**	**SOC 2**	**ISO 27001**	**NIST 80-145**	**GDPR**
Network module	Оцінка можливості протидії DoS/DDoS атакам, на L3/L4/L7 рівнях моделі OSI	-	+	+	+	+	-
	Оцінка можливості використання Load-Balancing для балансування навантаження між декількома VPC/VDS серверами.	+	+	+	+	+	+
Storage module	Оцінювання можливості реплікації, створення резервних копій та клонування розгорнутих віртуальних машин.	+	+	+	+	+	+
	Оцінка можливості шифрування дискового простору та управління ключами шифрування.	+	+	+	+	+	+
Servers module	Оцінка фізичної доступності до Центру обробки даних постачальника хмарних сервісів.	+	+	+	+	-	-
	Оцінка використовуваного в постачальника хмарного сервісу міжмережевого екрану та систем виявлення та попередження вторгнень.	+	+	+	+	+	+
Virtualization module	Оцінка використовуваної системи віртуалізації та проведення аудиту її безпекових налаштувань.	+	+	+	+	-	-
	Оцінка можливостей системи віртуалізації з точки зору кібербезпеки.	+	+	+	+	-	-
	Оцінка системи авторизації в систему віртуалізації із використанням 2FA/MFA.	+	+	+	+	-	-

Модуль	Назва оцінки	Оцінювані стандарти та Регламенти					
		HIPAA	PCI-DSS	SOC 2	ISO 27001	NIST 80-145	GDPR
Operation System module	Оцінка можливостей налаштування та генерації сповіщень системою під час виявлення певної події.	+	+	+	+	-	-
	Оцінка рівня доступу до кібербезпекових налаштувань операційної системи, якою управляє постачальник хмарного сервісу.	+	+	+	+	-	-
	Перевірка регулярності проведення оновлень операційної системи та її компонентів.	+	+	+	+	-	-
	Оцінка впровадженої політики пошуку вразливостей у підтримуваних операційних системах.	+	+	+	+	-	-
Container Technology module	Оцінка рівня доступності контейнерів із різних середовищ, виділених під різних замовників.	-	+	+	+	-	-
	Перевірка послідовності дій при виявленні аномальної активності на базі розгорнутого контейнера чи кластера контейнерів.	-	+	+	+	-	-
Runtime module	Оцінка рівня логування, що застосовується до підтримуваного програмного продукту.	+	+	+	+	-	+
	Оцінка впровадженої політики та системи управління вразливостями.	+	+	+	+	-	+
	Перевірка процесу проведення перевірки на вразливості відкритого коду програмного продукту, як на стадії розробки, так і під час використання.	-	+	+	+	-	-
Application module	Оцінка проведення навчання по кібербезпеці співробітникам постачальника хмарних сервісів.	+	+	+	+	-	+
	Перевірка процедури підтримки власного програмного забезпечення шляхом випуску оновлень із виправленими недоліками та покращеними кібербезпековими функціями.	+	+	+	+	-	-
Data module	Оцінка можливості проведення класифікації даних та їх типів, що обробляються на ресурсах постачальника хмарного сервісу.	+	+	+	+	-	+
	Перевірка можливості доступу до даних сторонніми особами, що обробляються на ресурсах постачальника хмарного сервісу.	+	+	+	+	-	+
Наявність рекомендацій для кожного із оцінювальних модулів		-	Част.	-	Част.	-	-

Висновки. В даній статті було проведено аналіз існуючих на сьогоднішній день стандартів, що використовуються для висування вимог щодо забезпечення працездатності інформаційних середовищ. Враховуючи, що кожен із стандартів має свій рівень впливу на інформаційну інфраструктуру, було розроблено критерії оцінювання стандартів, щоб продемонструвати сучасні реалії при яких в існуючих стандартах відсутня повна відповідність всім необхідним полям та критеріям щодо оцінки стану захищеності хмарних сервісів об'єктів інформаційних систем. Також за результатами аналізу було побудовано таблицю, що містить повну інформацію щодо проведеного аналізу оцінюваних хмарних сервісів. Разом з цим виявлено, що існуючі стандарти та регламенти в сфері Кібербезпеки не містять чітких рекомендацій, що чітко описують послідовність дій у разі відповідності/невідповідності положенням стандарту/регламенту інформаційних систем.

Окрім цього, із всіх перерахованих стандартів тільки два з них напряму стосуються хмарних сервісів, а всі інші розроблялися для наземного розгортання, що дає нам зрозуміти, що на поточний момент часу не існує чіткого переліку критеріїв оцінювання кіберзахищеності хмарних сервісів із чітко визначеними рекомендаціями, що будуть застосовані для покращення захищеності кожного із модулів хмарних сервісів.

Список літератури

[1]. How Mainframe Computers Have Changed Over the Years? [Electronic resource] : Maintec Technologies. Mode of access: https: // www.linkedin.com /

pulse/how-mainframe-computers-have-changed-over-years/ (date of access: 01.09.2024).

[2]. Keith D. Foote. A Brief History of Cloud Computing [Electronic resource] / Keith D. Foote // Dataversity. 2021. Mode of access: https://www.dataversity.net/brief-history-cloud-computing/ (date of access: 02.09.2024).

[3]. Tim Matthews. The Origins of Web Security and the Birth of Security Socket Layer (SSL) Protocol [Electronic resource] / Tim Matthews // Exabeam. 2019. Mode of access: https://www.exabeam.com/blog/infosec-trends/the-origins-of-web-security-and-the-birth-of-security-socket-layer-ssl-protocol/ (date of access: 03.09.2024).

[4]. 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. pp. 110-117. Mode of access: https://www.sciencedirect.com/science/article/pii/S1877050922009164 (date of access: 04.09.2024).

[5]. Peter Mell. The NIST Definition of Cloud Computing / Peter Mell, Tim Grance// NIST. 2011. Mode of access: https: // csrc.nist.gov / publications/detail/sp/800-145/final (date of access: 04.08.2024).

[6]. PaaS vs. IaaS vs. SaaS vs. CaaS: How are they different? [Electronic resource]: Google. Mode of access: https://cloud.google.com/learn/paas-vs-iaas-vs-saas (date of access: 05.09.2024).

[7]. What is function as a service (FaaS)? [Electronic resource]: IBM. Mode of access: https://www.ibm.com/topics/faas (date of access: 06.09.2024).

[8]. Sacha Roger. IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS — What's the difference? / Sacha Roger // Medium. 2020. Mode of access: https: // stample.com/link/ stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference (date of access: 06.09.2024).

[9]. Google is a Leader for the 5th consecutive year, in the 2024 Gartner® Magic Quadrant™ for Cloud AI Developer Services (CAIDS) [Electronic resource] : Google Cloud. Mode of access: https://cloud.google.com/resources / gartner-caids-mq-report (date of access: 07. 09.2024).

[10]. Pedchenko Y. Mathematical model of security cloud services assessment / Shulha Volodymyr, Korchenko Oleksandr, Ivanchenko Yevheniia, Vyshnevska Natalia, Pedchenko Yevhenii, Petrovska Mari // Problemsoff Scientific, Technical and Legal Support for Cybersecurity in The Modern World. UKEN. Krakow, 2024. pp. 5-12.

[11]. Health Information Privacy [Electronic resource]: U.S. Department of Health and Human Services. Mode of access: https://www.hhs.gov/hipaa/index.html (date of access: 08.09.2024).

[12]. PCI-DSS [Electronic resource]: PCI Security Standards Council. Mode of access: https://www.pcisecuritystandards.org/ (date of access: 09.09.2024).

[13]. SOC 2 [Electronic resource]: SOC System and Organization Controls. Mode of access: https://soc2.co.uk/ (date of access: 10.09.2024).

[14]. ISO/IEC 27001:2022 [Electronic resource]: ISO. Mode of access: https://www.iso.org/standard/27001 (date of access: 11.09.2024).

[15]. General Data Protection Regulation (EU GDPR) [Electronic resource]: GDPR Text. — Mode of access: https://gdpr-text.com/uk/ (date of access: 12.09.2024).

УДК 004.056.5

Ivanchenko I., Pedchenko Y. Analysis of models and methods for assessing the state of cybersecurity of cloud services of information infrastructure objects

Abstract. *This article describes the analysis of existing standards in the field of cybersecurity aimed at providing requirements for the functioning of the company's information environment. The article will describe cloud services, their types, and the structural model of each of the selected types. Based on the analysis of the structural models of cloud service types, the main evaluation criteria will be determined. To assess the compliance of cybersecurity standards with the defined evaluation criteria, a comparative analysis will be carried out using these criteria.*

Keywords: *cybersecurity, information security, assessment, model, method, audit, CSP, Cloud Service Provider, IaaS, PaaS, CaaS, FaaS, SaaS.*

Іванченко Ігор Сергійович, к.т.н., доцент, доцент кафедри технічного захисту інформації Національного авіаційного університету, Україна.

Ihor Ivanchenko, Ph.D., Associate Professor, Associate Professor of the Technical Information Protection Department of the National Aviation University, Ukraine.

Педченко Євгеній Максимович, аспірант, асистент кафедри кібербезпеки Національного авіаційного університету, Україна.

Yevhenii Pedchenko, graduate student, assistant of the cyber security department of the National Aviation University, Ukraine.

Отримано *3 червня 2024 року,* затверджено редколегією *26 червня 2024 року*