НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«БЕЗПЕКА ХМАРНИХ ОБЧИСЛЕНЬ: АНАЛІЗ РИЗИКІВ ТА МЕТОДІВ ЗАХИСТУ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Тарасюк Михайло Юрійович

Керівник: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Рецензент: к.т.н., доцент
Бойко Віктор Дмитрович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Тарасюку Михайлу Юрійовичу

1. Тема роботи: «Безпека хмарних обчислень: аналіз ризиків та методів захисту»
Керівник роботи: к.т.н, доцент Ахмаметьєва Ганна Валеріївна
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16 » вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Приміт ка
1	Аналіз предметної області та пошук науково-технічної інформації за темою роботи	Вересень-жовтень 2024	
2	Узгодження теми з науковим керівником, формулювання мети завдань дослідження	Листопад 2024	
3	Робота над першим розділом	Листопад-грудень 2024	
4	Робота над другим розділом	Січень-лютий 2025	
5	Робота над третім розділом	Лютий-березень 2025	
6	Уточнення подальшого обсягу роботи та його коригування	Березень-травень 2025	
7	Оформлення звітної частини	Травень 2025	
8	Захист роботи	12.06.2025	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Безпека хмарних обчислень: аналіз ризиків та методів захисту» виконана для здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» в освітній програмі «Кібербезпека», містить 12 ілюстрацій, 2 таблиці та 22 використані літературні джерела, наведені у переліку посилань. Робота виконана на 66 сторінках загального тексту, з яких 56 сторінки основного тексту.

Метою дослідження є всебічний аналіз безпекових аспектів у контексті хмарних обчислень на прикладі сервісу Amazon Web Services (AWS), зокрема платформи Amazon EC2, а також вивчення ключових принципів організації безпеки у хмарних інфраструктурах. У роботі детально розглядаються основні загрози, які притаманні хмарним обчисленням, та методи їх ідентифікації і мінімізації ризиків.

Особлива увага приділена аналізу моделей побудови хмарних сервісів і відповідних моделей безпеки, а також специфіці забезпечення захисту даних, що зберігаються і передаються у хмарі. Розглянуто роль механізмів контролю доступу, їх ефективність та вплив на загальний рівень безпеки системи. У роботі описані сучасні методи шифрування інформації в хмарних середовищах, а також додаткові заходи захисту, які враховують життєвий цикл даних – від їх створення до видалення.

Праця має прикладну цінність і може бути використана для підвищення рівня безпеки інформаційних систем на підприємствах, що використовують хмарні технології, а також для подальших досліджень у галузі кібербезпеки хмарних сервісів.

ХМАРА, AMAZON EC2, ХМАРНА БЕЗПЕКА, ХМАРНІ ОБЧИСЛЕННЯ, ПАРАМЕТРИ БЕЗПЕКИ, ЗАХИСТ ДАНИХ, КОНТРОЛЬ ДОСТУПУ, ШИФРУВАННЯ, АНАЛІЗ РИЗИКІВ.

.

ABSTRACT

The qualification work titled “Cloud Computing Security: Risk Analysis and Protection Methods” is prepared to obtain the first (bachelor’s) level of higher education in the specialty 125 “Cybersecurity” under the educational program “Cybersecurity”, includes 12 illustrations, 2 tables and references 22 literary sources listed in the bibliography. The work consists of 66 pages of general text, including 56 pages of the main text.

The aim of the study is a comprehensive analysis of security aspects within cloud computing, using the example of the Amazon Web Services (AWS) platform, specifically Amazon EC2, as well as the examination of key principles for organizing security in cloud infrastructures. The work thoroughly examines the main threats inherent to cloud computing and methods for identifying and mitigating associated risks.

Particular attention is given to analyzing cloud service models and corresponding security frameworks, as well as the specifics of ensuring data protection stored and transmitted in the cloud. The role and effectiveness of access control mechanisms are reviewed, along with their impact on the overall system security level. The study describes modern methods of data encryption in cloud environments, as well as additional protection measures considering the data lifecycle – from creation to deletion.

This work has practical value and can be used to enhance the security level of information systems in enterprises employing cloud technologies, as well as for further research in the field of cloud service cybersecurity.

CLOUD, AMAZON EC2, CLOUD SECURITY, CLOUD COMPUTING, SECURITY PARAMETERS, DATA PROTECTION, ACCESS CONTROL, ENCRYPTION, RISK ANALYSIS.

ЗМІСТ

ВСТУП

У сучасному цифровому світі хмарні обчислення стали ключовим елементом інформаційної інфраструктури. Завдяки своїй гнучкості, масштабованості та економічній доцільності, хмарні сервіси активно використовуються як в бізнесі, так і в державному секторі. Водночас стрімке зростання обсягів даних, що передаються та зберігаються у хмарі, супроводжується зростанням ризиків, пов’язаних із їх безпекою.

Безпека хмарних обчислень є критично важливою складовою кібербезпеки загалом, оскільки від неї залежить захист конфіденційної, комерційної та персональної інформації. Перенесення обробки даних у хмарне середовище вимагає ретельного аналізу потенційних загроз, ефективного управління ризиками, дотримання стандартів відповідності (комплаєнсу) та впровадження сучасних технічних і організаційних заходів захисту.

Мета роботи полягає в аналізі ризиків хмарної безпеки та дослідженні сучасних методів захисту в Amazon EC2 з урахуванням технічних і правових аспектів.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- визначити поняття та основні характеристики хмарного сервісу Amazon EC2, його функціональність і особливості використання;
- дослідити основні принципи забезпечення безпеки в хмарній інфраструктурі Amazon, включаючи моделі відповідальності та інструменти захисту;
- проаналізувати методи організації управління безпекою хмарних сервісів, включаючи стратегії та підходи до впровадження безпечних практик;
- оцінити підходи до управління ризиками безпеки в хмарній платформі Amazon, включаючи ідентифікацію, аналіз і пом’якшення ризиків;
- визначити вимоги комплаєнсу та юридичні аспекти, пов’язані з використанням хмарних сервісів, включаючи відповідність стандартам і регуляціям;

- дослідити процеси аудиту безпеки хмарних сервісів та використання інструментів Cloud Security Alliance (CSA) для оцінки безпеки;
- проаналізувати особливості хмарного зберігання та передачі даних, включаючи архітектуру та технології, що застосовуються в Amazon EC2;
- розробити методи захисту даних у хмарі, включаючи технології та практики для забезпечення конфіденційності та цілісності даних;
- дослідити методи шифрування в моделях IaaS, PaaS та SaaS, їх особливості та застосування в хмарних сервісах Amazon;
- проаналізувати процеси керування ключами шифрування, додаткові параметри захисту даних у Amazon EC2.

Об’єкт дослідження – хмарні обчислення як процес надання інформаційно-технологічних ресурсів, зокрема сервіс Amazon Elastic Compute Cloud (EC2) у складі екосистеми Amazon Web Services (AWS), що породжує проблемну ситуацію, пов’язану із забезпеченням безпеки даних та інфраструктури в хмарному середовищі.

Предмет дослідження – параметри безпеки хмарного сервісу Amazon EC2, включаючи політики контролю доступу, механізми шифрування, управління ключами, життєвий цикл захисту даних, а також відповідність правовим і нормативним вимогам.

Практичне значення отриманих результатів – результати дослідження мають прикладну цінність і можуть бути використані для підвищення рівня безпеки інформаційних систем на підприємствах, що застосовують хмарні технології, зокрема Amazon EC2. Запропоновані методи управління ризиками, шифрування, контролю доступу та аудиту безпеки сприяють зниженню вразливостей і забезпеченню конфіденційності, цілісності та доступності даних. Результати також можуть слугувати основою для подальших досліджень у галузі кібербезпеки хмарних сервісів, а також для розробки практичних рекомендацій щодо впровадження безпечних хмарних рішень у різних сферах діяльності.

1 ХМАРНА ІНФРАСТРУКТУРА AMAZON EC2: ОСНОВИ ТА ФУНКЦІОНАЛЬНІСТЬ

1.1 Поняття хмарного сервісу Amazon EC2

Хмарні обчислення – це сучасна модель надання IT-ресурсів, що базується на принципах абстракції та автоматизації. Абстракція дозволяє відокремити ресурси від фізичної інфраструктури, формуючи уніфікований пул обчислювальних потужностей. Автоматизація забезпечує гнучке керування цими ресурсами – їхнє швидке виділення, масштабування або вилучення.

На відміну від традиційної віртуалізації, хмара передбачає високий рівень оркестрації та гнучкості, що робить її більш ефективною для бізнесу. Основними перевагами хмарних обчислень є зменшення витрат, швидке впровадження інновацій та стійкість до змін навантаження.

Amazon Web Services (AWS) є однією з найпопулярніших глобальних хмарних платформ, яка охоплює широкий спектр сервісів у моделях IaaS і PaaS – від обчислень і сховищ до машинного навчання, аналітики та IoT [1].

Amazon EC2 (Elastic Compute Cloud) – ключовий сервіс AWS, який забезпечує користувачів віртуальними машинами з можливістю вибору операційної системи, процесора, типу зберігання та мережевих характеристик. EC2 надає понад 750 типів інстансів, підтримку процесорів Intel, AMD, Arm, EC2 Mac, а також мережу з пропускною здатністю до 400 Гбіт/с, що забезпечує високу продуктивність для будь-яких сценаріїв – від SAP і HPC до машинного навчання та Windows-додатків [2].

Сервіси AWS вирізняються широкими функціональними можливостями. Користувачі можуть обирати оптимальні інструменти для баз даних, зберігання, обробки даних тощо. AWS підтримує найбільшу спільноту клієнтів і партнерів, включаючи стартапи, корпорації та державні установи, а також партнерську мережу з тисячами інтеграторів і розробників [2].

Платформа також гарантує високий рівень безпеки: понад 300 вбудованих сервісів і функцій, підтримка 143 сертифікатів відповідності, а також відповідність вимогам фінансових і оборонних установ [3].

Завдяки інноваціям на зразок AWS Lambda (безсерверні обчислення) та Amazon SageMaker (машинне навчання), компанія постійно розширює горизонти хмарних технологій, забезпечуючи перевірену надійність для критично важливих додатків.

Amazon Web Services надає найбільш широкий набір функцій серед усіх постачальників хмарних рішень, що дозволяє охоплювати найрізноманітніші сценарії використання – від базових інфраструктурних потреб до впровадження передових технологій. Зокрема, користувачам доступний великий вибір баз даних, спеціалізованих під різні задачі: реляційні, документно-орієнтовані, графові, таймсерієві тощо. Це забезпечує можливість оптимального підбору інструментів для конкретних типів навантажень, що підвищує ефективність роботи застосунків і знижує витрати на обчислювальні ресурси. Завдяки такому підходу AWS підтримує гнучку архітектуру систем, яка адаптується під потреби клієнтів.

EC2-інстанс представляє собою віртуальний сервер, який працює у хмарному середовищі Amazon Web Services, як зображено на рисунку 1.1.

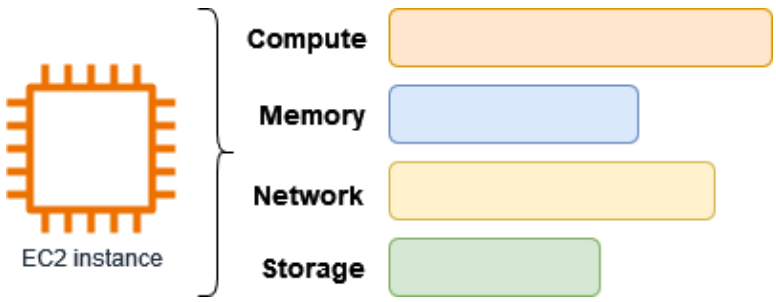

Рисунок 1.1 – Віртуальний сервер, який працю у хмарному середовищі Amazon Web Services.

Однією з ключових переваг AWS є її масштабна та динамічна спільнота, яка об'єднує мільйони активних клієнтів по всьому світу. До цієї екосистеми входять як малі стартапи, так і великі транснаціональні корпорації, а також державні

установи, що свідчить про універсальність та надійність платформи. Партнерська мережа AWS охоплює тисячі системних інтеграторів, консультантів і технологічних провайдерів, які надають спеціалізовані послуги з впровадження, налаштування та супроводу рішень на базі AWS. Крім того, десятки тисяч незалежних постачальників програмного забезпечення (Independent Software Vendors, ISV) адаптують свої продукти до інфраструктури AWS, що дає змогу клієнтам легко інтегрувати додаткові інструменти та сервіси у свої хмарні середовища. Завдяки потужній партнерській екосистемі та постійній підтримці з боку спільноти, AWS забезпечує високий рівень експертизи та допомоги користувачам на всіх етапах реалізації проєктів – від планування до масштабування та оптимізації.

Платформа Amazon Web Services спочатку проєктувалася як надійне, масштабоване та захищене середовище для обробки й зберігання даних у хмарі. Архітектура базової інфраструктури відповідає найвищим міжнародним вимогам до безпеки, зокрема стандартам, що застосовуються у банківському секторі, оборонній промисловості та державному управлінні. AWS забезпечує багаторівневий захист даних на фізичному, операційному та прикладному рівнях, а також пропонує понад 300 спеціалізованих сервісів і функцій, спрямованих на реалізацію політик захисту, контролю доступу, шифрування, моніторингу та дотримання нормативних вимог. Крім того, платформа підтримує понад 140 міжнародних стандартів та сертифікатів, зокрема ISO/IEC 27001, SOC 1/2/3, PCI DSS, HIPAA та інші, що засвідчує її відповідність вимогам регуляторів у багатьох сферах [3].

Однією з головних переваг AWS є її орієнтація на постійне впровадження передових технологій, що дозволяє клієнтам пришвидшити інноваційні процеси та розробку нових продуктів. AWS надає доступ до інструментів, які суттєво спрощують експериментування та скорочують цикл створення програмних рішень. Так, у 2014 році компанія стала піонером у сфері безсерверних обчислень, запровадивши сервіс AWS Lambda, який дозволяє запускати програмний код без попереднього налаштування або керування серверною інфраструктурою. Крім

того, для підтримки розвитку в галузі штучного інтелекту та машинного навчання було створено Amazon SageMaker – повністю керований сервіс, що надає розробникам та дослідникам без досвіду у Data Science інструменти для швидкої побудови, тренування та впровадження моделей машинного навчання.

За понад 18 років функціонування AWS зарекомендувала себе як лідер ринку хмарних технологій завдяки стабільності, масштабованості та високій продуктивності своїх сервісів. Інженерні рішення, що лежать в основі платформи, ретельно оптимізовані для забезпечення безперебійної роботи найважливіших бізнес-додатків в умовах різного навантаження. Сервіси AWS активно використовуються мільйонами клієнтів у всьому світі, серед яких представники комерційного, державного та наукового секторів. Здатність платформи ефективно функціонувати як у малих проєктах, так і у масштабних корпоративних рішеннях підтверджує її універсальність та надійність, що є вирішальними критеріями для компаній при виборі хмарного провайдера.

Одним із ключових напрямів діяльності Amazon Web Services є сприяння розвитку цифрових навичок користувачів та фахівців, зацікавлених у впровадженні хмарних технологій. З цією метою було створено освітню платформу AWS Training and Certification, а також онлайн-академію AWS Skill Builder, яка надає доступ до широкого спектра навчальних матеріалів, курсів, практичних лабораторій та сертифікаційних програм. Ця екосистема навчання охоплює як базовий рівень знань для початківців, так і поглиблену підготовку для досвідчених спеціалістів з архітектури хмарних рішень, DevOps, безпеки, аналізу даних та машинного навчання [4].

Навчальні програми створюються експертами AWS з урахуванням сучасних вимог ринку праці та постійно оновлюються відповідно до технологічних змін. Онлайн-платформа Skill Builder пропонує як безкоштовні, так і платні курси, що дозволяє широкому колу слухачів отримати необхідні знання у зручному темпі. Особливу цінність мають інтерактивні тренажери, які імітують роботу з реальним середовищем AWS, дозволяючи слухачам не лише засвоїти теоретичний матеріал, а й закріпити його на практиці.

Крім того, AWS активно підтримує процес офіційного підтвердження знань через сертифікацію. Існує декілька рівнів сертифікації – від початкового (Foundational) до професійного (Professional) та спеціалізованого (Specialty), що дозволяє фахівцям демонструвати свою кваліфікацію на глобальному ринку праці. Така система є цінною як для окремих спеціалістів, так і для компаній, які прагнуть забезпечити високий рівень компетентності своїх команд у хмарних технологіях [5].

AWS Training and Certification відіграє важливу роль у формуванні висококваліфікованих IT-кадрів і є невід'ємною складовою глобальної стратегії AWS щодо підвищення цифрової грамотності та адаптації підприємств до викликів цифрової трансформації.

1.2 Основні принципи безпеки у хмарі Amazon

Надійний захист інформаційних ресурсів є фундаментальним елементом, що забезпечує успішне впровадження цифрових трансформацій та інновацій у сучасних організаціях. Amazon Web Services (AWS) приділяє першочергову увагу безпеці, створюючи середовище, яке не лише відповідає найвищим стандартам, але й сприяє активному розвитку бізнесу завдяки ефективним механізмам ідентифікації, контролю доступу та відповідності нормативним вимогам. Безпека є стратегічним пріоритетом AWS і лежить в основі всієї архітектури платформи, що проектувалась як найбезпечніша глобальна хмарна інфраструктура для розробки, міграції та управління різноманітними додатками та робочими навантаженнями.

Інфраструктура AWS підтримує широкий спектр сервісів безпеки – понад 300 функцій і сервісів, які охоплюють захист даних, моніторинг, керування ідентичністю, аудит та відповідність міжнародним стандартам. Завдяки цьому мільйони клієнтів, включно з організаціями, які працюють у найбільш чутливих сферах, таких як державні установи, медичні заклади та фінансові служби, довіряють AWS для захисту своїх критичних систем і даних [6].

AWS активно впроваджує інноваційні рішення, що дозволяють клієнтам безпечно та з упевненістю масштабувати свої бізнес-процеси. Хмарна інфраструктура в поєднанні з потужними інструментами безпеки та партнерською мережею дає змогу інтегрувати комплексні рішення контролю доступу, шифрування, моніторингу загроз і реагування на інциденти [6]. Це дозволяє організаціям безперешкодно впроваджувати інновації, одночасно підтримуючи високий рівень кібербезпеки.

Основу хмарної безпеки AWS становить застосування міжнародно визнаних стандартів та рамкових документів. Одним із ключових таких документів є NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США (NIST). Цей фреймворк містить структурований набір рекомендацій і найкращих практик для зниження організаційних кіберризиків, які допомагають підприємствам ефективно управляти інформаційною безпекою. NIST Cybersecurity Framework був створений за ініціативою адміністрації президента США, щоб сформувати єдину термінологію та стандарти для органів державної влади, які зазнають постійних кіберзагроз. Цей документ став універсальним керівництвом для фахівців із безпеки та менеджменту, що дозволяє створити спільну мовну базу і стандартизовані підходи до захисту [7].

Згідно з дослідженнями 2016 року, близько 70% опитаних організацій визнали NIST Cybersecurity Framework найпопулярнішою методологією для побудови надійної системи кібербезпеки. Його було перекладено багатьма мовами, включно з українською, що свідчить про глобальне застосування стандарту. Крім державних структур і підприємств критичної інфраструктури, цей фреймворк активно впроваджується і у комерційному секторі, слугуючи орієнтиром для побудови ефективної системи інформаційної безпеки.

NIST Cybersecurity Framework базується на ієрархічній структурі основних принципів, які охоплюють п’ять ключових функцій: виявлення (Identify), захист (Protect), виявлення загроз (Detect), реагування (Respond) і відновлення (Recover). Ця модель дозволяє організаціям системно підходити до управління безпекою,

формуючи цілісну та адаптивну стратегію кіберзахисту, яка відповідає сучасним викликам і загрозам [8].

Таким чином, Amazon Web Services не лише забезпечує фізичний і технічний захист своїх центрів обробки даних, а й підтримує комплексний підхід до кібербезпеки, який базується на міжнародних стандартах та передових практиках. Це дозволяє клієнтам впевнено розвивати інноваційні сервіси, мінімізуючи ризики, пов’язані з безпекою в хмарі.

Застосування моделі NIST Cybersecurity Framework у середовищі AWS забезпечує системний підхід до інформаційної безпеки. Кожна з п’яти функцій виконує важливу роль у створенні надійної захисної інфраструктури:

Identify (Визначення) – передбачає аналіз активів, їхніх вразливостей, а також оцінку ризиків для формування чіткої картини безпекового профілю організації. У AWS для цього застосовуються сервіси, що забезпечують керування доступом і аудит конфігурацій ресурсів.

Protect (Захист) – полягає у реалізації технічних та адміністративних заходів, спрямованих на обмеження доступу до критичних даних і сервісів, шифрування інформації, а також запобігання кібератакам.

Detect (Виявлення) – спрямована на своєчасне ідентифікування потенційних загроз і аномалій у роботі систем. Інструменти моніторингу й аналізу безпекових подій дозволяють швидко отримувати інформацію про інциденти.

Respond (Реагування) – охоплює заходи з оперативного реагування на виявлені інциденти, локалізації проблем та мінімізації негативних наслідків для бізнесу.

Recover (Відновлення) – спрямована на відновлення працездатності систем та даних після інцидентів, забезпечуючи безперервність бізнес-процесів.

Впровадження такої структури допомагає організаціям ефективно протистояти сучасним кіберзагрозам, організовувати контроль безпеки і послідовно підвищувати рівень захисту.

Для ефективного управління безпекою у хмарному середовищі AWS застосовує принципи, що базуються на міжнародно визнаних стандартах, зокрема

на NIST Cybersecurity Framework [9]. Цей фреймворк структурує підходи до інформаційної безпеки за п’ятьма основними функціями: виявлення, захист, реагування, відновлення та ідентифікація. У таблиці 1.1 наведено, як AWS реалізує кожну з цих функцій, забезпечуючи комплексний та системний підхід до кібербезпеки.

Таблиця 1.1 – Основні функції безпеки у хмарі AWS за моделлю NIST Cybersecurity Framework

Функція	Опис	Приклади сервісів AWS
Identify	Визначення, оцінка та управління ризиками безпеки	AWS Identity and Access Management (IAM), AWS Config
Protect	Захист ресурсів, обмеження доступу, шифрування	AWS Key Management Service (KMS), AWS Shield, AWS WAF
Detect	Виявлення потенційних інцидентів та загроз	Amazon GuardDuty, AWS CloudTrail, AWS Security Hub
Respond	Реагування на інциденти, їх локалізація та мінімізація шкоди	AWS Systems Manager Incident Manager, AWS Lambda
Recover	Відновлення нормальної роботи після інцидентів	AWS Backup, AWS Elastic Disaster Recovery

Інтеграція принципів NIST Cybersecurity Framework у хмарну платформу AWS робить безпеку не просто окремою функцією, а складовою частиною загальної архітектури і операційної діяльності. Це дозволяє автоматизувати багато процесів безпеки, підвищувати адаптивність системи та знижувати людський фактор, який часто стає джерелом вразливостей.

AWS також підтримує концепцію «Shared Responsibility Model» (Модель спільної відповідальності), згідно з якою безпека у хмарі – це спільна задача між постачальником послуг і клієнтом. AWS забезпечує фізичний захист центрів

обробки даних, безпеку інфраструктури, мережі та базових сервісів, тоді як користувачі відповідають за безпеку своїх додатків, управління доступом, налаштування захисту даних і дотримання політик [10].

Також платформа постійно розвивається: впроваджуються нові засоби автоматичного виявлення загроз із застосуванням штучного інтелекту, вдосконалюються алгоритми шифрування та контролю доступу. Завдяки цьому AWS залишається на передньому краї технологій кібербезпеки, надаючи клієнтам інструменти, необхідні для захисту сучасних, масштабованих і складних IT-систем.

AWS як платформа забезпечує універсальність, надійність і високий рівень безпеки, підтверджений підтримкою міжнародних стандартів і сертифікатів. Безпека є стратегічним пріоритетом AWS, що реалізується через багаторівневий захист, автоматизацію процесів безпеки та інтеграцію з міжнародними стандартами, зокрема NIST Cybersecurity Framework. Цей фреймворк структурує підхід до кібербезпеки через п’ять ключових функцій: визначення, захист, виявлення, реагування та відновлення, що дозволяє створювати адаптивну та цілісну стратегію захисту. Модель спільної відповідальності AWS чітко розмежовує обов’язки між провайдером і клієнтом, забезпечуючи фізичну та інфраструктурну безпеку з боку AWS і покладаючи на користувачів відповідальність за налаштування додатків і даних.

Крім того, AWS підтримує розвиток цифрових навичок через освітні платформи, такі як AWS Training and Certification та AWS Skill Builder, що сприяють підготовці кваліфікованих фахівців і підвищенню цифрової грамотності. Загалом, Amazon EC2 та AWS забезпечують гнучку, масштабовану та безпечну інфраструктуру, яка відповідає сучасним вимогам бізнесу та сприяє інноваційному розвитку організацій.

2 УПРАВЛІННЯ БЕЗПЕКОЮ ТА РИЗИКАМИ У ХМАРНИХ ОБЧИСЛЕННЯХ

2.1 Організація управління безпекою хмарних сервісів.

Управління безпекою та ризиками в контексті хмарних обчислень є ключовим компонентом сучасних інформаційних технологій та бізнес-стратегій. Зі збільшенням масштабу використання хмарних сервісів різними організаціями – від малих підприємств до великих корпорацій – виникають нові виклики, пов’язані з забезпеченням конфіденційності, цілісності та доступності даних, а також ефективним управлінням кіберризиками. Хмарні технології відкривають широкі можливості завдяки своїй гнучкості, масштабованості та економічній ефективності, проте для їх безпечного застосування необхідний комплексний і системний підхід до безпеки [11].

Ефективне управління безпекою хмарних обчислень базується на впровадженні передових методик і міжнародних стандартів, зокрема NIST Cybersecurity Framework, який допомагає організаціям послідовно ідентифікувати загрози, впроваджувати механізми захисту, виявляти інциденти, реагувати на них та відновлювати нормальну роботу. Такий підхід дозволяє не лише мінімізувати ризики компрометації даних, а й підвищити рівень довіри користувачів та бізнес-партнерів до хмарних сервісів.

При управлінні безпекою та ризиками у хмарі необхідно звертати увагу на кілька ключових аспектів. По-перше, це специфіка взаємодії з постачальниками хмарних послуг, що включає детальне опрацювання контрактів, визначення зон відповідальності та механізмів контролю. По-друге, важливо розуміти, як вплив хмари змінює підходи до управління ризиками на рівні всієї організації, враховуючи як технічні, так і організаційні фактори [12]. Окрему увагу слід приділяти юридичним аспектам, зокрема дотриманню нормативних вимог і проходженню аудитів у хмарних середовищах. Для підтримки цих процесів корисними є рекомендації та інструменти від спільноти Cloud Security Alliance, які сприяють системній оцінці ризиків і їх ефективному управлінню.

Розглядаючи структуру управління безпекою у хмарних середовищах, варто виділити ієрархічний підхід, що передбачає багаторівневий захист інформаційних ресурсів. Ця ієрархія охоплює різні рівні безпеки – від базових заходів фізичного захисту дата-центрів до мережевих, операційних та прикладних заходів, спрямованих на захист даних і користувацьких додатків. Завдяки такому багатошаровому підходу створюється ефективний бар’єр проти широкого спектру загроз, що дозволяє знизити ймовірність успішних атак та забезпечити стабільну роботу хмарної інфраструктури.

На рисунку 2.1 зображено принцип спрощенної ієрархієї.

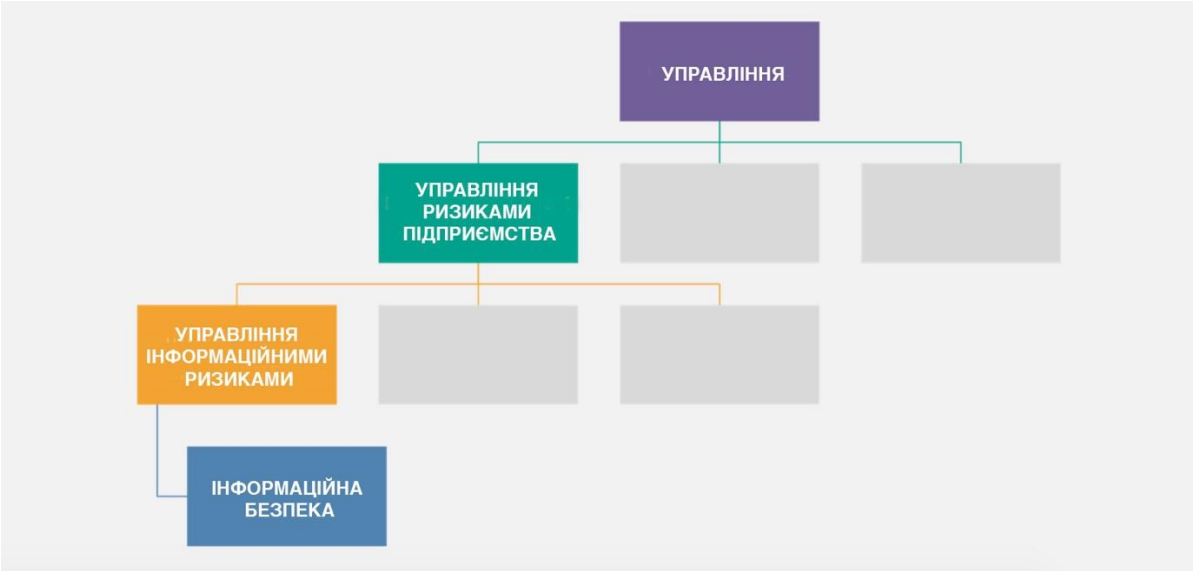

Рисунок 2.1 – Спрощена ієрархія в управлінні безпекою у хмарних середовищах

На першому, базовому рівні спрощеної ієрархії управління безпекою у хмарних сервісах розташована інформаційна безпека. Вона забезпечує фундаментальний захист даних, додатків та інфраструктури від різноманітних кіберзагроз, таких як несанкціонований доступ, шкідливе ПЗ, втрати інформації або атаки типу відмова в обслуговуванні (DDoS). На цьому рівні застосовуються основні технічні заходи безпеки, включно з автентифікацією, шифруванням, контролем доступу та моніторингом подій безпеки.

Другий рівень ієрархії присвячений управлінню інформаційними ризиками. Цей рівень зосереджений на системному підході до ідентифікації, оцінки та мінімізації ризиків, що виникають під час обробки, зберігання та передачі інформації в хмарному середовищі. Управління ризиками включає впровадження політик безпеки, процедур реагування на інциденти, а також регулярний аналіз потенційних загроз і вразливостей для своєчасного запобігання негативним наслідкам.

Третій рівень – управління ризиками підприємства – інтегрує питання інформаційної безпеки у загальну систему управління ризиками організації. Тут розглядаються більш широкі аспекти, які включають фінансові, операційні, репутаційні та регуляторні ризики. Цей рівень забезпечує узгодженість стратегій безпеки з бізнес-цілями та допомагає приймати обґрунтовані рішення щодо розподілу ресурсів і пріоритетів.

Найвищий, четвертий рівень – управління хмарою – охоплює комплексне керівництво всіма аспектами використання хмарних ресурсів і сервісів. Він гарантує безперебійну, ефективну та безпечну роботу хмарної інфраструктури, включаючи контроль над доступом, моніторинг виконання політик, відповідність нормативним вимогам, управління контрактами з провайдерами та аудит безпеки. На цьому рівні також здійснюється координація між різними командами і зацікавленими сторонами для підтримки цілісності та стійкості хмарних сервісів.

Загалом, така багаторівнева ієрархія управління безпекою забезпечує комплексний та системний підхід, що дозволяє організаціям адаптуватися до швидкозмінного технологічного середовища і динамічних бізнес-вимог. Інструментами ефективного керування виступають договори з постачальниками, оцінка їхніх послуг, а також регулярні звіти щодо відповідності стандартам безпеки [13]. Цей підхід визначає, як саме здійснюється управління безпекою у хмарних рішеннях на всіх рівнях організації, забезпечуючи належний баланс між технологіями, процесами і людським фактором.

Інструменти хмарного керування відіграють ключову роль у забезпеченні ефективного управління безпекою та відповідністю вимогам при роботі з хмарними постачальниками.

Першим і найважливішим інструментом є контракти, як зазначено на рисунку 2.2. Вони поширюють управління та внутрішній контроль на хмарного постачальника, чітко визначаючи ролі та обов'язки сторін у моделі спільної відповідальності.

Рисунок 2.2 – Інструменти хмарного керування

Контракт є основою для взаєморозуміння і забезпечує правову базу для співпраці, що охоплює такі важливі аспекти, як:

- Визначення взаємовідносин між клієнтом та постачальником;
- Умови використання сервісів та обмеження;
- Сфера застосування послуг, що надаються;
- Процедури у випадку порушень або інцидентів;
- Механізми управління та контролю за діяльністю хмарного постачальника.

Другим важливим інструментом є оцінка постачальників. Це систематичний процес перевірки та аналізу їхніх можливостей, безпеки, стабільності та відповідності стандартам. Оцінка допомагає клієнтам приймати обґрунтовані рішення щодо вибору надійних партнерів, що відповідають бізнес-вимогам.

Третім ключовим елементом є звіти про відповідність нормам і стандартам (compliance reports). Вони підтверджують, що хмарний постачальник дотримується вимог регуляторних органів, галузевих стандартів та внутрішніх політик клієнта.

Ці звіти забезпечують прозорість та довіру, а також полегшують проведення аудитів і контрольних перевірок.

Загалом, застосування цих інструментів дозволяє організаціям не лише контролювати та управляти безпекою у хмарі, а й зміцнювати партнерські відносини з постачальниками, створюючи надійну основу для безпечної та ефективної роботи в хмарному середовищі.

Щодо оцінки ризиків у хмарних середовищах, вона починається з чіткого розуміння ролі управління, яке встановлює політики і процедури, необхідні для контролю ризиків, як зазначено на рисунку 2.3. Важливим елементом є толерантність до ризику – визначення рівня ризику, який організація готова прийняти, щоб досягти своїх бізнес-цілей без надмірних втрат.

Рисунок 2.3 – Від управління до ризику

Оцінка постачальника є критичним кроком, що дозволяє перевірити, наскільки хмарний провайдер відповідає вимогам безпеки і регуляторним стандартам. Вона включає аналіз його технічних можливостей, сертифікацій, процедур управління ризиками і загальної надійності.

Договори з постачальниками встановлюють формальні умови співпраці, чітко визначаючи ролі і відповідальність сторін. Вони допомагають формалізувати

модель спільної відповідальності, що описує, які аспекти безпеки належать провайдеру, а які – користувачу.

Управління ризиками включає процеси і заходи, спрямовані на виявлення, оцінку і мінімізацію загроз. Це комплексний підхід, що об'єднує всі перераховані елементи і забезпечує безперервний контроль та адаптацію до змін у ризиковому середовищі.

Таким чином, ефективна оцінка ризику вимагає гармонійного поєднання управління, врахування толерантності до ризику, ретельної оцінки постачальника, укладення відповідних договорів і чіткої моделі спільної відповідальності.

2.2 Управління ризиками безпеки у хмарній платформі Amazon

Управління ризиками підприємства охоплює комплексне управління всіма видами ризиків, що можуть впливати на організацію в цілому. Головною метою цього процесу є надання цінності зацікавленим сторонам за рахунок системного вимірювання, контролю та мінімізації невизначеності, пов’язаної з ризиками.

У контексті хмарних технологій та платформи Amazon управління ризиками безпеки базується на поєднанні корпоративного рівня та специфіки інформаційних активів. Зокрема, управління інформаційними ризиками зосереджується на виявленні, оцінці та контролі ризиків, які безпосередньо впливають на інформацію, та має бути узгодженим з рівнем толерантності до ризику, визначеним власником даних [14].

Ключовим елементом цього процесу є узгодження управління ризиками з толерантністю власника даних, що дозволяє балансувати між прийнятним рівнем ризику та необхідними заходами безпеки. Для підтримки прийняття обґрунтованих рішень щодо IT-безпеки і забезпечення конфіденційності, цілісності та доступності (CIA) інформаційних активів, застосовуються різноманітні інструменти та системи, серед яких:

Системи управління ризиками (Risk Management Systems) – платформи для ідентифікації, аналізу, оцінки та контролю ризиків у режимі реального часу.

Автоматизовані засоби моніторингу (Automated Monitoring Tools) – інструменти для постійного відстеження стану безпеки та виявлення потенційних загроз.

Аналітика безпеки та системи виявлення аномалій (Security Analytics and Anomaly Detection Systems) – рішення, які аналізують поведінку систем і користувачів, щоб оперативно визначати відхилення від нормальної діяльності.

Інструменти управління доступом (Access Management Tools) – механізми контролю та обмеження прав доступу до ресурсів згідно з принципом мінімальних привілеїв.

Системи резервного копіювання та відновлення (Backup and Recovery Systems) – забезпечують збереження та оперативне відновлення даних у разі інцидентів.

Політики безпеки та стандарти (Security Policies and Standards) – документи, що регламентують правила і процедури безпечної роботи з інформацією.

Аудит та перевірки безпеки (Security Audits and Assessments) – регулярні оцінки для підтвердження відповідності встановленим стандартам і виявлення слабких місць.

Впровадження цих інструментів та практик формує комплексний підхід до управління безпекою, що дозволяє організаціям не лише ефективно захищати свої інформаційні активи, а й приймати обґрунтовані рішення в умовах мінливої кіберзагрозливої обстановки.Для ефективного управління ризиками безпеки у хмарних платформах, зокрема Amazon, використовують різноманітні інструменти і методи.

Наступна таблиця систематизує основні засоби підтримки прийняття рішень у сфері IT-безпеки, що допомагають забезпечити конфіденційність, цілісність і доступність інформаційних активів.

Застосування вказаних інструментів забезпечує системний підхід до захисту інформаційних активів, дозволяє вчасно виявляти і реагувати на загрози, а також підтримує прийняття обґрунтованих рішень у сфері кібербезпеки.

Таблиця 2.1 – Основні засоби підтримки прийняття рішень у сфері IT-безпеки у хмарних платформах

№	Інструмент	Призначення та функції
1.	Системи управління ризиками	Ідентифікація, аналіз, оцінка і контроль ризиків у реальному часі
2.	Автоматизовані засоби моніторингу	Постійне відстеження стану безпеки та виявлення загроз
3.	Аналітика безпеки та системи виявлення аномалій	Аналіз поведінки систем і користувачів для виявлення відхилень
4.	Інструменти управління доступом	Контроль і обмеження прав доступу згідно з принципом мінімальних привілеїв
5.	Системи резервного копіювання та відновлення	Збереження і відновлення даних у разі інцидентів
6.	Політики безпеки та стандарти	Регламентування правил і процедур безпечної роботи з інформацією
7.	Аудит та перевірки безпеки	Регулярні оцінки відповідності стандартам та виявлення слабких місць

Зусилля, спрямовані на оцінку ризиків, мають бути пропорційними цінності та важливості даних або сервісів, що розміщуються у хмарі. Переміщення інформації чи додатків у хмарне середовище не означає автоматично підвищення їх значущості з погляду ризиків безпеки. Важливо розуміти, що різні моделі хмарних сервісів мають різний рівень контролю та відповідальності за безпеку. Наприклад, інфраструктурні сервіси як IaaS найбільше нагадують традиційну IT-інфраструктуру, де користувачі зберігають значний контроль над своїми ресурсами. У той же час, сервісні моделі SaaS більше покладаються на безпеку, що забезпечується самим хмарним постачальником, що змінює природу і типи ризиків [15].

Ризики, які виникають у приватній хмарі, можуть бути досить схожими з ризиками у публічній хмарі, особливо коли приватна хмара розташована у дата-центрі стороннього провайдера або управляється зовнішньою компанією. В таких випадках організація все ще має відповідальність за управління ризиками, але їй необхідно враховувати додаткові фактори, пов’язані з рівнем довіри до третьої сторони, вимогами до контролю і дотриманням нормативів.

Тому оцінка ризиків має базуватися на глибокому розумінні особливостей кожного типу хмарної платформи, моделей відповідальності, а також специфіки бізнес-процесів і критичності даних. Це дозволяє сформувати адекватні заходи з безпеки та захисту, які будуть ефективними і співрозмірними з потенційними загрозами.

2.3 Комплаєнс (відповідність) та юридичні аспекти для хмари

Комплаєнс, або відповідність, - це важливий інструмент, який допомагає організаціям виконувати свої корпоративні зобов’язання. Ці зобов’язання виникають з різних джерел, зокрема:

- законодавства;
- контрактів із партнерами та клієнтами;
- галузевого регулювання;
- загальних нормативних вимог.

У контексті хмарних сервісів відповідність включає не лише дотримання законів, а й виконання внутрішніх політик і галузевих стандартів безпеки. Це важливо для забезпечення захисту даних, підтримки довіри клієнтів і зменшення ризиків для бізнесу.

Процеси аудиту відіграють ключову роль у системі комплаєнсу. Аудити – це механізми перевірки відповідності, які можуть проводитися як внутрішніми фахівцями організації, так і незалежними зовнішніми аудиторами. Вони допомагають своєчасно виявляти слабкі місця в системі безпеки, усувати вразливості і підтримувати високий рівень контролю.

Регулярний аудит та моніторинг дозволяють управляти ризиками, що виникають у хмарних середовищах, і підтверджують, що організація дотримується всіх необхідних нормативних та корпоративних вимог.

Таким чином, комплаєнс і аудит є невід'ємними складовими ефективного управління безпекою у хмарі, що забезпечують відповідність стандартам та зобов'язанням, а також підвищують загальну надійність хмарних сервісів.

У хмарних середовищах відповідальність за комплаєнс завжди залишається за клієнтом, однак він тепер може частково покладатися на свого хмарного постачальника. Такий розподіл відповідальності змінює підхід до забезпечення відповідності, оскільки клієнти дедалі більше спираються на незалежні оцінки та звіти третіх сторін, що підтверджують відповідність послуг постачальника вимогам і стандартам. Відповідність спадкування зображено на рисунку 2.4.

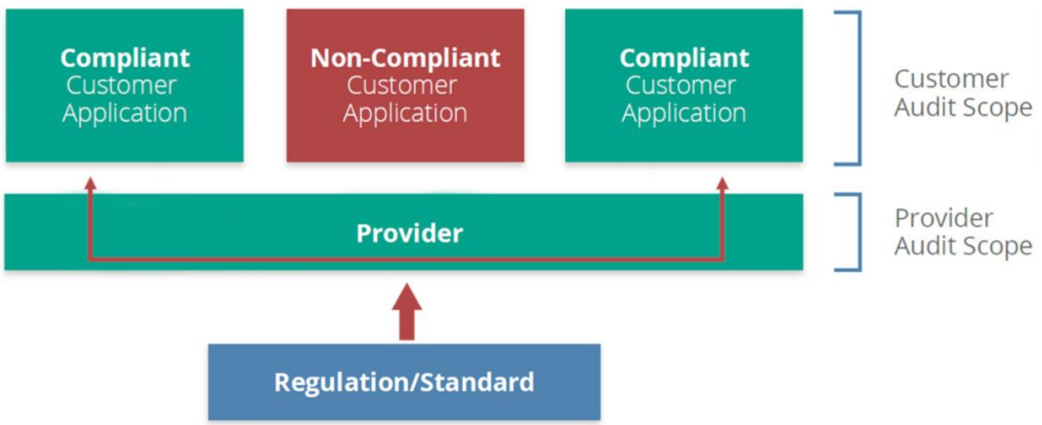

Рисунок 2.4 – Відповідність спадкування

Модель управління хмарою часто охоплює різні юрисдикції, тоді як дані і активи клієнта можуть залишатися під окремим правовим регулюванням. Цей факт ускладнює процес забезпечення відповідності, оскільки необхідно враховувати різноманітні нормативні вимоги для різних зон відповідальності. Важливо інтегрувати цю мультиюрисдикційну специфіку у внутрішні процедури управління комплаєнсом.

Не всі хмарні постачальники однакові з точки зору рівня відповідності, а також не всі послуги одного постачальника можуть бути включені в одну й ту ж сферу аудиту, атестації чи сертифікації. Тому клієнтам потрібно ретельно оцінювати можливості та звіти конкретного провайдера.

Для прикладу, в екосистемі Amazon EC2 користувачам доступні різні сервіси, які підтримують процеси аудиту, атестації та сертифікації:

AWS Config – інструмент для оцінки, аудиту та моніторингу конфігурацій ресурсів AWS. Він надає детальний огляд змін у конфігураціях та їх відповідність встановленим політикам безпеки.

AWS CloudTrail – сервіс, що записує дії користувачів і API-запити до AWS. Це критично важливо для аудиту, оскільки дозволяє відстежувати та аналізувати події в інфраструктурі.

AWS Security Hub – об’єднує дані з різних сервісів AWS, забезпечуючи централізований огляд безпеки. Підтримує відповідність стандартам і нормативам, що спрощує процес сертифікації.

Amazon Inspector – автоматизований сервіс для оцінки безпеки додатків на Amazon EC2, який допомагає виявляти вразливості та відхилення від найкращих практик.

AWS Audit Manager – інструмент, що автоматизує аудиторські процеси та управління відповідністю, генерує звіти, які відповідають конкретним стандартам і вимогам.

AWS IAM (Identity and Access Management) – система управління доступом до ресурсів AWS, яка забезпечує безпечний і контрольований доступ, що є важливим для відповідності і аудиту.

Ці сервіси формують комплексний підхід до управління конфігураціями, моніторингу подій, оцінки безпеки та контролю доступу. Вони допомагають організаціям ефективно проходити аудити, атестації та сертифікації у сфері безпеки.

Отже, хмара змінює концепцію відповідності, перетворюючи її на спільну відповідальність між споживачем і постачальником хмарних послуг.

Відповідність вимогам, аудит і підтвердження мають бути безперервними процесами. Їх не слід розглядати лише як одноразову діяльність, оскільки багато сучасних стандартів і нормативних актів орієнтуються саме на постійне підтримання відповідності. Це особливо актуально для хмарних обчислень, де як постачальник, так і клієнт часто зазнають змін, і рідко перебувають у статичному стані.

Хмарні постачальники повинні відкрито і чітко повідомляти про результати аудиту, сертифікати та атестації, приділяючи увагу таким аспектам:

1. Обсяг і межі проведених оцінок.

2. Конкретні функції та послуги, які охоплюються, а також регіональні та юрисдикційні особливості.

3. Як клієнти можуть розгортати сумісні програми і сервіси на платформі хмари.

4. Додаткові зобов’язання та обмеження, що накладаються на клієнтів.

Також постачальники зобов’язані підтримувати чинність своїх сертифікатів та атестацій протягом тривалого часу та заздалегідь інформувати про будь-які зміни у їх статусі.

Хмарний сервіс Amazon EC2 активно бере участь у безперервних ініціативах щодо забезпечення відповідності, що допомагає уникати прогалин у безпеці та мінімізує ризики для клієнтів.

Постачальник надає користувачам необхідні докази відповідності, такі як журнали адміністративної діяльності, які клієнт самостійно зібрати не може.

Користувачам потрібно ретельно оцінювати атестації та сертифікати третьої сторони, надані постачальником, і співвідносити їх з власними вимогами.

Важливо чітко розуміти обсяг оцінювання і сертифікації хмарного сервісу, включно з механізмами управління та охопленими функціями і послугами. Слід визначити, які артефакти відповідності потрібно отримати, а також налагодити їхнє ефективне збирання і управління.

Якщо артефактів недостатньо, необхідно створювати власні, що підтверджують відповідність.

Для зручності рекомендується вести реєстр використовуваних хмарних провайдерів, відповідних вимог відповідності та поточного статусу їх виконання. У цьому може допомогти інструмент CSA Cloud Controls Matrix.

Концепція успадкування відповідності означає, що якщо послуга хмарного провайдера відповідає встановленим нормам і стандартам, споживачі хмари можуть на її основі створювати сумісні додатки і сервіси. Проте це не гарантує автоматичної відповідності всього рішення, оскільки клієнт може розробити несумісну програму навіть на базі сумісної послуги.

Хмарний сервіс Amazon EC2 дотримується цих принципів, забезпечуючи чіткі правила для підтримання і передачі відповідності.

Завдяки природі хмарних обчислень стало значно легше передавати дані між різними країнами та регіонами. Облако дозволяє швидко і просто переміщувати інформацію по всьому світу. Однак ця легкість передачі даних створює складні правові виклики. Дані підпадають під дію численних правових систем, кожна з яких має власні вимоги та норми регулювання. Тому дуже важливо не лише враховувати технічні аспекти, але й розуміти правове різноманіття, а також подібності і відмінності між законами, що регулюють хмарні сервіси.

За останні десять років кількість країн, які прийняли закони про конфіденційність і безпеку даних, зросла більш ніж удвічі. Також значно збільшилась кількість нормативних актів, що регулюють захист як корпоративних, так і персональних даних. Це свідчить про глобальну тенденцію до посилення контролю за використанням і зберіганням інформації у зв’язку з підвищенням рівня кіберзагроз та ризиків витоків.

Одним із головних напрямів світового законодавства є захист права громадян на конфіденційність і надання їм контролю над тим, як збираються та використовуються їхні персональні дані. В різних країнах і регіонах посилюється законодавство щодо формалізації політик безпеки даних. Такі політики повинні містити заходи для запобігання несанкціонованому доступу, захисту від витоків і оперативного реагування на інциденти.

Важливо усвідомлювати, що порушення безпеки можуть статися з різних причин – дії державних акторів, хакерські атаки, недобросовісні або незадоволені співробітники, а також людський фактор і випадкові помилки. Законодавство вимагає своєчасного інформування як постраждалих осіб, так і відповідних державних органів про такі інциденти. Це сприяє мінімізації наслідків і підвищує прозорість у роботі з даними.

Ще однією складністю є те, що законодавство щодо даних у різних країнах і регіонах часто відрізняється. Наприклад, у США різні штати можуть мати власні вимоги, а в Європі, Азії чи інших регіонах – інші. Ці відмінності створюють бар'єри для вільного переміщення даних і вимагають від компаній комплексного підходу для дотримання нормативних вимог і уникнення штрафів. Особлива увага приділяється тому, щоб передавати дані лише тим суб'єктам, які можуть гарантувати «належний рівень захисту».

Юридично важливим аспектом є договірна база. Хоча хмарні сервіси часто надаються на основі типових угод користувача, які можна швидко прийняти кліком кнопки «Я погоджуюсь», такі угоди мають юридичну силу. Тому вкрай важливо уважно читати і розуміти умови договорів із хмарними провайдерами. У них можуть бути зазначені обмеження, умови відповідальності, особливості обробки даних та інші важливі положення, що впливають на дотримання законодавства і безпеку.

Amazon EC2, як і інші великі хмарні платформи, працює в умовах численних регулятивних вимог і приділяє значну увагу дотриманню юридичних та комплаєнс норм. Провайдер надає своїм клієнтам необхідні документи, сертифікати та звіти, що підтверджують відповідність вимогам. Це допомагає користувачам успішно проходити як внутрішні, так і зовнішні аудити та мінімізувати юридичні ризики.

Отже, використання хмарних сервісів Amazon EC2 потребує комплексного підходу до юридичних аспектів. Основними завданнями є розуміння різноманіття правових систем, постійне дотримання норм у сфері захисту даних, а також ретельне управління договірними відносинами з провайдером. Це дозволить

ефективно застосовувати хмарні технології, мінімізувати ризики та захистити дані в умовах постійно змінного правового поля.

При використанні хмарних сервісів важливо розуміти, яке законодавство застосовується у конкретній ситуації. Це може залежати від того, де розташована ваша компанія, де фізично зберігаються дані, або де проживають користувачі та клієнти. У різних країнах діють різні нормативні акти, що регулюють захист даних і конфіденційність.

В Австралії основним законом у цій сфері є Закон про конфіденційність 1988 року, який встановлює правила збору, зберігання і обробки персональних даних. Цей закон базується на 13 австралійських принципах конфіденційності (APP), які визначають стандарти обробки інформації, зокрема щодо її захисту, доступу та використання. Важливо, що він поширюється на приватних неприбуткових постачальників медичних послуг з оборотом понад три мільйони австралійських доларів. Також в Австралії діє Закон про захист прав споживачів (ACL), який забезпечує захист від фальшивих або оманливих контрактів, а також регулює обов’язок організацій повідомляти про порушення безпеки даних. Особливо слід зауважити, що Закон про конфіденційність поширюється на австралійських клієнтів незалежно від того, де фізично розташований хмарний постачальник послуг.

У Китаї регулювання у сфері кібербезпеки здійснюється на основі Закону про кібербезпеку 2017 року, який охоплює діяльність операторів мереж та вимагає забезпечення високого рівня безпеки інформаційних систем. Особливістю китайського законодавства є вимога локалізації даних, тобто обов’язок зберігати певні категорії інформації всередині країни. Законодавчий ландшафт конфіденційності в Китаї ще розвивається, тому правила і вимоги можуть змінюватися, що потребує постійного моніторингу та адаптації для компаній, які працюють з китайськими даними.

Таким чином, при роботі з хмарними сервісами в регіоні APAC слід особливо уважно враховувати локальні нормативи та вимоги щодо захисту персональних

даних і безпеки, адже порушення цих норм може призвести до значних юридичних і фінансових наслідків.

У Японії основним нормативним актом, що регулює обробку персональних даних, є Закон про захист персональної інформації (APPI). Цей закон покладає на організації приватного сектору обов'язок забезпечити належний захист особистих даних громадян. Особливу увагу закон приділяє передачі даних третім сторонам за межі країни – така передача можлива лише за умови попередньої згоди суб'єкта даних. Водночас, якщо одержувач даних відповідає певним критеріям, затвердженим Японською комісією із захисту персональних даних, передача може відбуватися без додаткової згоди. Це створює більш гнучку, але все ж захищену систему поводження з персональною інформацією, що відповідає глобальним трендам у сфері конфіденційності.

У країнах Європейського Союзу та Європейської економічної зони основним нормативом у сфері захисту персональних даних є Загальний регламент захисту даних (GDPR), який набув чинності у 2018 році. Цей регламент має екстериторіальну дію, тобто поширюється не лише на компанії, що знаходяться в межах ЄС/ЄЕЗ, але й на ті, які обробляють дані громадян ЄС/ЄЕЗ з-за меж цього регіону. Це особливо важливо для хмарних провайдерів, таких як Amazon EC2, адже їх діяльність може охоплювати користувачів з усього світу.

GDPR вимагає від компаній ведення обліку всіх дій, пов'язаних з обробкою персональних даних, а також впровадження принципів «конфіденційності за проектом» і «конфіденційності за замовчуванням». Регламент також гарантує користувачам низку прав – зокрема, право знати, яка інформація про них зберігається, право на виправлення або видалення даних, заперечення проти їх використання, а також «право бути забутим».

Важливою складовою є обмеження на транскордонну передачу персональних даних. Якщо країна-одержувач не забезпечує рівноцінного рівня захисту, компанія повинна впровадити додаткові механізми, які гарантують безпеку обробки. Порушення норм GDPR можуть спричинити серйозні наслідки: у разі витоку даних компанія зобов'язана повідомити як наглядовий орган, так і самих суб'єктів даних.

У разі грубих порушень передбачені фінансові санкції до 4% річного світового доходу компанії або до 20 мільйонів євро – залежно від того, яка сума є більшою.

Крім GDPR, у Європі діють також інші нормативні акти: Директива про конфіденційність та електронні комунікації 2002 року, яка регулює питання електронного маркетингу та використання файлів cookie, та Директива NIS, що зосереджена на безпеці критичної цифрової інфраструктури та захисті основних цифрових послуг. Новий Регламент електронної конфіденційності, який має замінити чинну директиву, наразі перебуває на етапі погодження, але вже зараз зрозуміло, що вектор розвитку законодавства в ЄС спрямований на посилення прав громадян і послідовну відповідальність бізнесу.

Директива з безпеки інформаційної мережі (NIS) є першим всеосяжним законодавчим актом ЄС, спрямованим на забезпечення високого рівня кібербезпеки у країнах-членах. Вона зобов’язує уряди держав ЄС/ЄЕЗ впроваджувати національне законодавство, яке регламентує вимоги до безпеки мереж та інформаційних систем, зокрема для операторів критично важливих цифрових послуг. Це охоплює сфери електронної комерції, пошукових систем і хмарних обчислень.

Особливістю директиви є її екстериторіальний характер: навіть компанії, що знаходяться за межами ЄС, але надають послуги європейським користувачам, повинні дотримуватись її вимог. Якщо такий провайдер зазнає серйозного інциденту, який може вплинути на стабільність або доступність його послуг, він зобов’язаний повідомити про це відповідні національні органи. Таким чином, Директива NIS посилює не лише технічну, а й юридичну відповідальність суб’єктів цифрової інфраструктури за підтримання належного рівня безпеки.

У регіоні EMEA, який охоплює Європу, Близький Схід та Африку, багато країн, що не входять до ЄС або ЄЕЗ, активно впроваджують власні нормативні акти, які за своєю суттю подібні до GDPR або попередньої Директиви ЄС 95/46/ЕС. Наприклад, у Дубаї, Ізраїлі, Марокко, Сенегалі, Південній Африці та Катарі діють закони, які встановлюють високі стандарти захисту персональних даних і визнаються Європейською Комісією як такі, що забезпечують адекватний рівень

захисту. Це дозволяє організаціям з цих країн легше взаємодіяти з компаніями в ЄС у контексті передачі персональних даних.

У країнах Латинської Америки, таких як Аргентина, Чилі, Колумбія, Мексика, Перу та Уругвай, правове регулювання захисту даних часто базується на положеннях Директиви ЄС 95/46/ЕС, яка була чинною до впровадження GDPR. Це означає, що ключові принципи, як-от обмеження мети, згода на обробку даних, права суб'єктів і заходи безпеки, вже давно присутні у місцевому законодавстві.

Крім того, ці країни дедалі активніше беруть участь у міжнародних ініціативах, таких як рамки конфіденційності АТЕС (Азійсько-Тихоокеанського економічного співробітництва), які сприяють гармонізації підходів до захисту даних у глобальному масштабі. Це дозволяє місцевим компаніям не лише забезпечувати права користувачів, але й відповідати вимогам міжнародних партнерів щодо обробки персональної інформації.

У Канаді основним нормативно-правовим актом у сфері захисту даних є Закон про захист персональної інформації та електронних документів (PIPEDA). Цей закон застосовується до організацій, що знаходяться під федеральною юрисдикцією, а також до суб'єктів господарювання в провінціях, які не мають власного законодавства, що відповідає федеральним стандартам. У тих провінціях, де діє власне законодавство про захист даних (наприклад, Квебек, Британська Колумбія, Альберта), воно повинно забезпечувати рівень захисту, еквівалентний PIPEDA. Закон регулює порядок збору, використання та розкриття персональної інформації в комерційних цілях і встановлює вимоги до отримання згоди, обмеження мети та забезпечення безпеки даних.

На відміну від ЄС або Канади, Сполучені Штати не мають єдиного загальнонаціонального закону, який би комплексно регулював захист персональних даних. Замість цього діє множина галузевих і тематичних федеральних законів, серед яких:

- Закон Гремма-Ліча-Блілі (GLBA), що регулює конфіденційність у фінансовому секторі;

- Закон про підзвітність та перенесення страхових даних (HIPAA), який охоплює конфіденційність у сфері охорони здоров'я;

- Закон про захист конфіденційності дітей в Інтернеті (COPPA), що захищає інформацію про дітей віком до 13 років в онлайн-середовищі.

Ці акти зобов'язують організації впроваджувати «розумні заходи безпеки» щодо збереження персональної інформації, а також передбачають відповідальність не лише самої організації, а й її підрядників чи партнерів.

Крім того, у кожному штаті діють власні закони щодо конфіденційності та безпеки даних. Такі норми поширюються на будь-яку організацію, яка збирає або обробляє дані резидентів штату – незалежно від місця фізичного зберігання чи обробки цих даних. Багато штатів вимагають укладення письмових угод із третіми сторонами-постачальниками послуг, які передбачають забезпечення належного рівня безпеки персональної інформації.

Американське законодавство також передбачає обов'язкове інформування користувачів у разі порушення безпеки персональних даних. Таке повідомлення має бути зроблене своєчасно й відповідно до вимог конкретного штату чи галузевого закону.

Контроль за дотриманням вимог здійснюють як федеральні агентства, так і прокурори окремих штатів. Зокрема, Федеральна торгова комісія (FTC) відіграє провідну роль у забезпеченні підзвітності компаній та розслідуванні порушень, пов'язаних із недобросовісною практикою обробки даних. У багатьох випадках FTC або органи штатів ухвалюють приписи, які вказують організаціям, як слід поводитися з персональними даними, щоб уникнути подібних порушень у майбутньому.

Закон Каліфорнії про конфіденційність споживачів (CCPA). З моменту набуття чинності в січні 2020 року CCPA став одним із найвпливовіших законів у США щодо захисту персональних даних. Закон забезпечує права окремих осіб, сімей і навіть пристроїв на контроль над особистою інформацією. CCPA надає споживачам право знати, які дані збираються, право на видалення, заборону

продажу даних та інші ключові гарантії. Закон також передбачає значні наслідки для компаній, які його порушують.

Особливістю американського судочинства є широкі повноваження сторін щодо «відкриття» (discovery) документів, які можуть мати значення для справи. Це означає, що кожна сторона має право запитувати та отримувати інформацію, зокрема в електронному вигляді (ESI). Ускладнення виникає, коли дані зберігаються в хмарних середовищах, адже через їхнє розпорошення важко ідентифікувати повний обсяг релевантної інформації.

Оскільки більшість ділової інформації поступово переміщується в хмару, постачальники та їхні клієнти повинні заздалегідь розуміти, де і як зберігаються документи, як забезпечити їхню цілісність та доступність у разі судових розглядів.

Галузеві стандарти, як Багато стандартів у сфері хмарних технологій розробляються не державними органами, а приватними організаціями. Вони не мають сили закону, однак широко застосовуються як «добра практика» або еталонні рамки безпеки, конфіденційності та надійності. Прикладами є ISO/IEC 27001, SOC 2, NIST, як зображено на рисунку 2.5.

Рисунок 2.5 – Галузеві стандарти

Ці стандарти можуть бути важливою частиною договорів з хмарними провайдерами, слугуючи основою для оцінки відповідності постачальника послуг вимогам клієнта.

Договори: правові та комерційні аспекти.

Перед укладанням договору важливо провести:

- юридичну перевірку власної організації;

- аналіз репутації, стабільності та політик провайдера;

- оцінку, чи допоможе послуга досягти цілей компанії, залишаючись у відповідності до вимог конфіденційності.

Ключові умови договору:

- Ціноутворення – прозорість та гнучкість витрат;

- Розподіл ризиків та відповідальності – чітке визначення, хто за що відповідає;

- Право власності на дані – дані мають залишатися власністю клієнта;

- Місце зберігання даних – важливо з огляду на вимоги юрисдикції;

- SLA (угода про рівень обслуговування) – гарантії доступності, швидкості відновлення тощо;

- Конфіденційність та захист персональної інформації – включно з PLA (Privacy Level Agreement).

Під час виконання договору слід забезпечити:

- Постійний моніторинг якості послуг та дотримання зобов’язань;

- Підготовку до розірвання та переходу до іншого провайдера;

- Оцінку непередбачених ситуацій – кіберінциденти, форс-мажори;

- Закриття договору з належним видаленням чи поверненням даних.

Законодавство у сфері захисту даних суттєво варіюється залежно від регіону, однак глобальна тенденція очевидна – підвищення вимог до безпеки та прозорості обробки персональної інформації. У країнах ЄС та тих, що орієнтуються на європейські стандарти (наприклад, Канада, Аргентина, Ізраїль), закони зосереджені на захисті прав суб’єктів даних, обов’язковому повідомленні про

інциденти безпеки та зобов’язаннях постачальників, незалежно від їхньої юрисдикції.

У США підхід більш фрагментований – відсутній єдиний національний закон, але діє низка галузевих і регіональних актів (CCPA, HIPAA, GLBA), а також потужна практика судового «електронного відкриття». Це накладає додаткові зобов’язання на компанії щодо контролю доступу до даних, дотримання контрактних умов із провайдерами та готовності до аудиту. У підсумку, незалежно від юрисдикції, компанії мають забезпечувати належну правову та технічну обачність при роботі з хмарними сервісами й персональними даними.

2.4 Аудит безпеки та інструменти CSA

Аудит безпеки в хмарному середовищі є одним із ключових механізмів оцінки надійності постачальника послуг та рівня відповідності вимогам інформаційної безпеки. Проте процес аудиту у хмарі значно складніший порівняно з традиційною IT-інфраструктурою через особливості розподіленого зберігання, обмежену прозорість і доступ до ресурсів постачальника.

Існує декілька типів аудитів і оцінок – від внутрішніх перевірок безпеки до незалежних сертифікаційних аудитів, таких як SOC 1/2/3, ISO/IEC 27001, CSA STAR тощо. Однак варто враховувати, що навіть якщо різні провайдери використовують однакові терміни для позначення аудитів, їхній масштаб, глибина та фокус можуть істотно відрізнятися. Наприклад, деякі постачальники можуть дозволяти лише читання звітів, але не надавати доступ до самих даних аудиту або артефактів.

Крім того, постачальники часто обмежують можливості проведення певних типів тестування, зокрема сканування вразливостей чи тестів на проникнення, оскільки такі дії можуть бути сприйняті як атаки. Це накладає додаткові вимоги на клієнтів – узгоджувати будь-які форми тестування із провайдером та заздалегідь отримувати дозвіл.

Під час роботи з хмарними сервісами компанії повинні самостійно піклуватися про збереження аудиторських доказів (артефактів), які підтверджують дотримання політик безпеки. До таких артефактів можуть належати системні журнали, логи змін конфігурацій, звіти про дії адміністраторів тощо. Важливо заздалегідь узгодити з провайдером можливість доступу до цих даних, а також створити інфраструктуру для їхнього централізованого зберігання. Наприклад, системні журнали рекомендується виводити у зовнішнє хмарне сховище (object storage), доступ до якого має лише клієнт.

Для підвищення прозорості й контролю варто додавати розширене логування у власні додатки, фіксувати конфігураційні зміни, зберігати дані про активність користувачів та адміністраторів, а також періодично перевіряти журнали на предмет аномалій чи ознак зловмисної активності.

Cloud Security Alliance (CSA) є авторитетною міжнародною організацією, що розробляє стандарти, рекомендації та інструменти для забезпечення безпеки у хмарних середовищах. Одним із таких інструментів є CSA Cloud Controls Matrix – детальний фреймворк, який допомагає оцінювати ризики й відповідність хмарних сервісів на основі контрольних пунктів. Крім того, CSA пропонує інструмент CAIQ – опитувальник, який використовується для оцінювання постачальників хмарних послуг і містить типові запитання про політики, процедури та технічні заходи захисту.

Організації можуть використовувати інструменти CSA як частину внутрішніх аудитів, підготовки до сертифікації або як засіб для обрання відповідального хмарного провайдера. CSA також підтримує публічний реєстр сертифікованих постачальників (STAR Registry), який дозволяє швидко перевірити, чи відповідає компанія основним вимогам безпеки.

Проведення аудитів безпеки у хмарному середовищі потребує чітко визначеного підходу, узгодження з постачальником та активної участі замовника. Клієнти повинні самостійно збирати артефакти відповідності, контролювати дії користувачів, забезпечувати збереження логів і використовувати галузеві стандарти, зокрема CSA CCM і CAIQ, як основу для оцінки. Надійний аудит та

контроль за відповідністю – важлива складова безпечного використання хмарних технологій.

На рисунку 2.7 зображено ключові компоненти, що формують артефакти відповідності у хмарному середовищі: політика та документація, процедури, журнали аудиту, звітність про діяльність і деталі конфігурації системи. Усі ці елементи є критично важливими для забезпечення прозорості, контрольованості та дотримання вимог стандартів інформаційної безпеки.

Рисунок 2.7 – Артефакти відповідності

Політики та документація визначають правила й вимоги до роботи з хмарною інфраструктурою. Процедури описують практичні кроки для забезпечення безпеки, реагування на інциденти та управління ризиками. Журнали аудиту відображають події у системі – від змін конфігурації до спроб доступу. Звітність про діяльність дозволяє аналізувати поведінку користувачів і виявляти аномалії. Конфігураційні деталі забезпечують контроль над змінами в інфраструктурі та відповідність вимогам до налаштувань.

Необхідно заздалегідь визначити, які саме дані потрібно зібрати для дотримання вимог законодавства чи корпоративних політик.

Важливо зрозуміти, яку саме інформацію постачальник хмарних послуг може надати та у якій формі. Це дозволить уникнути прогалин у відповідності.

Усі зібрані дані й докази потрібно зберігати в централізованому сховищі, до якого мають доступ лише уповноважені особи.

Якщо в деяких компонентах системи відсутнє повне логування, рекомендується вбудувати додаткові журналидля заповнення таких прогалин і збереження видимості.

Через постійну еволюцію хмарних сервісів – оновлення функціоналу, зміну архітектури, додавання нових інтеграцій – аудит безпеки має проводитися регулярно, а не лише при зміні провайдера або перед сертифікацією.

Рекомендується:

1. Впровадити періодичні оцінки на основі внутрішніх політик безпеки.

2. Використовувати стандартизовані підходи від Cloud Security Alliance, зокрема CSA STAR, CAIQ, CCM, які дозволяють проводити систематичну оцінку постачальників хмарних послуг.

3. Оцінювати не лише відповідність, а й ефективність реалізованих заходів безпеки – наскільки журнали покривають ключові події, чи виявляються аномалії, чи оновлюються політики відповідно до нових загроз.

Таким чином, належно організований аудит хмарної інфраструктури та грамотне управління артефактами відповідності є важливою складовою загального підходу до забезпечення кібербезпеки в умовах зростаючих загроз і змін у технологічному середовищі.

Cloud Security Alliance розробила низку інструментів і методологій, які допомагають організаціям впроваджувати, перевіряти та підтримувати належний рівень безпеки в хмарних середовищах. Ці інструменти стали галузевими стандартами і широко використовуються як постачальниками, так і споживачами хмарних послуг.

Cloud Controls Matrix є основним фреймворком CSA, що включає детальний перелік контрольних заходів безпеки, які організація має враховувати при роботі з хмарними сервісами. CCM охоплює домени, пов’язані з управлінням, операційною діяльністю, технічною безпекою, а також відповідністю законодавству.

Матриця:

– дозволяє зіставляти контрольні заходи з різними нормативними вимогами (наприклад, ISO/IEC 27001, GDPR, NIST, PCI DSS);

– є ефективним інструментом самооцінки безпеки хмарного середовища;

– допомагає клієнтам порівнювати постачальників за єдиними критеріями;

– підтримує розмежування відповідальності між хмарним провайдером і замовником.

Цей інструмент широко застосовується як для створення внутрішніх політик, так і під час аудитів, зокрема для реєстрації у CSA STAR.

Анкета CAIQ – це стандартизований набір запитань, які дозволяють швидко оцінити рівень безпеки постачальника хмарних послуг. Постачальники можуть заповнити CAIQ один раз і публікувати його у відкритому доступі, тим самим:

– спрощуючи процес перевірки для численних потенційних клієнтів;

– зменшуючи потребу відповідати на нестандартні запити пропозицій (RFP);

– дозволяючи споживачам безпосередньо порівнювати постачальників між собою за єдиним підходом.

CAIQ також може бути подано до CSA STAR Registry, що посилює прозорість та довіру до постачальника.

CSA STAR Registry – це публічний реєстр, у якому хмарні постачальники можуть оприлюднювати документи про свою відповідність стандартам безпеки. Він включає:

– відповіді на CAIQ;

– сертифікати відповідності (наприклад, ISO/IEC 27001 з доповненням CSA STAR);

– результати незалежних оцінок.

Інструмент StarWatch допомагає автоматизувати моніторинг відповідності та співставлення даних CAIQ з політиками замовника.

Переваги використання CSA CCM та пов'язаних інструментів:

– забезпечують єдиний підхід до безпеки в хмарному середовищі;

– сприяють прозорості між провайдерами та споживачами;

– полегшують аудит та відповідність вимогам законодавства;

– підтримують оцінку операційних ризиків та формування запитів на пропозиції (RFP);

– Сприяють внутрішній гармонізації заходів безпеки.

Хмарна матриця керування зображена на рисунку 2.8.

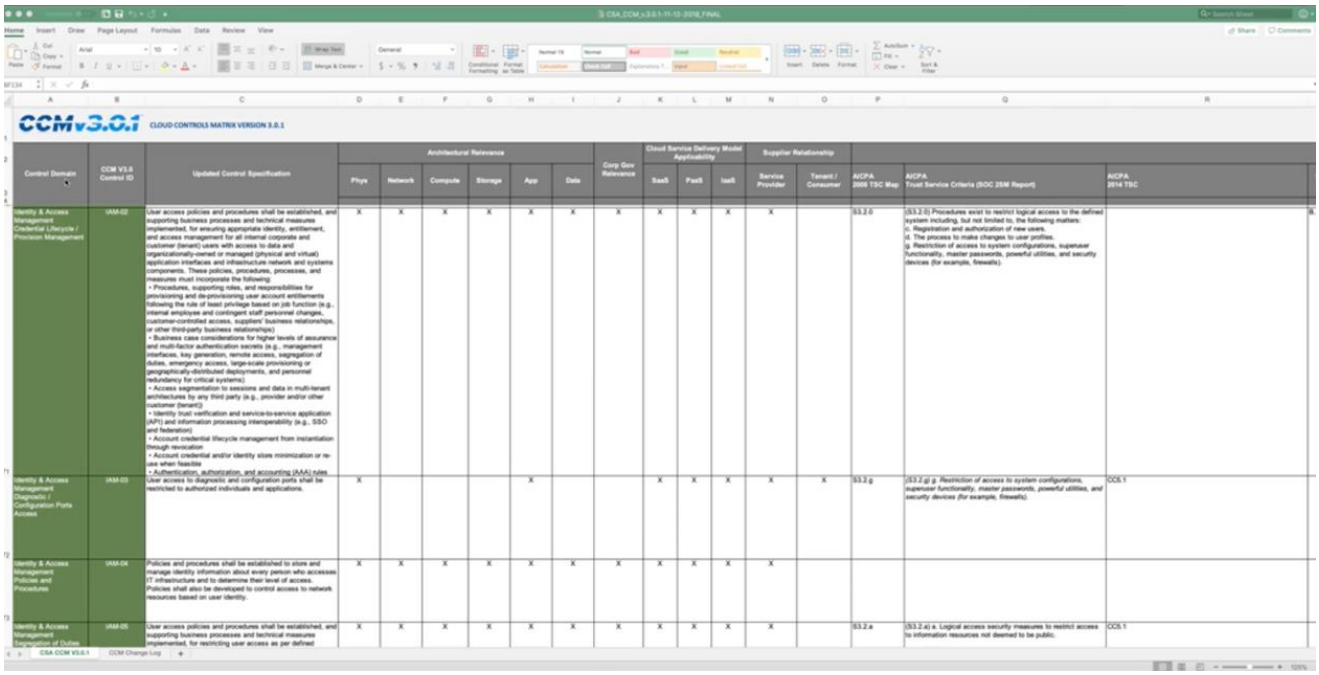

Рисунок 2.8 – Хмарна матриця керування

Анкета CAIQ є ключовим інструментом, створеним робочою групою CSA Consensus Assessments Initiative. Її головна мета – надати стандартизований механізм перевірки заходів безпеки, які впроваджує хмарний провайдер. Це дозволяє споживачам швидко й ефективно оцінити рівень інформаційної безпеки постачальника хмарних послуг без необхідності створення індивідуальних запитів.

Основні характеристики анкети CAIQ:

1. Стандартизація підходу до перевірки безпеки – усі провайдери відповідають на однаковий набір запитань.

2. Спрощення аудиту – клієнти отримують єдиний документ з повною інформацією про заходи безпеки.

3. Прозорість і відкритість – провайдери можуть публікувати CAIQ у відкритому доступі (наприклад, у реєстрі CSA STAR).

4. Супутній інструмент до Cloud Controls Matrix – CAIQ деталізує реалізацію конкретних контрольних елементів, вказаних у матриці.

Полегшення взаємодії між провайдерами, замовниками та регуляторами за рахунок узгодженої термінології та структури відповідей.

CAIQ є особливо корисною для хмарних постачальників, які прагнуть продемонструвати прозорість своєї програми інформаційної безпеки, а також для організацій, які проводять попередню оцінку ризиків при виборі хмарного партнера.

Cloud Security Alliance – це впливова міжнародна некомерційна організація, створена з метою розробки й поширення найкращих практик у сфері безпеки хмарних обчислень. CSA об'єднує експертів, представників індустрії, науковців та державні установи для досягнення спільної мети – підвищення рівня довіри до хмарних технологій.

Місія CSA формулюється так: «Заохочення активного використання найкращих практик безпеки в хмарному середовищі та навчання методам використання хмарних обчислень для захисту всіх інших форм обчислень» [16].

Організація є автором таких фундаментальних інструментів, як:

– Cloud Controls Matrix (CCM);

– CAIQ;

– CSA STAR Registry;

– сертифікаційна програма CSA STAR Certification;

– рекомендації щодо безпечного впровадження хмарних технологій.

CSA виступає платформою для стандартизації та координації зусиль у сфері кібербезпеки, дозволяючи учасникам ринку працювати на основі спільно визнаних критеріїв.

Програма CSA STAR – це добровільна ініціатива Cloud Security Alliance, яка спрямована на підвищення прозорості, довіри та рівня безпеки хмарних сервісів через стандартизовані оцінки та сертифікації. Вона поділяється на три основні рівні оцінки відповідності, кожен з яких має свої особливості та призначення.

CSA STAR, Рівень 1: Самостійна оцінка, на цьому рівні постачальник хмарних послуг добровільно проводить власну оцінку безпеки, використовуючи

інструмент Consensus Assessments Initiative Questionnaire (CAIQ) – стандартизовану анкету для оцінки стану безпеки хмарного середовища.

AWS публічно надає результати цієї самооцінки, що підтверджує їх відповідність рекомендаціям CSA. Такий підхід сприяє прозорості, дозволяє клієнтам отримати детальну інформацію про практики безпеки провайдера та швидко оцінити ризики.

CSA STAR, Рівень 2: Сертифікація. Другий рівень передбачає незалежну сторонню оцінку безпеки хмарного провайдера. Вона базується на суворих вимогах міжнародного стандарту ISO/IEC 27001:2013 та критеріях CSA Cloud Controls Matrix (CCM).

Сертифікація підтверджує, що послуги AWS відповідають найкращим практикам інформаційної безпеки та відповідають високим стандартам галузі. Сертифікати публікуються на офіційному сайті AWS та в системі AWS Artifact, де також зазначаються регіони та сервіси, які підпадають під область дії сертифікації.

Цей рівень забезпечує глибоку довіру з боку клієнтів та партнерів, оскільки перевірка здійснюється незалежними аудиторами, а результати підтверджують відповідність міжнародним стандартам.

Рівень 3 або безперервний моніторинг наразі є перспективним і орієнтований на безперервний моніторинг стану безпеки хмарного середовища. CSA все ще розробляє конкретні вимоги для цього рівня, тому офіційна сертифікація ще не запроваджена.

AWS пропонує своїм клієнтам інструменти, які підтримують постійний моніторинг та автоматизацію процесів безпеки через програму AWS Security by Design. Вона дозволяє користувачам контролювати конфігурації, виконувати аудит систем і підтримувати відповідність стандартам безпеки.

За допомогою стандартних директив та проектів з автоматизацією клієнти можуть швидко адаптуватися до вимог різних галузей та робочих навантажень, що істотно підвищує рівень оперативного управління безпекою.

Ця багаторівнева модель оцінки безпеки хмарних сервісів допомагає організаціям різного масштабу та типів приймати обґрунтовані рішення щодо вибору хмарних провайдерів, мінімізуючи ризики та підвищуючи загальну безпеку.

Загалом управління ризиками в хмарі передбачає чітке визначення зон відповідальності між клієнтом і постачальником, що реалізується через контракти, оцінку провайдерів і звіти про відповідність. Amazon EC2 пропонує широкий набір інструментів, таких як AWS Config, CloudTrail, Security Hub, Inspector, Audit Manager та IAM, які підтримують процеси моніторингу, аудиту та управління доступом, сприяючи забезпеченню конфіденційності, цілісності та доступності даних.

Комплаєнс у хмарних середовищах є спільною відповідальністю, що вимагає врахування мультиюрисдикційних нормативних вимог і регулярного аудиту. Юридичні аспекти, зокрема локалізація даних і договори з провайдерами, відіграють ключову роль у дотриманні законодавства, яке варіюється залежно від регіону (GDPR в ЄС, CCPA в США, APPI в Японії тощо). Глобальна тенденція до посилення регулювання захисту даних підкреслює необхідність безперервного моніторингу відповідності.

Аудит безпеки в хмарі, ускладнений розподіленою природою сервісів, потребує використання стандартизованих інструментів, таких як CSA Cloud Controls Matrix, CAIQ та STAR Registry, які забезпечують прозорість і дозволяють оцінювати рівень безпеки провайдерів. Amazon EC2 активно підтримує ці ініціативи, надаючи клієнтам докази відповідності та інструменти для автоматизації аудиту.

Таким чином, управління безпекою та ризиками в хмарних обчисленнях вимагає комплексного підходу, що поєднує технічні, організаційні та юридичні заходи. Amazon EC2, завдяки своїм розвиненим сервісам і відповідності міжнародним стандартам, створює надійне середовище для безпечного використання хмарних технологій, забезпечуючи організаціям можливість ефективно протистояти сучасним кіберзагрозам і відповідати нормативним вимогам.

3 ЗАХИСТ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ

3.1 Хмарне зберігання та передача даних

Безпека даних у хмарних обчисленнях є критично важливою у сучасному цифровому світі. Зі збільшенням обсягу даних, що зберігаються у хмарних сховищах, необхідно розуміти особливості різних моделей хмарних середовищ: публічної, приватної та гібридної.

Публічні хмари доступні через Інтернет широкому колу користувачів і є економічно вигідними, проте можуть не відповідати вимогам безпеки для чутливих даних.

Приватні хмари призначені виключно для однієї організації, що забезпечує гнучкіший контроль безпеки, але вони дорожчі у впровадженні та обслуговуванні.

Гібридні хмари поєднують переваги публічних та приватних моделей, забезпечуючи баланс між безпекою та економічною ефективністю.

Ключовими викликами безпеки у хмарі є забезпечення конфіденційності, цілісності та доступності даних. Загрози можуть виникати через неправильну конфігурацію сервісів, людські помилки, зловмисні атаки та недостатні заходи безпеки постачальників. Наприклад, витік даних можливий через слабкі паролі чи ненадійні процедури автентифікації.

Одним із важливих елементів захисту є контроль доступу. Надійні механізми, такі як багатофакторна автентифікація (MFA), ролево-орієнтований контроль доступу (RBAC) та постійний моніторинг активності користувачів, допомагають запобігти несанкціонованому доступу та зловживанням.

Важливо також враховувати різні моделі шифрування даних:

1. Шифрування на стороні клієнта (дані шифруються до відправлення у хмару, що підвищує безпеку, бо постачальник не має доступу до відкритих даних).

2. Шифрування на стороні сервера (дані шифруються після отримання у хмарі, що простіше, але може бути менш безпечним).

Для комплексного захисту даних використовуються додаткові заходи: резервне копіювання, виявлення та реагування на інциденти безпеки, регулярні

аудити. Резервне копіювання гарантує відновлення даних у випадку їх втрати, а аудити дозволяють вчасно виявляти та усувати вразливості.

Життєвий цикл безпеки даних охоплює всі етапи їх обробки – від створення до знищення. Захист має забезпечуватися на кожному етапі: при створенні, зберіганні, передачі та видаленні даних. Особлива увага приділяється вбудованій безпеці при розробці нових додатків і сервісів, що підвищує загальний рівень захищеності хмарної інфраструктури.

Дані, що зберігаються у хмарі, використовують різні технології абстракції та віртуалізації, через що користувач бачить знайомий інтерфейс, але зсередини механізми суттєво відрізняються від традиційних. Незважаючи на віртуалізацію, всі дані зрештою зберігаються на фізичних носіях.

Типи сховищ поділяютьс як на об’ємне та об’єктне сховище.

Об’ємне сховище – це віртуальні жорсткі диски, що імітують традиційне блочне сховище.

Об’єктне сховище – схоже на базу даних для файлів, керовану через API.

Бази даних у хмарі можуть бути мультитенантними і не обов’язково імітують локальні системи баз даних.

Хмарні додатки використовують різноманітні методи зберігання файлів, про які користувач може не знати.

Для підвищення стійкості більшість хмарних сховищ застосовують дисперсію даних – розподіл інформації між різними носіями, що ускладнює відстеження фізичного розташування дисків.

Хмарне сховище відрізняється від традиційних рішень завдяки абстракції та віртуалізації, які дозволяють створювати пул зберігання, відокремлений від фізичних носіїв. Замість класичних SAN/NAS рішень використовуються сучасні інноваційні технології, які, хоча й можуть виглядати як традиційні, мають суттєві відмінності у своїй архітектурі та функціональності. Безпека хмарного сховища зосереджена на контролі доступу, шифруванні даних і належній конфігурації сервісів, що забезпечує надійність і адаптацію до вимог сучасних інформаційних систем.

Основні типи хмарного зберігання включають об’ємне сховище, яке імітує традиційні віртуальні жорсткі диски для віртуальних машин чи екземплярів; об’єктне сховище, що функціонує як база даних для файлів і керується через API; бази даних, які охоплюють як реляційні, так і нереляційні масштабовані сервіси; а також сховища додатків і платформ, що включають мережі доставки контенту (CDN) і SaaS-додатки з інтегрованим зберіганням файлів.

Для керування міграцією даних у хмару застосовуються спеціалізовані інструменти, як зображено на рисунку 3.1. Моніторинг активності баз даних виявляє аномалії та небезпечну активність. Брокери безпеки хмарного доступу забезпечують контроль, моніторинг і захист доступу до хмарних сервісів. Системи запобігання втраті даних блокують несанкціоноване передавання конфіденційної інформації, а URL-фільтрація забезпечує уніфікований контроль доступу та безпеки.

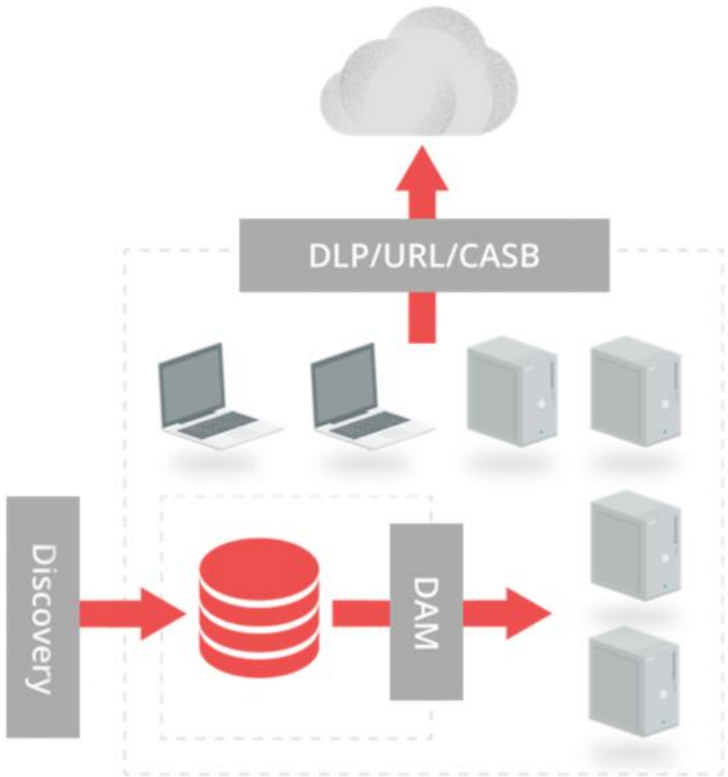

Рисунок 3.1 – Керування міграцією даних у хмару

Хмарний доступ і брокери безпеки (CASB). Також відомі як хмарні шлюзи безпеки. Процес включає:

- Виявлення використовуваних хмарних сервісів співробітниками.
- Моніторинг трафіку та активності в хмарі.
- -Захист, включаючи блокування небажаного доступу.
- Використовуються такі технології:
- DNS-записи для ідентифікації трафіку.
- URL-фільтри.
- Безпечні веб-шлюзи.
- Механізми блокування доступу за політиками безпеки.

Інструменти, такі як CASB, DLP та URL-фільтрування, забезпечують ефективний контроль і візуалізацію процесу міграції даних у хмару [17]. Передача даних може відбуватися з використанням шифрування: дані зашифровуються до міграції, захищаються під час передавання за допомогою TLS або інших мережевих протоколів шифрування. Крім того, локальні проксі-сервери можуть консолідувати та додатково шифрувати дані, що особливо актуально для резервного копіювання в хмарі.

3.2 Методи захисту даних у хмарі

Контроль доступу залишається найважливішим елементом безпеки, навіть у хмарних обчисленнях [18].

Хмарні провайдери пропонують широкий спектр засобів контролю доступу, а хмарне сховище вводить нові категорії контролю, зокрема механізми спільного доступу, які відрізняються від традиційних систем зберігання даних.

Що включає в себе контроль доступу у хмарі:

- Основні засоби контролю безпеки, які забезпечують захист даних;
- Різні рівні та площини управління доступом;
- Специфічні елементи керування для спільного доступу до ресурсів;
- Контроль доступу на рівні програмного забезпечення (додатків);

- Відмінності в деталізації та глибинах контролю доступу;

- Вплив моделі обслуговування (IaaS, PaaS, SaaS) на реалізацію контролю;

Ці складові контролю доступу взаємопов’язані та формують комплексний механізм захисту даних у хмарному середовищі. Вони дозволяють гнучко налаштовувати права користувачів, забезпечують сегментацію доступу за ролями та контекстом використання, а також враховують специфіку кожної моделі обслуговування. Такий підхід гарантує, що лише авторизовані користувачі отримують доступ до необхідних ресурсів у визначених межах, знижуючи ризики несанкціонованого доступу або випадкового витоку інформації.

Візуально схожі елементи керування можуть суттєво відрізнятися за змістом і функціями.

Перший і найголовніший контроль безпеки даних повинен належати власнику даних. Деталізація і реалізація засобів контролю доступу значно варіюється між різними платформами, сервісами та технологіями.

Чим більш точними є елементи керування доступом, тим вище рівень безпеки, але водночас це ускладнює адміністрування.

Важливо пам’ятати: на поверхні елементи керування можуть виглядати однаково, але на практиці вони суттєво відрізняються. Тому необхідно створювати чіткі матриці прав доступу, адаптовані під конкретну платформу чи сервіс (Рисунок 3.2).

Матриця прав – це детальна документація авторизацій, яка визначає, хто і які дії може виконувати з певними ресурсами у хмарному середовищі.

ENTITLEMENT	SUPER-ADMIN	SERVICE-ADMIN	STORAGE-ADMIN	DEV	SECURITY-AUDIT	SECURITY-ADMIN
VOLUME DESCRIBE	X	X		X	X	X
OBJECT DESCRIBE	X		X	X	X	X
VOLUME MODIFY	X	X		X		X
READ LOGS	X				X	X

Рисунок 3.2 – Матриця прав

Вона не лише регламентує, кому надається доступ до даних, а й описує рівні доступу, такі як читання, запис, видалення або адміністрування. Матриця прав допомагає уникнути надмірних або недостатніх привілеїв, що є критично важливим для мінімізації ризиків витоку інформації чи несанкціонованих змін.

Вона слугує основою для розробки політик безпеки, забезпечує прозорість і контроль за доступом, а також полегшує аудит і моніторинг активності користувачів. У разі змін у команді або організаційній структурі матриця прав дозволяє швидко і чітко оновлювати права доступу відповідно до ролей і функцій користувачів.

3.3 Шифрування в сервісах IaaS, PaaS та SaaS

Існує кілька рівнів, на яких можна застосовувати шифрування даних у хмарі, і кожен із них має свої переваги та певні складнощі. Шифрування на вищих рівнях стеку програм, наприклад, на рівні додатків або файлів, зазвичай забезпечує найвищий рівень захисту для окремих, дискретних даних, дозволяючи контролювати доступ і обробку інформації з максимальною точністю. Натомість шифрування на нижчих рівнях, таких як об’єм (volume) або блоки сховища, є більш ефективним для захисту великих масивів даних, де пріоритетом є швидкість і масштабованість процесу.

Рівні шифрування впливають на архітектуру системи та визначають, наскільки гнучко і надійно можна управляти ключами та даними. Важливо, що системи шифрування складаються з трьох основних компонентів: самих даних, механізму шифрування і управління ключами.

В ідеалі ключі шифрування слід зберігати окремо від даних і засобів шифрування, що мінімізує ризики компрометації. Рівні шифрування хмарних даних зображено на рисунку 3.3.

Для об’єктних сховищ дані можуть бути зашифровані на стороні клієнта ще до передачі в хмару, що підвищує конфіденційність і зменшує залежність від провайдера. Також можливе шифрування на стороні сервера, яке виконується після

отримання даних провайдером – це спрощує процес, але знижує рівень контролю користувача.

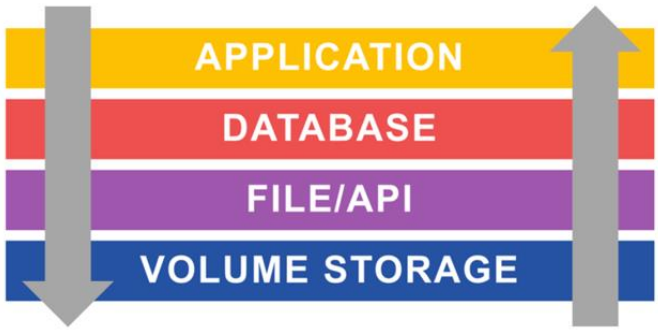

Рисунок 3.3 – Рівні шифрування хмарних даних

Крім того, шифрування може виконуватися через проміжні проксі-сервери сховища, що часто використовується для безпечного резервного копіювання даних.

Шифрування у платформах як послуга (PaaS) і програмному забезпеченні як послуга (SaaS) суттєво відрізняється від традиційних підходів, оскільки тут багато залежить від конкретного типу платформи та функціональних можливостей, які надає хмарний провайдер. У випадку PaaS користувачі часто мають можливість інтегрувати власні механізми шифрування безпосередньо на рівні додатку. Це означає, що шифрування може бути реалізоване в коді програми, де дані захищаються ще до передачі у хмарне середовище, що підвищує контроль над безпекою. Крім того, шифрування може відбуватися із залученням зовнішніх служб або серверів шифрування, що забезпечує додатковий рівень абстракції та безпеки, але й потребує більш складної архітектури.

Щодо баз даних, що працюють у хмарі як частина PaaS, часто використовується прозоре шифрування бази даних, яке автоматично шифрує дані «під капотом» без потреби втручання додатку. Водночас провайдери пропонують різні моделі керування ключами, а також шифрування на рівні окремих полів таблиць, що дозволяє більш гнучко захищати конфіденційну інформацію. При цьому важливо звертати увагу на те, хто має контроль над ключами шифрування – чи вони зберігаються у провайдера, чи клієнт має змогу самостійно управляти ними, що підвищує рівень безпеки, але збільшує складність управління.

У випадку SaaS, можливості користувача щодо шифрування суттєво обмежені. Зазвичай користувач повністю покладається на механізми безпеки та шифрування, які надає постачальник послуг. Альтернативою є використання проксі-серверів шифрування, які «сидять» між користувачем і SaaS-сервісом, забезпечуючи шифрування даних перед їх передачею в хмару. Проте такий підхід може створювати додаткові проблеми. По-перше, проксі-сервер повинен мати змогу розшифровувати і повторно шифрувати дані, що потенційно створює вразливість, оскільки фактично стає «людиною посередині». По-друге, це може негативно вплинути на продуктивність і функціональність програми, оскільки проксі-сервер інтерпретує й змінює потік даних, що не завжди підтримується SaaS-сервісом. Тому, хоча проксі-шлюзи можуть бути корисними в окремих сценаріях, їх застосування обмежене і вимагає ретельного оцінювання ризиків.

Загалом, питання шифрування в PaaS та SaaS-середовищах пов’язане з балансом між контролем користувача і зручністю платформи. Чим більше можливостей для користувача керувати шифруванням і ключами, тим вищий рівень безпеки, але це часто ускладнює процес інтеграції і експлуатації. Водночас повна довіра провайдеру знижує гнучкість і може викликати побоювання щодо конфіденційності та відповідності нормативам. Тому при виборі та налаштуванні хмарних сервісів потрібно ретельно вивчати, які опції шифрування пропонуються, і наскільки вони відповідають вимогам безпеки конкретного бізнесу чи організації.

У випадку шифрування в рамках PaaS, коли ви маєте контроль над власним кодом, у вас завжди є можливість реалізувати шифрування безпосередньо на рівні додатку. Це дає велику гнучкість і підвищує портативність, оскільки дані шифруються до того, як потрапляють у хмарне середовище, що зменшує залежність від конкретної платформи. Проте слід враховувати особливості роботи вашої платформи, зокрема потенційні проблеми з енергозалежною пам’яттю (volatile memory) та файлами підкачки, які можуть тимчасово зберігати незашифровані дані. Важливо розуміти, як саме ваша платформа обробляє ці дані, щоб не допустити випадкових витоків інформації. Якщо ви є хмарним провайдером, рекомендується застосовувати окремі ключі шифрування для

кожного клієнта, що суттєво підвищує рівень безпеки і мінімізує ризики масштабних порушень даних.

Що стосується SaaS, то тут питання шифрування набагато складніше, оскільки контроль над процесом практично повністю належить постачальнику послуг. Деякі провайдери пропонують варіанти керування ключами, де клієнт може частково контролювати ключі шифрування, однак це скоріше виняток, ніж правило. Якщо ж клієнт хоче самостійно забезпечити шифрування даних, найчастіше застосовують проксі-сервери шифрування. У цьому випадку весь трафік між користувачем і SaaS-програмою спрямовується через зовнішній інструмент, який шифрує дані перед тим, як вони потраплять до хмарного сервісу. Хоча такий підхід підвищує контроль над конфіденційністю, він має суттєві мінуси – проксі може порушувати роботу SaaS-додатків, обмежуючи їхню функціональність і знижуючи продуктивність. Більш того, для забезпечення безпеки проксі має мати можливість розшифровувати дані, що створює потенційну «вразливість людини посередині» і може бути складним у підтримці.

Таким чином, вибір між різними методами шифрування в PaaS і SaaS зумовлюється балансом між рівнем контролю, зручністю використання та потенційними ризиками безпеки. Важливо ретельно вивчати можливості провайдера, розуміти специфіку платформи і, за можливості, застосовувати підходи, які найкраще відповідають вимогам вашого бізнесу та політиці безпеки.

3.4 Керування ключами шифрування та додаткові параметри захисту даних у Amazon EC2

Правильне керування ключами шифрування є ключовим елементом забезпечення безпеки даних у хмарних середовищах, і хмарні обчислення надають для цього набагато більше можливостей, ніж традиційні локальні рішення [19]. Хмарні провайдери, зокрема Amazon EC2, можуть пропонувати фізичні апаратні засоби захисту, такі як апаратні модулі безпеки, що забезпечують надійне зберігання і обробку ключів шифрування. Окрім цього, можливе розгортання

віртуальних або програмних пристроїв у хмарі, які взаємодіють із ключами, або ж підключення до наявних фізичних пристроїв через гібридні архітектури.

Сучасні рішення також включають спеціалізовані служби керування ключами, які надають самі хмарні провайдери або сторонні сервіси. Вони можуть варіюватись від повністю керованих провайдером ключів до моделей, у яких клієнт має повний контроль над власними ключами. Важливо розуміти, що реалізація BYOK у різних провайдерів і сервісах може суттєво відрізнятися за рівнем безпеки, функціональністю та складністю інтеграції.

Вибір конкретного підходу до керування ключами повинен базуватися на аналізі моделей ризиків і загроз, які характерні для вашого бізнесу чи організації. Необхідно оцінити, які саме загрози ви намагаєтесь запобігти, і які технічні параметри пропонує обрана платформа. Водночас слід пам’ятати, що не всі типи даних потребують однакового рівня захисту, тому застосування максимально безпечних налаштувань за замовчуванням не завжди є доцільним. Раціональний підхід полягає в балансі між рівнем безпеки та зручністю керування.

Крім керування ключами, Amazon EC2 пропонує й інші важливі механізми захисту даних. Інтеграція Platform as a Service та інших сучасних архітектурних рішень дозволяє значною мірою перекласти відповідальність за безпеку інфраструктури на хмарного провайдера. Це дозволяє користувачам зосередитись на безпеці своїх додатків та даних, зменшуючи при цьому загальну площу поверхні атаки в стосунку до безпеки. Використання PaaS дає змогу ефективніше розвивати та підтримувати додатки, одночасно скорочуючи навантаження на IT-спеціалістів у питаннях безпеки, оскільки більшість технічних аспектів інфраструктури та захисту бере на себе провайдер.

Важливим елементом забезпечення безпеки хмарних даних є надійний моніторинг активності та своєчасне сповіщення про потенційні загрози. Amazon EC2, як частина екосистеми AWS, пропонує широкий спектр інструментів для контролю й управління безпекою, що дозволяють ефективно відстежувати всі події в хмарному середовищі. Зокрема, сервіс AWS CloudTrail фіксує всі дії, які виконуються в межах облікового запису користувача, створюючи детальний

журнал операцій. Це дає змогу виявляти аномальні чи небажані дії, швидко реагувати на інциденти та проводити аудит безпеки.

Ще одним важливим інструментом є AWS Config, який відповідає за моніторинг та відстеження змін у конфігурації хмарних ресурсів. Це дозволяє забезпечувати відповідність політикам безпеки та керувати ризиками, пов’язаними з неправильними налаштуваннями, що можуть створити вразливості.

Захист додатків від зовнішніх загроз значно посилюється завдяки використанню сервісів AWS Shield і AWS Web Application Firewall. AWS Shield спеціалізується на захисті від розподілених атак відмови в обслуговуванні (DDoS), які можуть паралізувати роботу додатків, у той час як AWS WAF допомагає блокувати відомі веб-загрози, такі як SQL-ін’єкції чи атаки через скрипти між сайтами.

Для централізованого та безпечного керування ключами шифрування AWS пропонує сервіс Key Management Service, який спрощує управління ключами, забезпечуючи при цьому надійний захист конфіденційних даних. Додатково, Amazon GuardDuty використовує алгоритми машинного навчання для аналізу мережевого трафіку і поведінкових аномалій, що дає змогу оперативно виявляти потенційні зловмисні дії в інфраструктурі.

Комплексна інтеграція цих сервісів створює багаторівневу систему захисту, що значно мінімізує ризики безпеки. Такий підхід підвищує загальний рівень довіри до хмарної інфраструктури, дозволяючи споживачам бути впевненими в захисті своїх додатків і даних, які вони розгортають на Amazon EC2.

Особливо важливою є і превентивна складова – запобігання втраті даних. Цей аспект часто є ключовим для SaaS-рішень і може бути реалізований через інтеграцію з інструментами CASB (Cloud Access Security Broker), які забезпечують контроль за доступом і політиками безпеки у хмарі.

Традиційні підходи до цифрового управління правами не завжди є ефективними у хмарних середовищах, проте деякі служби SaaS і PaaS вже впроваджують механізми, схожі на DRM, наприклад, контроль доступу, обмеження

перегляду або обробки контенту, що дозволяє забезпечувати аналогічний рівень захисту.

Ще одним важливим аспектом є маскування даних, яке є критично необхідним для створення безпечних тестових середовищ. Маскування гарантує, що у процесі розробки та тестування не відбувається розкриття реальних виробничих даних, що суттєво знижує ризики витоку конфіденційної інформації. Цей метод дозволяє створювати максимально наближені до реальних дані для тестування, одночасно зберігаючи приватність і безпеку.

Таким чином, поєднання моніторингу, керування ключами, застосування передових засобів захисту та контролю доступу, а також маскування даних формує надійний і комплексний підхід до безпеки хмарних даних у середовищі Amazon EC2 і суміжних сервісів.

Життєвий цикл безпеки даних у хмарі – це інструмент, який допомагає візуалізувати, як дані використовуються та розкриваються, а також визначати ключові точки для застосування заходів безпеки [21].

Життєвий цикл складається з шести фаз – від створення даних до їх остаточного знищення. Проте на практиці дані постійно переміщуються між цими фазами в процесі використання. Кожна фаза має власний набір потенційних ризиків і заходів контролю безпеки. Життєвий цикл безпеки даних зображено на рисунку 3.4.

Дані можуть перебувати в різних місцях, доступ до них здійснюється з різних пристроїв, користувачів і сервісів. Візуалізація цих процесів є важливою для розробки ефективних засобів контролю безпеки.

Залежно від розташування даних, конкретної фази життєвого циклу, а також учасників, які працюють з інформацією, формується перелік можливих ризиків і контрольних заходів. Порівнюючи цей перелік з тим, що дозволено політиками безпеки, ми відфільтровуємо потенційні загрози, залишаючи лише дозволені дії та доступи [22].

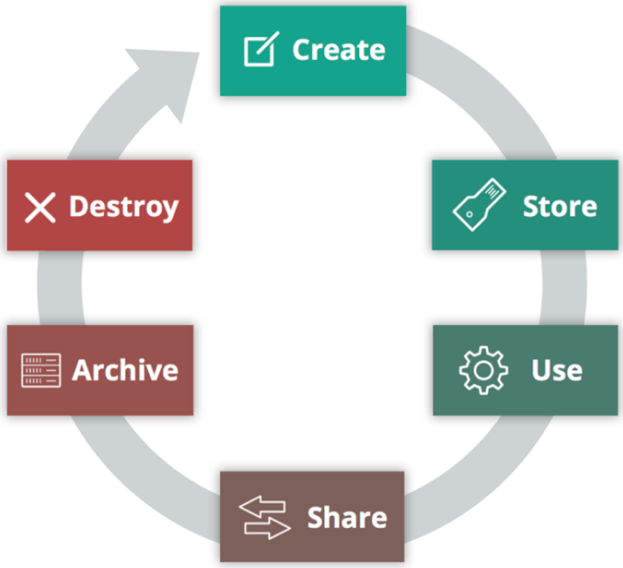

Рисунок 3.4 – Життєвий цикл безпеки даних

Ми можемо закодувати цей процес у вигляді матриці дозволів, яка чітко визначає, хто і які дії може виконувати з даними на кожній фазі життєвого циклу. Ця матриця слугує основою для реалізації засобів контролю безпеки, зокрема механізмів контролю доступу, які забезпечують відповідність фактичних дій встановленим політикам і мінімізують ризики несанкціонованого доступу або використання даних.

Підсумовуючи, життєвий цикл безпеки даних у хмарі є ключовим інструментом для системного управління захистом інформації на всіх етапах її обробки. Розуміння фаз цього циклу та потенційних ризиків допомагає впроваджувати ефективні заходи контролю, адаптовані до конкретних умов і сценаріїв використання даних. Використання матриці дозволів і впровадження відповідних механізмів контролю доступу створюють надійний каркас безпеки, що дозволяє мінімізувати загрози та забезпечити цілісність, конфіденційність і доступність даних у хмарних середовищах.

Загалом основними методами захисту є контроль доступу, шифрування, резервне копіювання, моніторинг і аудит. Контроль доступу, реалізований через багатофакторну автентифікацію, ролево-орієнтовані моделі та матриці прав, дозволяє мінімізувати ризики несанкціонованого доступу. Шифрування даних, що

застосовується на різних рівнях (клієнтському, серверному, програмному), забезпечує захист як у процесі передачі, так і під час зберігання. У сервісах IaaS, PaaS і SaaS шифрування має свої особливості: від повного контролю користувача в PaaS до обмежених можливостей у SaaS, де часто застосовуються проксі-сервери для додаткового захисту.

Керування ключами шифрування в Amazon EC2 підтримується через сервіс AWS Key Management Service, який забезпечує надійне зберігання та обробку ключів, а також інтеграцію з апаратними модулями безпеки. Додаткові інструменти, такі як AWS CloudTrail, AWS Config, AWS Shield, AWS WAF та Amazon GuardDuty, створюють багаторівневу систему захисту, що охоплює моніторинг, виявлення загроз і захист від атак. Особлива увага приділяється життєвому циклу безпеки даних, який включає шість фаз — від створення до знищення, з унікальними ризиками та заходами контролю на кожному етапі. Використання матриць дозволів і інструментів, таких як CASB, DLP та URL-фільтрація, сприяє ефективному управлінню безпекою.

Таким чином, захист даних у хмарних обчисленнях вимагає комплексного підходу, що поєднує технічні, організаційні та процедурні заходи. Amazon EC2, завдяки інтеграції передових сервісів і підтримці міжнародних стандартів, забезпечує надійне середовище для захисту даних, дозволяючи організаціям ефективно протистояти сучасним кіберзагрозам і відповідати вимогам безпеки.

ВИСНОВКИ

У кваліфікаційній роботі бакалавра проведено ґрунтовне дослідження параметрів захисту хмарних обчислень і даних на прикладі платформи Amazon EC2, що є однією з провідних у світі хмарних сервісів. Аналіз безпеки даних у хмарі показав, що ця тема є надзвичайно багатогранною і вимагає комплексного підходу. Розглянуто принципи побудови безпечної інфраструктури в Amazon EC2, методи управління безпекою, комплаєнс, юридичні аспекти та аудит, які формують фундамент для надійного захисту інформації у хмарних середовищах.

Особливу увагу приділено механізмам шифрування даних для різних моделей хмарних послуг, а також керуванню ключами шифрування, що є критично важливим для підтримки конфіденційності і цілісності інформації. У роботі розглянуто сучасні інструменти безпеки Amazon, такі як AWS CloudTrail, AWS Config, AWS Shield, KMS та інші, що забезпечують багаторівневий захист і моніторинг, сприяючи швидкому виявленню та реагуванню на загрози.

Значним є розуміння життєвого циклу безпеки даних у хмарі, який охоплює всі етапи роботи з інформацією – від її створення до знищення. Визначення потенційних ризиків і застосування матриці дозволів для контролю доступу дозволяє мінімізувати вразливості та забезпечити цілісність, доступність і конфіденційність даних.

Отже, забезпечення безпеки в хмарних обчисленнях потребує не лише застосування технічних рішень, але й продуманого управління ризиками, дотримання нормативних вимог і систематичного аудиту безпеки. Інтеграція сучасних технологій шифрування, керування ключами і механізмів контролю доступу створює надійний каркас для безпечного функціонування хмарних сервісів, що відповідають потребам сучасного бізнесу й суспільства. Ці підходи відкривають можливості для розвитку більш ефективних і захищених хмарних рішень у майбутньому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cloud computing with AWS. Aws. Офіційний сайт. URL: https://aws.amazon.com/what-is-aws/?nc1=h_ls (дата звернення: 23.02.2025).
2. Amazon EC2. AWS. Офіційний сайт. URL: https://aws.amazon.com/ec2/ (дата звернення: 23.02.2025).
3. AWS Cloud Security. AWS. Офіційний ресурс. URL: https://aws.amazon.com/security/ (дата звернення: 23.02.2025).
4. Security, Identity, and Compliance on AWS. AWS. Офіційний сайт. URL: https://aws.amazon.com/products/security/ (дата звернення: 23.02.2025).
5. NIST Cybersecurity framework. NIST. Офіційний сайт. URL: https://www.nist.gov/cyberframework (дата звернення: 23.02.2025).
6. Корченко О. и др. Метод оцінювання рівня підвищення стану кіберзахисту об’єктів критичної інфраструктури держави // *Наукоємні технології*. 2024. Т. 61. №. 1. С. 3-20.
7. Кошова О. П., Лисенко Д. В., Волков С. І. Сучасні технології моніторингу мережевої безпеки: роль SIEM WAZUH у виявленні та реагуванні на загрози //Таврійський науковий вісник. Серія: *Технічні науки*. 2025. №. 1. С. 67-75. DOI: https://doi.org/10.32782/tnv-tech.2025.1.7
8. Корченко О., Іванченко Є. Система оцінювання підвищення стану кіберзахисту об’єктів огляду критичної інфраструктури держави //*Ukrainian Scientific Journal of Information Security*. Т. 30. №. 1. С. 95-99.
9. Bermudez I., Traverso S., Munafo M., Mellia, M. A distributed architecture for the monitoring of clouds and CDNs: Applications to Amazon AWS. *IEEE Transactions on Network and Service Management*, 2014. №11(4). PP. 516-529.
10. Peters L. C. S. Data protection in Amazon Web Services Is the data of European data subjects sufficiently protected in Amazon Web Services?: master thesis. Tilburg University. LLM Law & Technology, 2020. 87 p.

11. Chythanya K. R. et al. Security and Safety in Amazon EC2 Service–A Research on EC2 Service AMIs‖ //*International Journal of Innovative Technology and Exploring Engineering (IJITEE)*. 2019. PP. 2278-3075.
12. Kota H. S. A., Shyam Mohan J. S., Challa N. P. A perspective of security features in amazon web services //*Congress on Intelligent Systems: Proceedings of CIS* 2020, Volume 1. Springer Singapore, 2021. PP. 659-673.
13. Ali S., Riasat H., Zubair S. Amazon Web Service EC2 and its Features: A Systematic Literature Review //*Journal of Information & Communication Technology (JICT)*. 2021. Т. 15. №. 1. PP. 7-16.
14. Kulkarni G., Sutar R., Gambhir J. Cloud computing-Infrastructure as service-Amazon EC2 //*International journal of Engineering research and applications*. 2012. Т. 2. №. 1. P. 117-125.
15. Орлов М., Дмитрів Ю. Аналіз програмних інструментів для автоматизації функцій конфігурування і управління в іт інфраструктурах. *SISN*. 2024; Vol. 15. PP. 370-388. DOI: https://doi.org/10.23939/sisn2024.15.370
16. Щерба М. О. Дослідження методів забезпечення інформаційної безпеки у хмарному середовищі. *Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023)* : матеріали дев'ятої Міжнар. наук.-техн. конф., м. Харків, 7 грудн. 2023 р. Харків : ХНУРЕ, 2023. С. 206-207.
17. Кустливий А. О., Михайлович Ч. В. Міграція в хмари. *Priority directions of science and technology development* : The 4 th International scientific and practical conference. (December 20-22, 2020). Kyiv, Ukraine. 2020. PP. 433.
18. Білова Т. Г., Ярута В. О. Методи підвищення безпеки обробки даних в хмарних обчисленнях //*Збірник наукових праць Харківського університету Повітряних Сил*. 2015. №. 4. С. 71-73.
19. Qureshi M.B.; Qureshi M.S.; Tahir S.; Anwar A.; Hussain S.; Uddin M.; Chen C.-L. Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud. *Symmetry* 2022. Vol. 14. DOI: https://doi.org/10.3390/sym14040695 (дата звернення: 15.03.2025).

20. Mosca P. et al. Cloud security: Services, risks, and a case study on amazon cloud services //*International Journal of Communications, Network and System Sciences*. 2014. T. 7. №. 12. PP. 529-535.
21. Singh Kashyap V. Scalable Cloud Computing Architecture for IoT Data Processing. *Computational Engineering and Technology Innovations*, 2024. № 1(1). PP. 52-59. https://doi.org/10.48314/ceti.v1i1.26
22. Balduzzi M. et al. A security analysis of amazon's elastic compute cloud service //*Proceedings of the 27th annual ACM symposium on applied computing*. 2012. PP. 1427-1434.

Додаток А. Ключові параметри безпеки даних в Amazon EC2

Таблиця А1

Пункт	Опис
Основні сервіси захисту	AWS CloudTrail, AWS Config, AWS Shield, AWS WAF, AWS KMS, Amazon GuardDuty
Модель керування ключами	Bring Your Own Key (BYOK), централізоване управління ключами (AWS KMS), HSM
Фази життєвого циклу даних	1. Створення, 2. Зберігання, 3. Використання, 4. Передача, 5. Архівування, 6. Знищення
Ризики на різних фазах	Неавторизований доступ, витік даних, пошкодження, втрата доступності
Основні засоби контролю	Шифрування, контроль доступу, моніторинг активності, сповіщення, аудит
Засоби моніторингу	AWS CloudTrail (логування дій), AWS Config (відстеження змін), GuardDuty (виявлення аномалій)
Захист від атак	AWS Shield (DDoS), AWS WAF (захист веб-додатків)
Підхід до безпеки даних	Комплексний: технічні засоби + управління ризиками + комплаєнс + аудит
Роль PaaS у захисті	Зниження навантаження на користувача, відповідальність провайдера за безпеку

Особливості хмарного середовища	Динамічне середовище, множинні користувачі, гібридні моделі, розподілені ресурси
Ключові рекомендації	Аналіз ризиків, сегментація даних за рівнями безпеки, регулярний аудит, резервне копіювання
Типи шифрування	Шифрування даних у спокої (at-rest) та під час передачі (in-transit)
Управління доступом	Мультифакторна аутентифікація (MFA), ролі та політики IAM
Резервне копіювання та відновлення	Автоматизовані бекапи, сценарії відновлення після збоїв
Логування та аудит	Централізоване збирання логів, аналіз інцидентів безпеки
Політика зберігання ключів	Визначення терміну життя ключів, регулярна ротація
Тестування безпеки	Проведення періодичних пенетраційних тестів та аудитів
Обробка інцидентів	Процедури реагування та інформування про інциденти
Відповідність стандартам	ISO/IEC 27001, GDPR, HIPAA, PCI DSS (за потреби)
Використання маскування даних	Для тестових та розробницьких середовищ
Особливості SaaS безпеки	Керування клієнтськими ключами, проксі-шифрування
Інструменти запобігання втраті даних (DLP)	Інтеграція з CASB, контроль передачі даних