МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Освітньо-професійна програма «Комп'ютерна інженерія

Спеціальність 123 «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА

БАКАЛАВРА

здобувача освіти денної форми навчання
БКС 27.27.000.00 БКР

Студзінського Дмитра Сергійовича

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Освітньо-професійна программа: «Комп'ютерна інженерія»
Спеціальність 123 «Комп'ютерна інженерія»
Група БКС-27

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра на тему:

«Аналіз загроз кібербезпеці хмарних сервісів та методів боротьби з ними»

Проектний матеріал складається з пояснювальної записки на 74 сторінках та мультимедійної презентації на 14 сторінках.

Здобувач освіти _____ (Студзінський Д.С.)

Керівник роботи _____ (Харченко Р.Ю.)

Консультанти:

з охорони праці _____ (Чорновол Н.І.)

за дотриманням вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувач кафедри _____ (Іванова Я.В.)

Завідуючий відділенням _____ (Скорнякова О.В)

Захист «26» 06 2023 р. Протокол ДКК № 3

Оцінка ДКК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

З метою визначення базових умов, щодо подальших досліджень для визначення загроз хмарним технологіям та мірам їх протидії, у роботі проведений розширений аналіз хмарних обчислень як сервісів. Серед наведених сервісів виділено базові сервіси IaaS, SaaS, PaaS, які є основою для існування більш уніфікованих сервісів (CaaS, MCaaS, DaaS, FaaS, IPaaS, MBaaS, NaaS, SeCaaS, DBaaS, MaaS, GaaS, STaaS, TaaS, DRaaS,), що збільшують область використання. Вказані можливі постачальники сервісів, в тому числі і українські. У дипломі буде зроблений огляд хмарних рішень та представлений загальний аналіз можливостей захисту їх застосування від загроз кібербезпеці.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 20____ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачу освіти *Студзінському Дмитру Сергійовичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз загроз кібербезпеці хмарних сервісів та методів боротьби з ними*

затверджена наказом по коледжу від "17" 10 20 22 р. № 235-А2-09

2. Термін здачі студентом кваліфікаційної роботи 16.06.2023 р.

3. Вихідні дані до роботи *1. Несанкціонований доступ до Веб-сайту; 2. Веб-додаткі; 3. Система захисту веб-сайту; 4. DDoS-атаки; 5. Firewal;l 6. Системи виявлення атак (СВА); 7. HTTP і HTTPS; 8. Web Firewall Application;9. IaaS, PaaS, SaaS.;10. Фаервол як сервіс*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1. Аналіз предметної області;

2. Аналіз загроз кібербезпеці хмарних сервісів;

3. Методи боротьби з загрозами кібербезпеці хмарних сервісів.

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) *Варіанти підключення до хмарної технології; Структура хмарних технологій;Моделі хмарних служ Фаєрвол (Firewall); Приклад інфраструктури IaaS; Архітектура IaaS облака; Модель загроз хмарного кіберпростору; Хмарне резервне копіювання; Принцип роботи CSPM Захист хмарних додатків за допомогою CASB; Схема роботи механізму розмежування доступу; Переваги безпеки як послуги; Вразливості віртуального середовища*

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що стосуються їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Харченко Р.Ю.*		
Охорона праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В..*		

7. Дата видачі завдання 01.05.2023

Керівник роботи *Харченко Р.Ю.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз предметної галузі*	5.05.2023	виконав
2.	*Аналіз технічного завдання та пошук літератури*	7.05.2023	виконав
3.	*Огляд концепції хмарних технологій*	9.05.2023	виконав
4.	*Огляд властивості та моделі хмарних обчислень*	11.05.2023	виконав
5.	*Аналіз послуг, що надаються хмарними системами*	13.05.2023	виконав
6.	*Аналіз архітектури хмарної інфраструктури*	16.05.2023	виконав
7.	*Інформаційна безпека у хмарній інфраструктурі*	18.05.2023	виконав
8.	*Основні загрози хмарних технологій*	20.05.2023	виконав
9.	*Модель загроз хмарного кіберпростору*	23.05.2023	виконав
10.	*Загрози хмарних обчислень та вимоги до їхньої безпеки*	25.05.2023	виконав
11.	*Аналіз проблем захисту хмарного кіберпростору*	27.05.2023	виконав
12.	*Забезпечення кібербезпеки хмарних сервісів*	30.05.2023	виконав
13.	*Результати аналізу сфери хмарної кібербезпеки*	3.06.2023	виконав
14.	*Аналіз ринку інструментів захисту хмарних середовищ*	5.06.2023	виконав
15.	*Розробка питань з охорони праці*	8.06.2023	виконав
16.	*Оформлення креслень та тексту ПЗ*	10.06.2023	виконав

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27. 27. 000. 00 БКР	Випускна робота бакалавра	74	
А4			БКС 27. 27 000. 00 БКР ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 27. 27. 000. 00 БКР		
Розробив		Студзінський Д.С.			Аналіз загроз кібербезпеці хмарних сервісів та методів боротьби з ними	Літ.	Аркуш 4 / Аркушів
Перевірив		Харченко Р.Ю.				У Д П	
Н. Контр.		Петрашова В.І.				ОТФК ОНТУ, гр. 2БКС-27	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Інформаційні ресурси відіграють дуже важливу роль у сучасній дійсності, оскільки розширюється спектр їх використання та коло користувачів, які мають доступ до інформаційних систем, що зберігають та обробляють ці ресурси, збільшується обсяг інформації, що обробляється та зберігається в електронних форматах. Розвиток також придбали методи та засоби автоматизації процесу зберігання та обробки інформації, оскільки необхідно надати безлічі користувачів різний рівень доступу до однієї інформаційної системи, забезпечивши при цьому повну безпеку ресурсів при передачі та обробці даних.

При цьому кількість уразливостей, які виявляються в цих інформаційних системах, та загроз їх використання неминуче збільшується. Тому в умовах стрімкої популяризації технологій зберігання та обробки інформації питання забезпечення інформаційної безпеки та, відповідно, створення стабільної системи захисту інформації є не менш важливим, ніж створення та підтримання стабільної системи обробки та зберігання даних.

Використання хмарних сервісів стає все більш поширеним, чи то обчислення будь-якої складності, проста обробка даних або зберігання різних обсягів даних. Це зручно для користувачів, оскільки забезпечує високопродуктивну, стійку до відмови віртуальну інфраструктуру, що дозволяє швидко і безпечно обробляти дані, але без необхідності інвестувати в дороге обладнання, його обслуговування, налаштування та відповідний рівень безпеки для найважливіших інформаційних ресурсів. Постачальники хмарних послуг відповідають за забезпечення безпеки ресурсів, надання необхідної обчислювальної потужності та забезпечення доступності даних для клієнтів.

1. ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1. Аналіз предметної області

1.1.1 Концепція хмарних технологій

Хмарні технології – інформаційно-технологічна концепція, що передбачає забезпечення повсюдного та зручного мережного доступу на вимогу до загального банку конфігурованих обчислювальних ресурсів (наприклад, мереж передачі даних, серверів, пристроїв зберігання даних, додатків та сервісів - як разом, так і окремо), які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними витратами. Хмарні технології - це стратегія, яка передбачає віддалену обробку та зберігання даних. Технологія надає користувачам Інтернету доступ до ресурсів серверних комп'ютерів і використання програмного забезпечення як онлайн-сервісу. Це означає, що будь-яке середовище з підключенням до Інтернету може використовувати потужності віддаленого сервера для виконання складних обчислень і обробки даних, (рис 1.1).

Рисунок 1.1 Варіанти підключення до хмарної технології

Суть хмарних технологій полягає в тому, щоб користувач міг працювати в будь-який час з потрібними додатками, файлами незалежно від конкретного «пристрою», на якому він працюватиме.

Власне, вся різниця полягає виключно у методі зберігання та обробки даних. Якщо всі операції відбуваються на нашому комп'ютері (з використанням його потужностей), то це - не "хмара", а якщо процес відбувається на сервері в мережі, це саме те, що і прийнято називати «хмарною технологією». Іншими словами, хмарні технології - це різні апаратні, програмні засоби, методології та інструменти, які надаються користувачеві, як інтернет-сервіси, для реалізації своїх цілей, завдань, проектів.

Рисунок 1.2 Структура хмарних технологій

У даному поданні «інфраструктура» – це набір фізичних пристроїв (сервери, жорсткі диски тощо), «платформа» - набір послуг та верхівка – програмне забезпечення, доступне на запит користувачів.

Cloud computing (англ. Cloud — хмара; computing — обчислення) — «хмарні обчислення» — концепція «обчислювальної хмари», згідно з якою програми запускаються та видають результати роботи у вікно стандартного

веб-браузера на локальному пристрої, при цьому всі додатки та їх дані, потрібні для роботи, знаходяться на віддаленому сервері в інтернеті. Комп'ютери, які здійснюють такі обчислення, називаються «обчислювальною хмарою». При цьому навантаження між комп'ютерами, що входять до обчислювальної хмари, розподіляється автоматично.

Хмарні послуги дозволяють клієнтським робочим місцям використовувати зовнішні обчислювальні ресурси, ємності для зберігання обробки інформації. Також забезпечується універсальний доступ по мережі – доступність користувачам по мережі передачі даних незалежно від використовуваного пристрою. Сервіс послуг об'єднує ресурси обслуговування великої кількості користувачів в єдиний центр обробки даних для динамічного перерозподілу потужностей між користувачами в умовах постійної зміни попиту. При цьому користувач контролює лише основні параметри послуги, що стосуються саме його, але фактичний розподіл ресурсів, що надаються користувачеві, здійснює хмарні сервери.

1.1.2 Властивості та моделі хмарних обчислень

Розглянемо характеристики хмар:

- можливість самообслуговування без участі людини із боку провайдера;
- наявність широкосмугового доступу до мережі;
- зосередженість ресурсів на окремих майданчиках для їхнього ефективного розподілу;
- швидка масштабованість - ресурси можуть необмежено виділятися та вивільнятися з великою швидкістю залежно від потреб;
- керований сервіс - система управління хмарою автоматично контролює та оптимізує виділення ресурсів, ґрунтуючись на параметрах

сервісу, що вимірюються (розмір системи зберігання, ширина смуги пропускання, число активних користувачів і т. д.).

Самообслуговування на вимогу (On-demand self-service). У споживача є можливість отримати доступ до обчислювальних ресурсів, що надаються, в односторонньому порядку в міру потреби, автоматично, без необхідності взаємодії зі співробітниками кожного постачальника послуг.

Широкий мережевий доступ (Broad network access). Обчислювальні ресурси, що надаються, доступні по мережі через стандартні механізми для різних платформ, тонких і товстих клієнтів (мобільних телефонів, планшетів, ноутбуків, робочих станцій тощо).

Об'єднання ресурсів у пули (Resorce pooling). Обчислювальні ресурси провайдера об'єднуються в пули обслуговування багатьох споживачів по багатоорендної (multi-tenant) моделі. Пули включають різні фізичні та віртуальні ресурси, які можуть бути динамічно призначені і перепризначені відповідно до споживчих запитів. Немає необхідності в тому, щоб споживач знав точне розташування ресурсів, однак можна вказати їх місцезнаходження на більш високому рівні абстракції (наприклад, країна, регіон або центр обробки даних). Прикладами таких ресурсів можуть бути системи зберігання, обчислювальні потужності, пам'ять, пропускна здатність мережі.

Миттєва еластичність (Rapid elasticity). Ресурси можуть бути еластично виділені та звільнені, у деяких випадках автоматично, для швидкого масштабування пропорційно з попитом. Для споживача можливості надання ресурсів бачаться як необмежені, тобто вони можуть бути присвоєні у будь-якій кількості та у будь-який час.

Вимірюваний сервіс (Measured service). Хмарні системи автоматично керують і оптимізують ресурси за допомогою засобів вимірювання, реалізованих на рівні абстрації стосовно різного роду сервісів ((наприклад, управління зовнішньою пам'яттю, обробкою, смугою пропускання або активними користувальницькими сесіями). Використані ресурси можна

відстежувати та контролювати, що забезпечує прозорість для постачальника, так споживача, що використовує сервіс.

Моделі хмарних служб:

Умовно всі види хмарних послуг можна поділити на три типи (рис.1.3)

Програмне забезпечення як послуга (SaaS). Можливість надання споживачеві використання додатків провайдера, що працюють в хмарній інфраструктурі. Програми доступні з різних клієнтських пристроїв або через тонкі інтерфейси клієнтів, такі як веб-браузер (наприклад, веб-пошта) або інтерфейси програм. Споживач при цьому не керує базовою інфраструктурою хмари, у тому числі мережами, серверами, операційними системами, системами зберігання і навіть індивідуальними налаштуваннями програм за винятком деяких налаштувань користувача конфігурації програми.

Платформа як послуга (PaaS). Можливість надання споживачеві для розгортання в хмарній інфраструктурі споживчих (створених або придбаних) програм, реалізованих за допомогою мов програмування, бібліотек, служб та засобів, які підтримує провайдер послуг. Споживач при цьому не керує базовою інфраструктурою хмари, у тому числі мережами, серверами, операційними системами та системами зберігання даних, але має контроль над розгорнутими програмами та, можливо, деякими параметрами конфігурації середовища хостингу.

Інфраструктура як послуга (IaaS). Можливість надання споживачеві систем обробки, зберігання, мереж та інших фундаментальних обчислювальних ресурсів для розгортання та запуску довільного програмного забезпечення, яке може включати операційні системи та додатки. Споживач при цьому не керує базовою інфраструктурою хмари, але має контроль над операційними системами, системами зберігання, розгорнутими програмами і, можливо, обмежений контроль вибору мережевих компонентів (наприклад, мережевий хост).

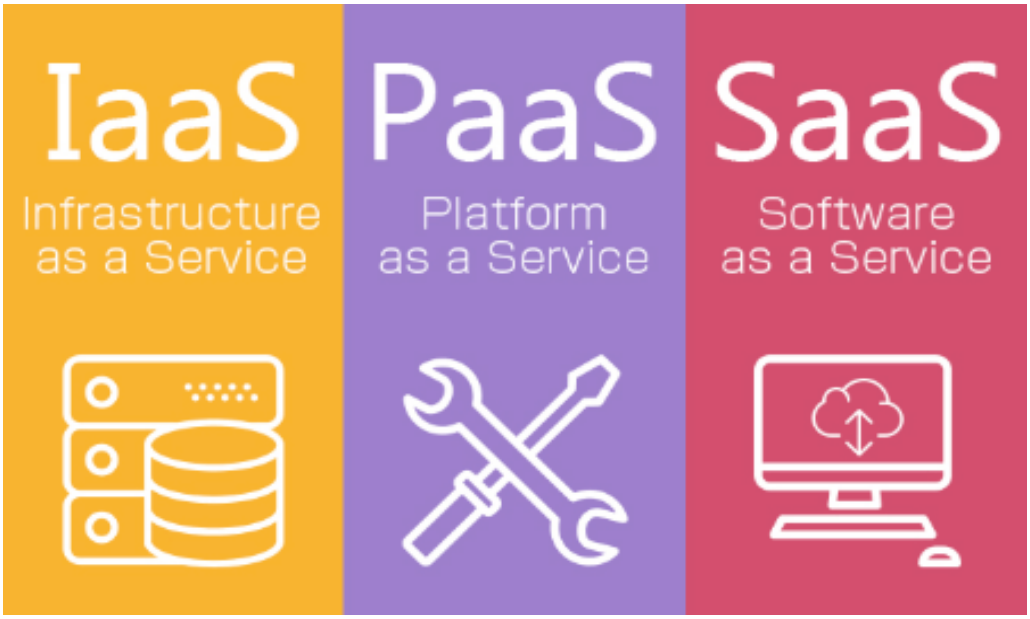


Рисунок 1.3 Моделі хмарних служб

Моделі розгортання:

Приватна хмара (Private Cloud). Хмарна інфраструктура, підготовлена для ексклюзивного використання єдиною організацією, що включає кілька споживачів (наприклад, бізнес-одиниць). Така хмара може перебувати у власності, управлінні та обслуговуванні у самої організації, у третьої сторони та розташовуватися як на території підприємства, так і за його межами.

Хмара спільноти та комунальна хмара (Community cloud). Хмарна інфраструктура, підготовлена для ексклюзивного використання конкретним співтовариством споживачів від організацій, які мають спільні проблеми (наприклад, місії, вимоги безпеки, політики). Хмара може перебувати у власності, управлінні та обслуговуванні в однієї або більше організацій у співтоваристві, у третій стороні і розташовуватися як на території організацій, так і за їх межами.

Публічна (або загальна) хмара (Public cloud). Хмарна інфраструктура, підготовлена широкому загалу для відкритого використання. Воно може перебувати у власності, управлінні та обслуговуванні у ділових, наукових та урядових організацій у будь-яких їх комбінаціях. Хмара є на території хмарного провайдера.

Гібридна хмара (Hybrid cloud). Хмарна інфраструктура є композицією з двох або більше різних інфраструктур хмар (приватні, громадські або державні), що мають унікальні об'єкти, але пов'язані між собою стандартизованими або власними технологіями, які дозволяють переносити дані або додатки між компонентами (наприклад, для балансування навантаження між хмарами) .

1.1.3Послуги, що надаються хмарними системами

Все, що стосується Cloud computing (далі CC), зазвичай прийнято називати aaS - «as a Service», тобто «як сервіс», або «у вигляді сервісу».

В даний час хмарні технології і, власне, їх концепція передбачає надання наступних типів послуг своїм користувачам:

Storage-as-a-Service («зберігання як сервіс»)

Найпростіший з CC - сервісів, що представляє собою дисковий простір на вимогу. Послуга Storage-as-a-Service дає можливість зберігати дані в зовнішньому сховище, в «хмарі». Для користувача воно буде виглядати, як додатковий логічний диск або папка. Сервіс є базовим для інших, оскільки входить до складу практично кожного з них. Прикладом може служити Google Drive та інші схожі сервіси.

Database-as-a-Service («база даних як сервіс»)

Послуга більше для адмінів, бо надає можливість працювати з базами даних, подібно так, як СУБД було встановлено на локальному ресурсі. В цьому випадку значно легше розділяти проекти між різними виконавцями та заощадити на комп'ютерному обладнанні та ліцензіях, необхідних для грамотного використання СУБД в великій чи середньої організації.

Information-as-a-Service («інформація як сервіс»)

Дає можливість віддалено використовувати будь-які види інформації, яка може змінюватися щохвилини або навіть щомиті.

Process-as-a-Service («управління процесом як сервіс»)

Віддалений ресурс, який може зв'язати воєдино кілька ресурсів (таких як послуги або дані, що містяться в межах однієї «хмари» або інших доступних «хмар»), для створення єдиного бізнес-процесу.

Application-as-a-Service («додаток як сервіс»)

Також називається, Software-as-a-Service («ПЗ як сервіс»). Позиціонується як «програмне забезпечення на вимогу», яке розгорнуто на віддалених серверах і кожен користувач може отримувати до нього доступ за допомогою Інтернету, причому всі питання оновлення та ліцензій на дане забезпечення регулюється постачальником даної послуги. Оплата, в даному випадку, відбувається за фактичне використання останнього. Як приклад можна навести Google Docs, Google Calendar і т.п. онлайн-програми.

Platform-as-a-Service («платформа як сервіс»)

Користувачеві надається комп'ютерна платформа з встановленою операційною системою і певним програмним забезпеченням.

Integration-as-a-Service («інтеграція як сервіс»)

Це можливість отримувати з «хмари» повний інтеграційний пакет, включаючи програмні інтерфейси між додатками і управління їх алгоритмами. Сюди входять відомі послуги та функції пакетів централізації, оптимізації та інтеграції корпоративних додатків (EAI), але вони надаються як «хмарний» сервіс.

Security-as-a-Service («безпека як сервіс»)

Даний вид послуги надає можливість користувачам швидко розгортати продукти, що вимагають безпечне використання веб-технологій, електронного листування, локальної мережі. Користувачі даного сервісу мають змогу економити на розгортанні та підтримці своєї власної системи безпеки.

Management / Governace-as-a-Service («адміністрування та управління як сервіс»)

Дає можливість керувати і задавати параметри роботи одного або багатьох «хмарних» сервісів. Це в основному такі параметри, як топологія, використання ресурсів, віртуалізація.

Infrastructure-as-a-Service («інфраструктура як сервіс»)

Користувачеві надається комп'ютерна інфраструктура, зазвичай віртуальні платформи (комп'ютери), пов'язані в мережу, які він самостійно налаштовує під власні цілі.

Testing-as-a-Service («тестування як сервіс»)

Дає можливість тестування локальних або «хмарних» систем з використанням тестового ПЗ з «хмари» (при цьому жодного устаткування або забезпечення на підприємстві, не потрібно).

1.1.4 Архітектура хмарної інфраструктури

При розгляді хмарної архітектури необхідно обов'язково мати на увазі модель хмарних обчислень. У (розділі 1.1.2) було дано пояснення, у чому різниця між існуючими моделями - IaaS, PaaS, SaaS. Розглянемо архітектуру IaaS.

Хмара створюється з кількох фізичних вузлів, з'єднаних швидкими каналами передачі з метою єдиного управління та передачі великих обсягів інформації. Слово "кілька" можна сприймати буквально - фактично з 3-5 вузлів можна побудувати невелику хмару (рис.1.4). Насправді в дата-центрі хмарного провайдера — сотні і навіть тисячі вузлів. За допомогою спеціального ПЗ віртуалізації та формування хмарної інфраструктури користувачі можуть отримувати доступ до ресурсів хмари, при цьому не замислюючись ресурси якого саме фізичного вузла їм виділені. По суті, користувачеві все одно ресурси якого вузла він використовував і де виконується його завдання, де зберігаються його дані - важливо, щоб завдання було виконано, а дані залишилися цілими і безпекою.

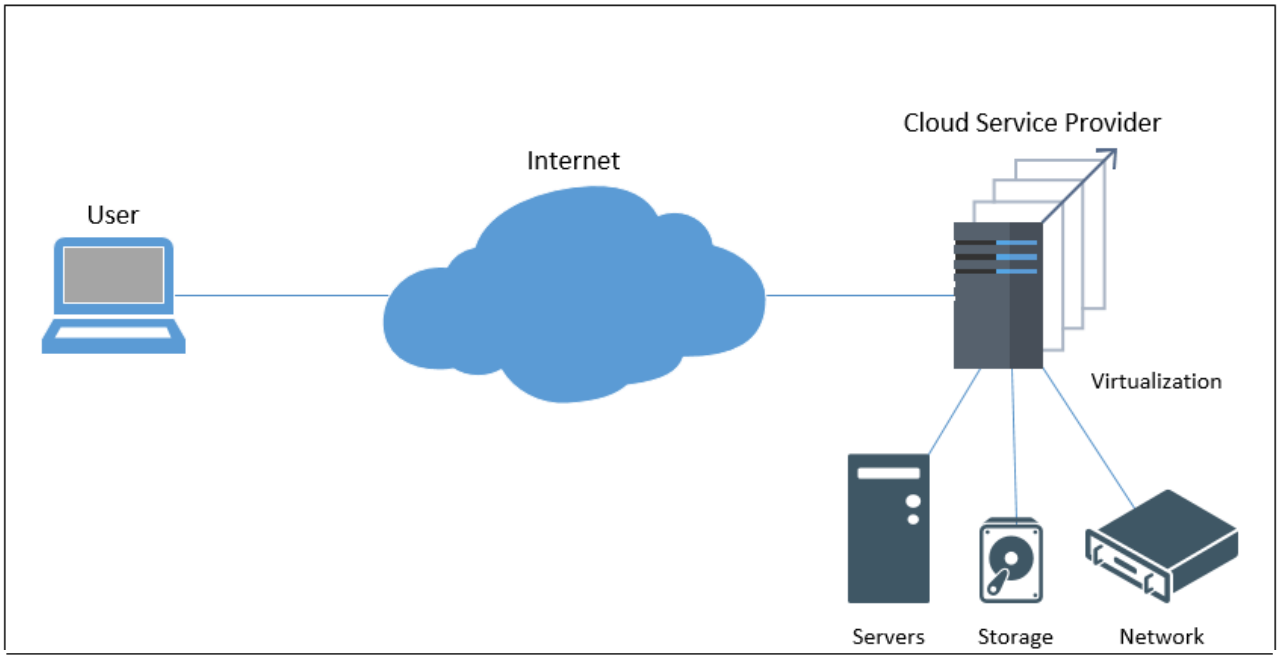


Рисунок 1.4 Приклад інфраструктури IaaS

За допомогою спеціального ПЗ віртуалізації та формування хмарної інфраструктури користувачі можуть отримувати доступ до ресурсів хмари, при цьому не замислюючись ресурси якого саме фізичного вузла їм виділені. По суті, користувачеві все одно ресурси якого вузла він використовував і де виконується його завдання, де зберігаються його дані - важливо, щоб завдання було виконано, а дані залишилися цілими і безпекою.

У хмарі створюються віртуальні машини, на яких запущені гостьові ОС та різні встановлені користувачем програми. У «віртуалці» може виконуватися будь-яка, по суті, «операційна система» — Windows Server, Linux, FreeBSD та ін. На одному апаратному вузлі можна запустити кілька десятків віртуальних машин, що здаються в оренду.

Архітектура хмари моделі IaaS виглядає так:

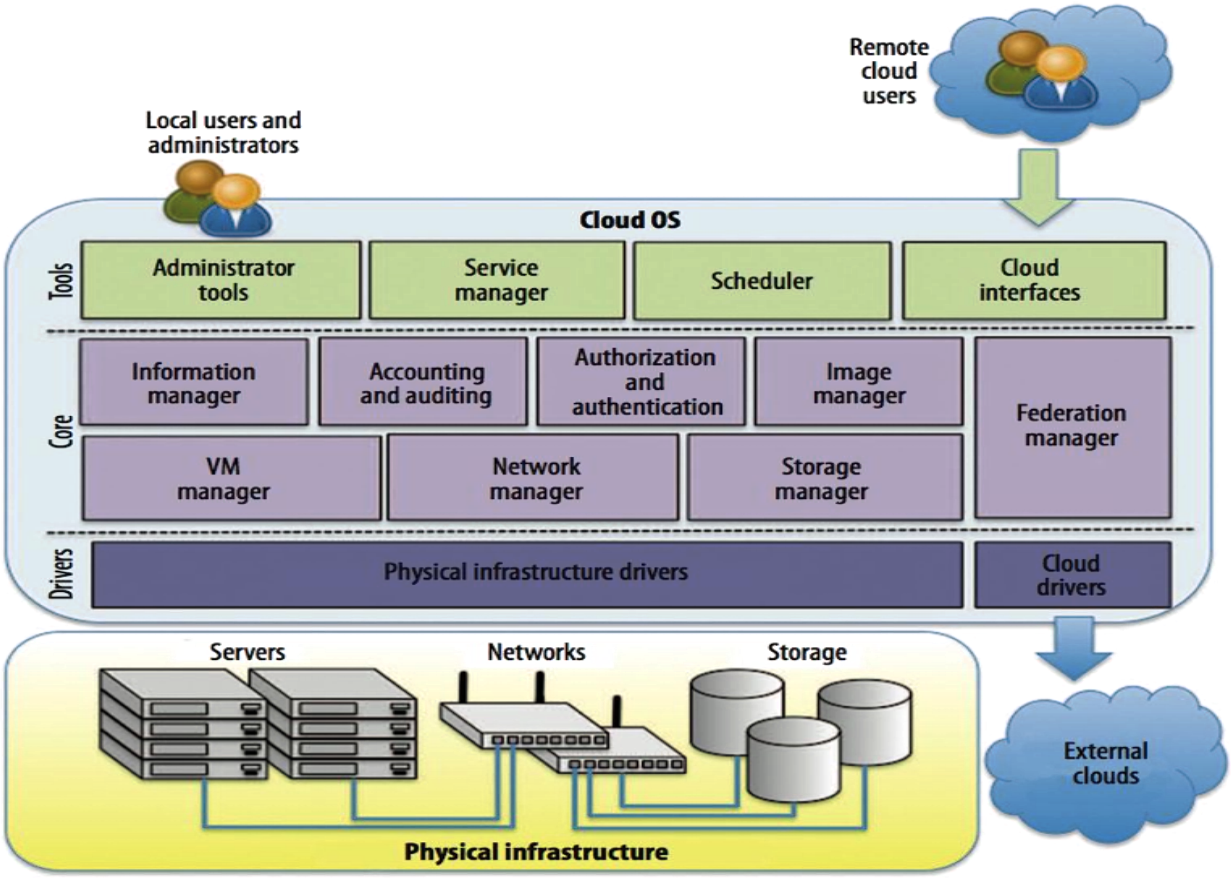


Рисунок 1.5 Архитектура IaaS облака

Більшості користувачів знати повну архітектуру і не потрібно, але все ж таки розглянемо основні моменти. Почнемо знизу нагору. Є якась фізична інфраструктура, що складається із серверів (Servers), мережевого обладнання (Networks) та пристроїв зберігання (Storage). На цій фізичній інфраструктурі виконується хмарна операційна система.

Як завжди, найнижчий рівень будь-якої операційної системи - це драйвери для взаємодії із залізом. Такі драйвери є й у нашої хмарної ОС – драйвери фізичної інфраструктури (Physical infrastructure drivers). Є й драйвери хмари (cloud drivers) - вони потрібні для з'єднання з іншими зовнішніми хмарами (external clouds).

Ядро нашої хмарної ОС – різні диспетчери. Є диспетчер віртуальних машин (VM manager), диспетчер мережі (Network manager), диспетчер сховища (Storage manager) і т. д. Кожен із диспетчерів відповідає за свою частину операційної системи.

На вершині нашої системи – різні засоби управління – засоби адміністратора (administrator tools), диспетчер служб (service manager), планувальник (scheduler), інтерфейси хмари (cloud interfaces). Саме через інтерфейси хмари до нього підключаються користувачі хмари. Інтерфейси можуть бути різними, але останнім часом найчастіше використовується веб-інтерфейс.

1.2. Загрози кібербезпеці хмарних сервісів

1.2.1 Інформаційна безпека у хмарній інфраструктурі

Питання забезпечення інформаційної безпеки хмарних додатків лежать у кількох площинах - юридичної, організаційної та технічної.

Юридичний аспект

Хмарні технології є порівняно новими технологіями. Забезпеченість стандартами в галузі інформаційної безпеки (ІБ) хмарних рішень зараз недостатня. Кількість стандартів можна перерахувати на пальцях. Вузькоспеціалізовані стандарти (наприклад, міжнародний стандарт захисту персональних даних у хмарі ISO/IEC 27018: 2014) почали лише впроваджуватись, починає напрацьовуватись практика їх використання.

Стандарти часто пропонують як вирішення всіх проблем, пов'язаних з хмарними сервісами, але оскільки ця модель послуг базується на вже існуючих, то виникає питання, чи варто встановлювати нові стандарти, наприклад, для хмарних сервісів додатків. Однак нові стандарти для вирішення операційної складності управління хмарними сервісами та стандарти оцінки для визначення безпеки та надійності провайдерів були б досить корисними. Хмарні сервіси розглядаються різними експертами як революційна технологія надання IT-послуг або як нова назва для способу надання послуг, який існує так само довго, як і самі IT.

Існує невизначеність щодо необхідності стандартизації у використанні хмарних сервісів. Однак, безпека є винятком, де досягнуто значного прогресу. Різниця полягає в тому, що технологічні можливості розвинулися настільки, що ідеї, які існували протягом тривалого часу, нарешті можуть бути реалізовані. До появи сучасних високошвидкісних каналів передачі даних централізоване надання більшості послуг було можливе лише з точки, географічно близької до одержувача. Сучасні мережі дозволяють об'єднати роботу централізовано керованих, географічно розподілених серверів.

На даному етапі було опубліковано кілька стандартів і методичних публікацій, огляд яких наведено нижче:

- ISO/IEC 19944: - Дані та їхній потік між пристроями та хмарними сервісами. Описує різні типи потоків даних у хмарних обчисленнях і вплив підключених пристроїв на дані, що обробляються хмарною системою. Описує фреймворк, який розширює існуючий словник хмарних обчислень і базову архітектуру, щоб охопити пристрої, які використовують хмарні сервіси. Визначає категорії даних, що надходять на пристрої користувачів хмарних сервісів, і підвищує прозорість політик і практик, щоб користувачі хмарних сервісів могли розуміти і захищати приватність і конфіденційність своїх даних.
- ISO/IEC 17788:2014 (Information technology - Cloud computing - Overview and vocabulary) – Хмарні обчислення. – Огляд та глосарій -Стандарт містить визначення ключових понять у сфері хмарних обчислень, включаючи опис моделі SPI.
- ISO/IEC 17789:2014 (Information technology - Cloud computing - Reference architecture) – Хмарні обчислення. – Еталонна архітектура – Стандарт надає базові принципи еталонної архітектури хмарних сервісів та описує основні ролі, які взаємодіють у просторі хмарних технологій.
- ISO/IEC 27018:2014 (Information technology – Security techniques – Information security management systems – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) -

Інформаційні технології - Технології безпеки - Системи управління інформаційною безпекою - Кодекс практики захисту персональних даних (PII) у публічних хмарах, що виступають в якості процесорів PII, є набором правил, спрямованих на забезпечення захисту персональних даних у хмарі. Він базується на стандарті інформаційної безпеки ISO 27002 і містить вказівки щодо застосування засобів контролю, передбачених цим стандартом, які застосовуються до персональних даних, а також набір додаткових засобів контролю та пов'язаних з ними інструкцій, а також набір додаткових засобів контролю та пов'язаних з ними рекомендацій для виконання вимог щодо захисту персональних даних у публічних хмарах, на які не поширюються заходи контролю стандарту ISO 27002.

- ISO/IEC 27018 (draft) – надає додаткові поради щодо впровадження належного управління інформаційною безпекою відповідно до стандарту ISO 27002.
- Проект Закону про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень, а саме до наступних законів:

– "Про захист інформації в інформаційно-телекомунікаційних системах"

– "Про захист персональних даних".

Організаційний аспект

Сьогодні підприємствам пропонується широкий спектр засобів захисту хмарних середовищ для забезпечення безпеки під час перенесення робочих навантажень та даних у хмару. Однак деякі з цих інструментів постачаються з індивідуальними інструкціями та пропонуються як окремі послуги. Користувачі та адміністратори хмарних рішень повинні знати, як працюють сервіси хмарної безпеки, як їх правильно налаштувати та як підтримувати розгорнуті хмарні рішення. Хоча сьогодні не бракує різних систем забезпечення безпеки, їх може бути складно налаштовувати і можна легко

припуститися помилки в одній області. Крім того, постійний ризик фішингу і шкідливих програм, кібершахрайство, що росте, і цілий ряд неправильно сконфігурованих хмарних сервісів чинять ще більший тиск на програми кібербезпеки, які вже вирішують так дуже складні завдання. В результаті організації стикаються з витоком даних, а це спричиняє збитки бренду, витрати на відновлення та штрафи. Нижче наведено кілька важливих вимог для забезпечення безпеки даних у хмарі:

- Загальна відповідальність за безпеку та довіру: довіра має першорядне значення при виборі партнера по хмарі, який відповідатиме за свою частину моделі загальної безпеки. Організації повинні чітко розуміти свої ролі та обов'язки, а також мати доступ до незалежних сторонніх аудитів та атестацій систем безпеки.
- Автоматизація та машинне навчання: хмарні погрози мчать зі швидкістю автомобіля, а традиційні корпоративні системи безпеки можуть аналізувати інциденти та реагувати на них зі швидкістю людини. Сучасна система безпеки у хмарних середовищах має автоматизувати виявлення загроз та реагування на них. Для складних загроз потрібні нові сучасні рішення безпеки, які здатні прогнозувати, запобігати, виявляти загрози та реагувати на них за допомогою машинного навчання.
- Ешелонований захист: багаторівнева система безпеки по всьому технологічному стеку повинна включати засоби превентивного, детективного та адміністративного контролю за відповідними людьми, процесами та технологіями для забезпечення безпеки фізичних центрів обробки даних постачальників хмарних послуг.
- Керування обліковими записами: у міру того, як мобільні пристрої, програми та відомості про користувачів використовуються все ширше, облікові записи стають новим периметром. Найважливіше значення має контроль доступу та привілеїв у хмарі та локальних системах.

- Прозорість: брокер захисту доступу у хмару та рішення для управління засобами забезпечення безпеки у хмарі збільшують прозорість та контроль над усім хмарним середовищем організації.
- Постійна відповідність вимогам: відповідність нормативним вимогам є обов'язковою, але відповідність та безпека – це не те саме. Організації можуть порушити нормативні вимоги, не порушуючи при цьому безпеку, наприклад, внаслідок змін та помилок конфігурації. Для компаній дуже важливо мати рішення щодо управління хмарними середовищами, яке надає повні, своєчасні та дієві дані, пов'язані з дотриманням нормативних вимог, по всіх хмарних середовищах.
- Безпека за промовчанням: Постачальник хмарних послуг повинен активувати засоби контролю безпеки за умовчанням, а не вимагати від підприємства пам'ятати про те, що їх потрібно вмикати. Не всі мають чітке уявлення про різні засоби управління безпекою та про те, як вони працюють разом для зниження ризику та створення повноцінної системи безпеки. Наприклад, шифрування даних має бути увімкнено за замовчуванням. У хмарах повинні застосовуватись узгоджені засоби контролю та політики захисту даних.
- Моніторинг та міграція: для забезпечення безпеки робочих навантажень адміністраторам політик безпеки слід налаштувати та забезпечити дотримання політик безпеки для хмарних користувачів та секцій. Уніфікація подання всіх засобів контролю хмарної безпеки всім користувачам хмари також необхідно для виявлення помилок конфігурації ресурсів і небезпечних дій по всіх користувачах, що надає адміністраторам безпеки можливість відстежувати і вирішувати проблеми безпеки хмари.
- Поділ обов'язків та доступ до мінімальних привілеїв: принципи поділу обов'язків та доступу до мінімальних привілеїв – це практичні рекомендації з безпеки, які слід застосовувати у хмарних середовищах. Таким чином Ви зможете гарантувати, що окремі особи не матимуть надмірних

адміністративних прав і не зможуть отримати доступ до конфіденційних даних без додаткової авторизації.

Технічний аспект

При використанні хмарного сховища безпека є одним із головних питань забезпечення безперебійної роботи системи та захисту даних від несанкціонованого доступу. Хмарні провайдери зазвичай забезпечують високий рівень безпеки, використовуючи сучасні технології шифрування даних, мультифакторну автентифікацію та системи виявлення вторгнень.

Список заходів безпеки, які зазвичай застосовуються у хмарному хостингу:

- Резервне копіювання даних;
- Шифрування даних;
- Мультифакторна автентифікація;
- Системи виявлення вторгнень;
- Регулярні аудити безпеки;
- Обмеження прав доступу.

Хоча хмарні провайдери забезпечують високий рівень безпеки, є низка заходів, які потрібно вжити для забезпечення безпеки своїх серверів. По-перше, слід забезпечити захист паролів та облікових записів, використовуючи мультифакторну автентифікацію та складні паролі. По-друге, слід встановити та оновлювати антивірусне та антишпигунське програмне забезпечення. По-третє, слід регулярно перевіряти та оновлювати програмне забезпечення серверів та операційних систем.

Список заходів, які потрібно вжити для забезпечення безпеки своїх серверів:

- Використання мультифакторної аутентифікації та складних паролів;
- Встановлення та оновлення антивірусного та антишпигунського програмного забезпечення;

- Регулярне оновлення програмного забезпечення серверів та операційних систем;
- Регулярне створення резервних копій;
- Обмеження прав доступу до серверів;
- Проведення аудитів безпеки.

1.2.2 Основні загрози хмарних технологій

Малі та середні підприємства, як і глобальні компанії, все більше покладаються на послуги безпеки хмарних обчислень для підтримки повсякденних бізнес-функцій, розробки програмного забезпечення і навіть для забезпечення технологічної інфраструктури, необхідної для роботи.

Нижче наведено основні хмарні загрози:

Витік даних або несанкціонований доступ до даних. Все більше підприємств малого та середнього бізнесу розміщують у хмарі велику кількість даних, включаючи конфіденційні дані, які несуть інформацію, яка стосується транзакцій клієнтів. На відміну від даних, що зберігаються локально в корпоративних центрах обробки даних, дані у хмарі знаходяться за межами захисту брандмауера та вразливі до будь-яких загроз, з якими може зіткнутися постачальник хмарних послуг. Несанкціонований доступ до даних через недостатній контроль доступу або неправильне використання облікових даних співробітників може зробити важливі бізнес-дані відкритими для хакерів та інших зловмисників.

У нещодавньому звіті про основні загрози хмарних обчислень некомерційної організації Cloud Security Alliance (CSA), що займається просуванням передових методів забезпечення безпеки у хмарних обчисленнях та навчання використанню хмарних обчислень для забезпечення безпеки всіх інших форм обчислень. На думку CSA, негативні наслідки витоку даних можуть включати вплив на репутацію і довіру клієнтів або партнерів,

нормативні наслідки, які можуть призвести до грошових збитків, і вплив на бренд, який може викликати зниження ринкової вартості.

Неправильна конфігурація хмари. Ще однією поширеною проблемою, пов'язаною з хмарою, є неправильна конфігурація, яка впливає на безпеку. На базовому рівні це відбувається, коли адміністратор або користувач неправильно застосовує параметри безпеки для хмарної платформи. Це може містити такі проблеми, як неправильне обмеження доступу, неактивне шифрування даних, паролі за замовчуванням, неправильне керування дозволами.

Деякі неправильні налаштування можуть бути результатом внутрішніх загроз, включаючи ненавмисні помилки, недбалість або відсутність інформування користувачів про безпеку. Випадкові зміни налаштувань також можуть спричинити неправильну конфігурацію.

Спеціалісти CSA повідомили, що неправильна конфігурація хмарних ресурсів є однією з основних причин витоку даних і може призвести до видалення або зміни ресурсів та переривання обслуговування.

"Відсутність ефективного контролю змін є найпоширенішою причиною неправильної конфігурації у хмарному середовищі", – заявили в CSA. "Хмарні середовища та методології безпеки хмарних обчислень відрізняються від традиційних [IT], тим, що зміни складніше контролювати".

DDoS атаки. DDoS – ще одна поширена загроза, з якою стикаються організації під час використання хмарних послуг. У ході таких атак кіберзлочинець прагне зробити систему або мережевий ресурс недоступним для користувачів, порушуючи роботу вузла, підключеного до мережі.

Відмова в обслуговуванні зазвичай досягається шляхом заповнення машини або іншого ресурсу запитами у спробі перевантажити системи та завадити виконанню реальних запитів. При DDoS-атаках вхідний трафік, що викликає переповнення, надходить із кількох джерел. Враховуючи, що малі та середні підприємства дедалі більше ведуть бізнес в Інтернеті, такі атаки можуть спричинити серйозні проблеми та призвести до втрати бізнесу.

Злом акаунтів. Використовуючи злом облікових записів, зловмисники можуть отримати доступ до облікових записів користувачів хмарних сервісів. За даними CSA, найбільшим ризиком є облікові записи хмарних сервісів або підписки.

“Фішингові атаки, експлуатація хмарних систем або крадіжка облікових даних можуть скомпрометувати ці акаунти”, – йдеться у звіті організації. “Ці загрози – унікальні та потенційно потужні – можуть спричинити значні порушення у роботі хмарного середовища, такі як втрата даних та ресурсів, а також скомпрометовані операції”. За словами представників організації, наслідки таких атак іноді бувають дуже серйозними, а в недавніх випадках злому мали місце значні збої в операційній діяльності та бізнесі.

Серед способів, якими зловмисники можуть захопити облікові записи, – фішинг, коли користувачі викрадають інформацію під час відвідування незахищених веб-сайтів; кейлоггінг, коли програма записує натискання клавіш користувача та надсилає інформацію зловмисникам; і переповнення буфера, коли зловмисники перезаписують дані пам’яті іншими даними, що дає їм несанкціонований доступ.

Незахищені програмні інтерфейси програм (API). API можуть бути надзвичайно корисними для інтеграції різних хмарних платформ та інструментів, однак вони несуть у собі можливі ризики безпеки. Якщо API не захищені, зловмисники можуть використовувати вразливість та отримати доступ до конфіденційних даних.

Дослідницька компанія Gartner прогнозує, що у 2023 року атаки на API стануть найчастішим вектором атак, що призводить до витоку даних із корпоративних веб-додатків. За даними компанії, багато широко розрекламованих вразливостей у безпеці API вже торкнулися цілої низки організацій.

CSA, яка віднесла незахищені інтерфейси і API до основних хмарних загроз, зазначає, що постачальники хмарних послуг надають набір інтерфейсів

і API, які дозволяють клієнтам керувати хмарними послугами і взаємодіяти з ними. За даними CSA, безпека та доступність загальних хмарних сервісів залежить від безпеки цих API, а погано продумані API можуть призвести до зловживань або витоку даних.

1.2.3 Модель загроз хмарного кіберпростору

Сьогодні спостерігається великий інтерес до хмарних технологій та впровадження на їх основі середовищ хмарних обчислень, які вже існують і широко використовуються в технологічно розвинених країнах. Використання технологій хмарних обчислень дає низку переваг, основними з яких є: гнучкість, обчислювальна потужність, великий обсяг файлового сховища, різноманітне програмне забезпечення, постійний доступ до ресурсів у хмарі та швидке розгортання сервісів, можливість нарощування навантаження на хмару, простота масштабування, резервного копіювання та самовідновлення, можливість управління та моніторингу навантаження в режимі реального часу тощо.

Загроза – це динамічний і непередбачуваний процес, який часто виникає на інтерактивних вузлах між віртуальними машинами. Вся процедура захисту даних базується на конфіденційності, цілісності та доступності. Конфіденційність - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом.. У випадку хмарних обчислень дані зберігаються в центрах обробки даних, де безпека і конфіденційність даних є ще більш важливими.

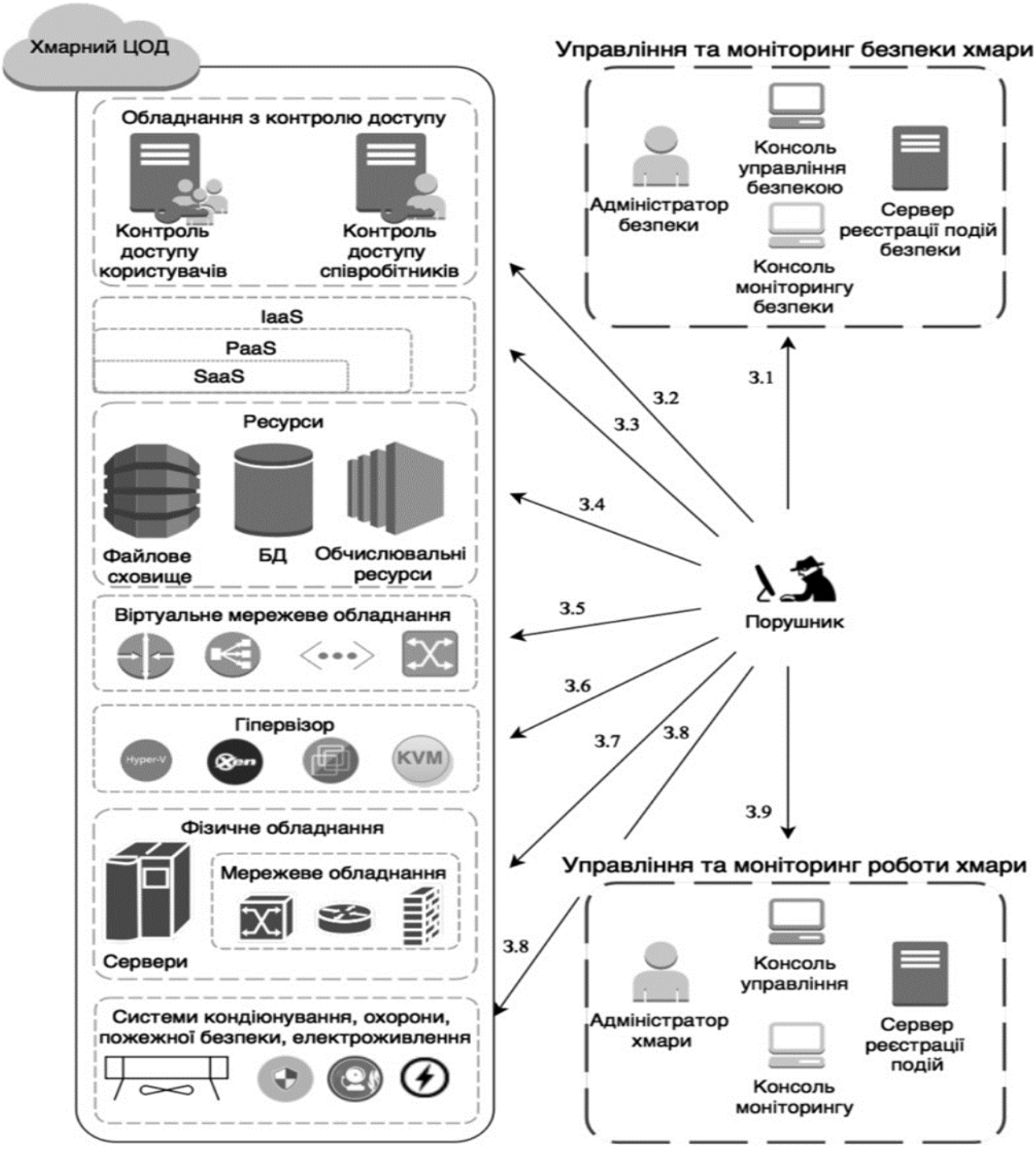


Рисунок 1.6 Модель загроз хмарного кіберпростору

Аналіз загроз показує, що найбільш ймовірними об'єктами атак є компоненти хмарної інфраструктури, які мають зовнішні інтерфейси доступу або розташовані у віртуалізованих середовищах.

Згідно аналізу моделі загроз, зображеної на Рисунку 1.6 , варто відзначити, що найбільш небезпечними є загрози управління хмарами (З.9) та її безпекою (З.1), а також загрози гіпервізору (З.6).

Ця модель базується на концепції інформаційного віртуального зв'язку, як способу опису мережевих взаємодій в середовищі хмарних обчислень. Для опису привілеїв суб'єкта використовується рольова модель, а привілеї ролі виражаються у вигляді правил фільтрації інформаційних сервісів для користувачів середовища хмарних обчислень. Обґрунтованість моделі підтверджується тим, що будь-яка мережева взаємодія в мережі TCP/IP може бути представлена у вигляді віртуального з'єднання, а також тим, що вона містить необхідні параметри для управління мережевими з'єднаннями відповідно до політики доступу.

На основі проведеного аналізу сучасного стану стандартизації та застосування хмарних сервісів, моделі хмарних обчислень та запропонованих ним порушень і загроз ІТС хмарних сервісів можна встановити, що найбільш проблемним питанням, яке потребує вирішення з точки зору забезпечення конфіденційності, цілісності, надійності, доступності сервісів тощо, є питання захисту ключів та ключової інформації. З цією метою на основі аналізу сучасного стану встановлено, що такі загрози, як компрометація, несанкціоноване знищення, перехоплення та зберігання, нав'язування слабкого ключа та несанкціоноване використання існують і можуть бути реалізовані в хмарному середовищі щодо ключових даних. Встановлено, що найбільшу небезпеку для ключових даних користувачів у середовищі хмарних обчислень становлять адміністратори хмарних сервісів, які мають доступ до середовища, в якому розгорнуті хмарні додатки користувачів.

Крім того, проведено детальний аналіз поточного стану та вимог до безпеки управління ключами з боку нормативних документів та стандартів, утому числі проектів, обґрунтовано механізми захисту особистих, та відкритих ключів користувачів від ідентифікованого комплексу загроз. Вони зводяться до використання низки технічних, організаційних та організаційно-технічних заходів та інструментів для досягнення високого рівня безпеки, тобто зменшення ймовірності загрози, в середовищі хмарних обчислень. Перелік

загроз, виявлених в результаті аналізу, та розроблена модель загроз для ключових даних дозволили зробити висновок, що хоча зловмисники потенційно можуть реалізувати багато з перелічених у підрозділі загроз, найбільша небезпека для ключових даних користувачів у середовищі хмарних обчислень виникає тоді, коли вони використовуються в межах наявної інфраструктури, без використання криптографічних сервісів.

1.2.4 Загрози хмарних обчислень та вимоги до їхньої безпеки

Центр обробки даних (ЦОД) (рис.1.7). є сукупністю серверів, розміщених на одному майданчику з метою підвищення ефективності та захищеності. Захист центрів обробки даних являє собою мережевий та фізичний захист, а також стійкість до відмов і надійне електроживлення. В даний час на ринку представлений широкий спектр рішень для захисту серверів та ЦОД від різних загроз. Їх поєднує орієнтованість на вузький спектр розв'язуваних завдань.

Рисунок 1.7 Центр обробки даних

Однак спектр цих завдань зазнав деякого розширення внаслідок поступового витіснення класичних апаратних систем віртуальними платформами. До відомих типів загроз (мережеві атаки, уразливості у додатках операційних систем, шкідливе програмне забезпечення) додалися складності, пов'язані з контролем середовища (гіпервізора), трафіку між гостьовими машинами та розмежуванням прав доступу.

Розширилися внутрішні питання та політики захисту ЦОД, вимоги зовнішніх регуляторів. Робота сучасних ЦОД у низці галузей потребує закриття технічних питань, і навіть питань пов'язані з їх безпекою. Фінансові інститути, наприклад банки, підпорядковані низці стандартів, виконання яких закладено лише на рівні технічних рішень. Проникнення платформ віртуалізації досягло того рівня, коли практично всі компанії, що використовують ці системи, дуже серйозно зайнялися питаннями посилення безпеки в них. Зазначимо, що буквально рік тому інтерес був скоріше теоретичний.

У сучасних умовах стає все складніше забезпечити захист критично важливих для бізнесу систем та додатків. Поява віртуалізації стала актуальною причиною масштабної міграції більшості систем на ВМ, однак вирішення завдань забезпечення безпеки, пов'язаних з експлуатацією додатків у новому середовищі, потребує особливого підходу. Багато типів загроз досить вивчені і для них розроблені засоби захисту, проте їх ще потрібно адаптувати для використання у хмарі.

Загрози хмарних обчислень:

Контроль та управління хмарами є проблемою безпеки. Гарантій, що всі ресурси хмари пораховані і немає неконтрольованих віртуальних машин, не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари немає. Це високорівневий тип небезпек, він пов'язаний з керованістю хмарою, як єдиною інформаційною системою і для неї загальний захист слід будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмарних інфраструктур.

В основі забезпечення фізичної безпеки лежить суворий контроль фізичного доступу до серверів та мережевої інфраструктури. На відміну від фізичної безпеки, мережна безпека в першу чергу являє собою побудову надійної моделі загроз, що включає захист від вторгнень і міжмережевий екран. Використання міжмережевого екрану передбачає роботу фільтра, щоб розмежувати внутрішні мережі ЦОД на підмережі з різним рівнем довіри. Це

можуть бути окремі сервери, доступні з Інтернету або сервери з внутрішніх мереж.

У хмарних обчислення найважливішу роль платформи виконує технологія віртуалізації. Для збереження цілісності даних та забезпечення захисту розглянемо основні відомі загрози для хмарних обчислень.

Проблеми при переміщенні звичайних серверів у обчислювальну хмару.

Вимоги до безпеки хмарних обчислень не відрізняються від вимог безпеки до центрів обробки даних. Однак, віртуалізація ЦОД та перехід до хмарних середовищ призводять до появи нових загроз. Доступ через Інтернет до управління обчислювальною потужністю є однією з ключових характеристик хмарних обчислень. У більшості традиційних ЦОД доступ інженерів до серверів контролюється фізично, у хмарних середовищах вони працюють через Інтернет. Розмежування контролю доступу та забезпечення прозорості змін на системному рівні є одним із головних критеріїв захисту.

Динамічність віртуальних машин. Віртуальні машини динамічні. Створити нову машину, зупинити її роботу, запустити знову можна зробити за короткий час. Вони клонуються та можуть бути переміщені між фізичними серверами. Ця мінливість важко впливає розробку цілісності системи безпеки. Однак, уразливість операційної системи або додатків у віртуальному середовищі поширюються безконтрольно і часто виявляються після довільного проміжку часу (наприклад, при відновленні з резервної копії). У хмарних обчисленнях важливо надійно зафіксувати стан захисту системи, при цьому це не повинно залежати від її стану та розташування.

Вразливості віртуального середовища. Сервери хмарних обчислень і локальні сервери використовують ті самі операційні системи та програми. Для хмарних систем загроза віддаленого злому або зараження шкідливим програмним забезпеченням висока. Ризик для віртуальних систем також високий. Паралельні віртуальні машини збільшує поверхню, що «атакується». Система виявлення та запобігання вторгненням повинна бути здатна виявляти

шкідливу активність на рівні віртуальних машин, незалежно від їх розташування у хмарному середовищі.

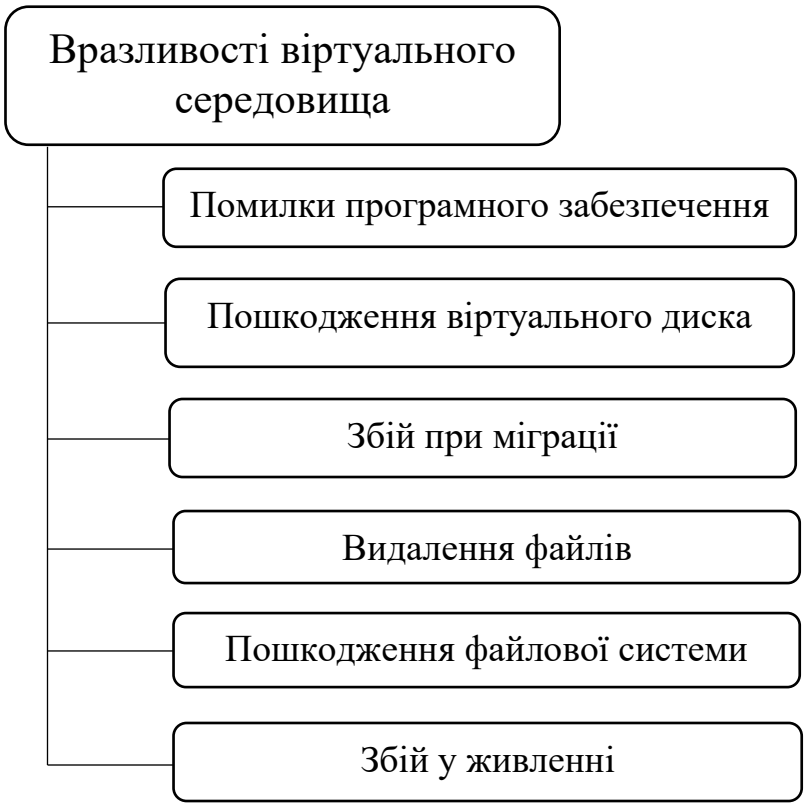


Рисунок 1.8 Вразливості віртуального середовища

Віртуальні машини мають безліч вразливостей (рис1.8), які часто призводять до пошкодження критичних даних або їх втрати:

- Помилки програмного забезпечення. Програмне забезпечення для віртуалізації також може мати внутрішні недоліки, через які воно може несподівано вийти з ладу, що призведе до втрати існуючих файлів;
- Пошкодження віртуального диска. Віртуальні диски, як і інші комп'ютерні файли, схильні до пошкоджень, які можуть бути спричинені атаками шкідливих програм, збоями програмного забезпечення або плином часу;
- Збій при міграції. Збій під час міграції віртуальних машин можуть бути спричинені різними факторами, включаючи збій в мережі та раптове

відключення пристроїв зберігання даних під час перенесення віртуальних дисків, що може призвести до пошкодження файлів віртуальних машин;

- Видалення файлів. Випадкове видалення файлів конфігурації віртуальної машини або файлів віртуальних дисків може статися через помилку користувача або адміністратора, а більшість гіпервізорів не мають вбудованих засобів відновлення;
- Пошкодження файлової системи. Якщо файлова система віртуального диска або хоста, на якому розташована віртуальна машина, пошкоджена, її файли неможливо прочитати стандартними засобами;
- Збій у живленні. Збій живлення зазвичай призводить до примусового вимкнення системи, що не тільки пошкоджує основне обладнання, але й може пошкодити віртуальні машини, які були активні.

Захист бездіяльних віртуальних машин. Коли віртуальна машина вимкнена, вона наражається на небезпеку зараження. Доступу до сховища образів віртуальних машин через мережу достатньо. На вимкненій віртуальній машині неможливо запустити захисне програмне забезпечення. У цьому випадку повинна бути реалізована захист не тільки всередині кожної віртуальної машини, але і на рівні гіпервізора.

Захист периметра та розмежування мережі.

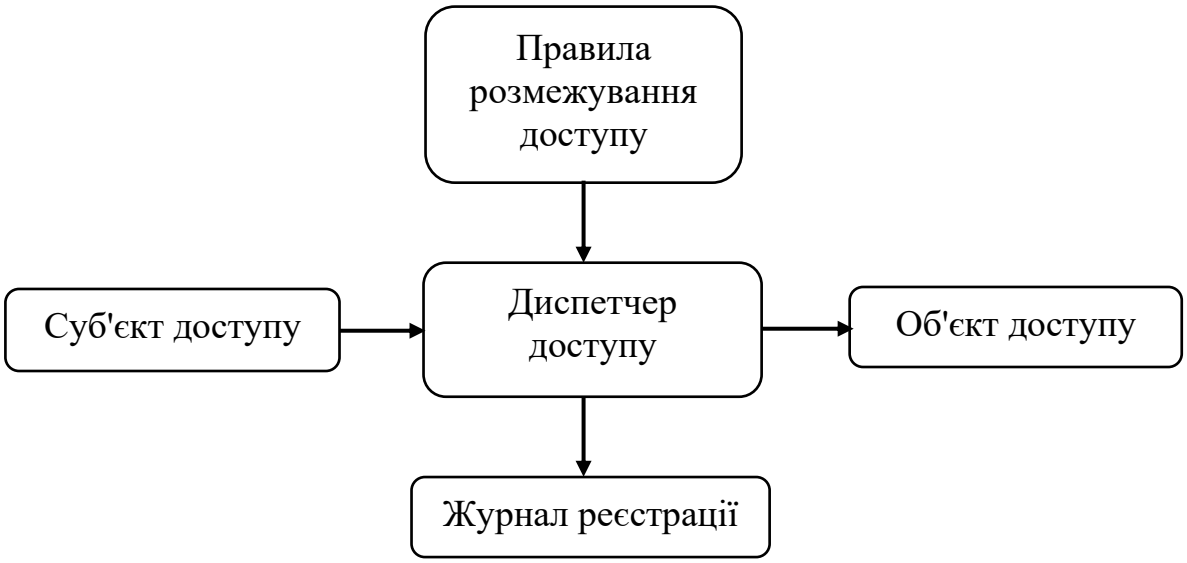


Рисунок 1.9 Схема роботи механізму розмежування доступу

У разі використання хмарних обчислень периметр мережі розмивається або зникає. Це призводить до того, що захист менш захищеної частини мережі визначає загальний рівень захищеності. Для розмежування сегментів з різними рівнями довіри у хмарі віртуальні машини повинні забезпечувати себе захистом, переміщуючи мережевий периметр до самої віртуальної машини (рис 1.9). Корпоративний firewall — основний компонент для впровадження політики IT безпеки та розмежування сегментів мережі, що не в змозі вплинути на сервери, розміщені у хмарних середовищах.

Атаки на хмари та рішення щодо їх усунення:

Традиційні атаки на ПЗ. Вразливості операційних систем, модульних компонентів, мережевих протоколів та ін. — традиційні загрози, для захисту від яких достатньо встановити міжмережевий екран, firewall, антивірус, IPS та інші компоненти, що вирішують цю проблему. При цьому важливо, щоб ці засоби захисту ефективно працювали в умовах віртуалізації.

Функціональні атаки на елементи хмари. Цей тип атак пов'язаний із багатошаровістю хмари, загальним принципом безпеки. У статті про небезпеку хмар було запропоновано наступне рішення: Для захисту від функціональних атак для кожної частини хмари необхідно використовувати такі засоби захисту: для проксі – ефективний захист від DoS-атак, для веб-сервера – контроль цілісності сторінок, для сервера додатків – екран рівня додатків, для СУБД — захист від SQL-ін'єкцій, системи зберігання даних – правильні бекапи (резервне копіювання), розмежування доступу. Окремо кожні з цих захисних механізмів вже створені, але вони не зібрані разом для комплексного захисту хмари, тому завдання інтеграції їх у єдину систему потрібно вирішувати під час створення хмари.

Атаки на клієнта. Більшість користувачів підключаються до хмари за допомогою браузера. Тут розглядаються такі атаки, як Cross Site Scripting, «викрадення» паролів, перехоплення веб-сесій, «людина посередині» та багато інших. Єдиний захист від цього виду атак є правильна автентифікація та

використання шифрованого з'єднання (SSL) із взаємною автентифікацією. Однак, дані засоби захисту не дуже зручні та дуже марнотратні для творців хмар. У цій галузі інформаційної безпеки є ще багато невирішених завдань.

Атаки на гіпервізор. Гіпервізор - це процес, який відокремлює операційну систему та програми комп'ютера від його апаратного забезпечення. Гіпервізори впроваджують концепцію віртуалізації, дозволяючи фізичному хост-комп'ютеру керувати великою кількістю гостьових віртуальних машин. Це гарантує, що обчислювальні ресурси, такі як пам'ять, пропускна здатність мережі та процесорні цикли, використовуються максимально ефективно.

Хоча гіпервізори вважаються безпечним варіантом, це не означає, що гіпервізори вільні від проблем безпеки. Наприклад, теоретично хакери можуть створити шкідливе програмне забезпечення, яке встановлюється як гіпервізор під операційною системою. Цей процес відомий як "гіперджекінг" і його складніше виявити. Це пов'язано з тим, що такі шкідливі програми можуть перехоплювати операції операційної системи (наприклад, введення пароля), а оскільки шкідливий код працює в операційній системі, антивірус не програмне забезпечення може не знати про це.

Гіпервізор є одним із ключових елементів віртуальної системи. Основною його функцією є розподіл ресурсів між віртуальними машинами. Захист гіпервізора необхідний, коли є ризик отримання несанкціонованого доступу до гіпервізора, що управляє віртуальним середовищем (що дає зловмиснику потенційний доступ до всіх даних, що зберігаються на кожній віртуальній машині), або вразливі загальні апаратні кеші, мережа і потенційний доступ до фізичного сервера. Атака на гіпервізор може призвести до того, що одна віртуальна машина зможе отримати доступ до пам'яті та ресурсів іншої. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витіснити віртуальну машину із сервера. Як стандартні методи захисту рекомендується застосовувати спеціалізовані продукти для віртуальних середовищ, інтеграцію хост-серверів зі службою каталогу Active Directory,

використання політик складності та старіння паролів, а також стандартизацію процедур доступу до керуючих засобів хост-сервера, застосовувати вбудований брандмауер віртуалізації. Також можливе відключення таких служб, що часто не використовуються, як, наприклад, веб-доступ до сервера віртуалізації.

Вирішення проблем безпеки гіпервізора пов'язане із забезпеченням його захисту протягом усього життєвого циклу, включаючи розробку та впровадження. Для цього є кілька методів – введення обмежень користувачів у локальній системі; скорочення поверхонь атаки шляхом запуску гіпервізорів на виділеному хості, який не виконує жодних додаткових ролей; оновлення систем за рахунок дотримання передових методів керування виправленнями; налаштування хоста для роботи як частини захищеної мережі.

Крім того, можна застосувати:

- шифрування віртуальних машин для запобігання доступу до ВМ зловмисників;
- шифрування сховища, де знаходяться віртуальні машини, за допомогою BitLocker або іншої аналогічної системи;
- використання управління доступом на основі ролей (RBAC) для обмеження адміністративних прав;
- використання виділеного фізичного мережевого адаптера для керування трафіком;
- використання виділеного фізичного мережевого адаптера для трафіку міграції віртуальних машин;
- використання виділеного фізичного мережевого адаптера кластерного трафіку.

Атаки на системи управління. Велика кількість віртуальних машин, що використовуються в хмарах, потребує наявність систем управління, здатних надійно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в систему управління може призвести до появи віртуальних

машин - невидимок, здатних блокувати одні віртуальні машини та підставляти інші.

1.3 Методи боротьби з загрозами кібербезпеці хмарних сервісів

1.3.1 Аналіз проблем захисту хмарного кіберпростору

14 квітня 2022 року стало відомо, що команда дослідників Palo Alto Unit 42 дійшла висновку, що хмарні користувачі, ролі, служби та ресурси надають надмірні дозволи, наражаючи організації на ризик компрометації. За словами експертів, неправильно налаштоване управління ідентифікацією та доступом (IAM) відчиняє двері для зловмисників, націлених на хмарну інфраструктуру та облікові дані.

Дослідники Unit 42 проаналізували понад 680 тис. посвідчень у 18 тис. хмарних облікових записах та більш ніж 200 різних організаціях з метою зрозуміти їх конфігурації та моделі використання. Як виявилося, 99% хмарних користувачів, ролей, сервісів та ресурсів надали «надмірні дозволи», які не використовувалися протягом 60 днів. Хакери можуть використовувати такі дозволи для переміщення по мережі жертви та розширення радіусу атаки.

Невикористовуваних чи надмірних дозволів у вбудованих політиках безпеки контенту (CSP) було вдвічі більше, ніж у політиках, створених клієнтами. Видалення цих дозволів може значно знизити ризик, який наражається на кожен хмарний ресурс, і звести до мінімуму поверхню атаки для всього хмарного середовища.

Неправильні налаштування, за твердженням компанії, є причиною 65% виявлених кіберинцидентів у хмарі, тоді як 53% проаналізованих хмарних облікових записів використовували ненадійний пароль, а 44% повторно

використовували паролі. Понад те, майже дві третини (62%) організацій мають загальнодоступні хмарні ресурси.

Команда Unit 42 виявила та ідентифікувала п'ять кіберзлочинних угруповань, які використовують незвичайні методи для безпосереднього нападу на платформи хмарних сервісів:

- TeamTNT - одне з досить небезпечних загроз з погляду методів підрахунку хмарних ідентифікаторів. Операції угруповання включають переміщення всередині кластерів Kubernetes, створення ботнетів IRC та захоплення скомпрометованих ресурсів хмарного робочого навантаження для майнінгу криптовалюти Monero.
- WatchDog - використовує спеціально створені скрипти мовою Go, а також перепрофільовані скрипти криптоджекінгу від інших угруповань (включаючи TeamTNT) і є загрозою, націленою на відкриті хмарні екземпляри та програми.
- Kinsing – угруповання, націлене на збір хмарних облікових даних, відкриті API-інтерфейси Docker Daemon з використанням шкідливих процесів на основі GoLang у контейнерах Ubuntu.
- Rocke - спеціалізується на операціях з програмами-вимагачами та криптоджекінгом у хмарних середовищах і відома тим, що використовує обчислювальну потужність скомпрометованих систем на базі Linux, які зазвичай розміщені в хмарній інфраструктурі.
- 8220 - угруповання використовує інструменти PwnRig або DBUsed, які є варіантами програмного забезпечення для майнінгу XMRig Monero.

Компанія Varonis, один із представників світового ринку безпеки та аналітики даних, 2 вересня 2021 року поділилася результатами звіту про ризики SaaS за 2021 рік. У звіті розглянуто основні тенденції та проблеми, з якими стикаються компанії при спробі контролювати цифрові особи користувачів та тіньові привілеї, а також ризики корпоративних даних у крос-хмарній інфраструктурі.

Аналітики Varonis проаналізували дані понад 200 000 цифрових осіб та сотні мільйонів хмарних активів за допомогою рішення DatAdvantage Cloud. ПЗ Varonis DatAdvantage консолідує інформацію про користувачів, дані та події доступу, отриману зі служб каталогів та файлових серверів. Зібрана інформація піддається ретельному аналізу, який виявляє докладну картину використання даних, а також визначає правильну модель доступу, що відповідає бізнес-логіці компанії.

З'ясувалося, що 43% усіх хмарних облікових записів застаріли, не використовуються та наражаються на ризик. При цьому облікові записи користувачів, які більше не використовують хмарні сервіси, стають легкою мішенню та суттєво збільшують поверхню атаки на організацію.

Також три із чотирьох хмарних облікових записів зовнішніх підрядників залишаються активними навіть після припинення співпраці з організацією. Одна з чотирьох «особистостей» у SaaS-додатках та половина в IaaS-сервісах є машинними. На відміну від живих людей, вони піддаються загрозі злому цілодобово, оскільки завжди перебувають у системі і зазвичай ігноруються службами безпеки через роботу у фоновому режимі.

44% привілеїв користувачів хмарних сервісів налаштовані некоректно - це може зробити організацію вразливою для злому облікових записів або ексфільтрації даних. Також три із п'яти привілейованих користувачів хмарних сервісів є тіньовими адміністраторами. Вони можуть вносити зміни на рівні адміністратора та потенційно завдати шкоди хмарному сервісу.

Аналітики з'ясували, що 15% співробітників переносять критично важливі для компанії дані до своїх особистих хмарних облікових записів. У кращому разі це означає, що дані знаходяться поза контролем служби безпеки, у гіршому — свідчить про крадіжку даних. А 16% усіх користувачів хмарних сервісів виконують привілейовані дії і 20% мають доступ до конфіденційних корпоративних даних. Все це може негативно вплинути на роботу хмарного сервісу або на більшість його користувачів.

Завдяки хмарі зникли межі між особистими та корпоративними обліковими записами. Навіть рядові користувачі, які не є адміністраторами, легко порушують принципи найменших привілеїв одним натисканням кнопки "поділитися". Якщо ви не контролюєте весь стек SaaS/IaaS у вашій організації, користувачі можуть мовчки копіювати, видаляти або розкривати критично важливі дані практично будь-кому. Це може бути ваш список клієнтів Salesforce, вихідний код на GitHub, документи в Box та Google Drive.

Щоб убезпечити роботу у хмарах, компанія Varonis підготувала чек-лист правил безпеки. Експерти радять відкривати співробітникам мінімальний доступ, необхідний для виконання їхніх службових обов'язків, перевіряти активність користувачів щодо підозрілих або непередбачених політиками безпеки дій та усувати тіньові облікові записи.

На думку фахівців Varonis, зберігати дані в безпеці допоможуть регулярна перевірка прав доступу, використання крос-хмарних інструментів виявлення загроз, періодичний аудит налаштувань конфігурації загального доступу до хмари, а також гігієна облікових записів дистанційних співробітників та підрядників.

1.3.2 Забезпечення кібербезпеки хмарних сервісів

Тема захисту хмарної інфраструктури наразі є дуже актуальною. Це, безсумнівно, пов'язано з поширенням хмарних платформ і рішень, які приваблюють клієнтів легким горизонтальним масштабуванням, прозорими планами витрат і можливістю передати частину робіт з обслуговування інфраструктури хмарному провайдеру. Крім того, останнім часом на вітчизняний ринок хмарної інфраструктури вийшла низка відомих компаній, які пропонують хмарні рішення та сервіси для обробки персональних даних, функціонування в складі ГІС (державної інформаційної системи) та обробки конфіденційної інформації, захищеної від несанкціонованого доступу. Хоча ці

пропозиції зробили хмарні сервіси доступними для державних організацій, доступність хмарної інфраструктури все ще залишається під питанням для багатьох компаній. Серед основних проблем - дотримання законодавства, конфіденційність інформації про компанію як для постачальників послуг, так і для "сусідів" по інфраструктурі, складність міграції з локальної інфраструктури, а також делікатність налаштування хмарних систем кібербезпеки.

В контексті інформаційної безпеки можна виділити такі терміни:

1. SECaaS (security as a service, «безпека як сервіс») - надання клієнтам послуг з кібербезпеки на основі підписки шляхом розміщення самих засобів захисту в хмарі провайдера, включаючи системи резервного копіювання, сканери вразливостей, системи автентифікації та контролю доступу, а також рішення для збору та аналізу подій безпеки.

Безпека як послуга (SECaaS) дозволяє компаніям передавати управління кібербезпекою на аутсорсинг як вимогу до послуги. Аутсорсингові рішення для захисту даних включають антивірусний захист, виявлення вторгнень і запобігання втраті даних. Крім того, підприємства можуть отримати вигоду з досвіду та інновацій відданої кібербезпеки команди обслуговування. Який спеціалізується на запобіганні порушенням безпеки як послуги серед хмарних обчислень, працюючи з постачальником SECaaS.

Безпека як послуга усуває необхідність локальної доставки рішень для захисту даних. При цьому наш IT-відділ встановлює антивірусне програмне забезпечення, програмне забезпечення для фільтрації спаму та інші рішення для захисту даних на кожному комп'ютері. Або підтримувати програму в актуальному стані або інструктувати їх використовувати її в системі захисту мережі або на сервері у нашому офісі.

Традиційний метод також дорогий. Ми повинні сплатити авансові платежі за обладнання та поточні ліцензійні збори для використання програми.

Однак використання тих самих технологій тільки з веб-браузером тепер стало простим і доступним завдяки безпеці як послуги.

Так само, як це роблять компанії, що надають програмне забезпечення як послугу (SaaS), служба безпеки як постачальник послуг часто стягує щомісячну абонентську плату для оплати витрат на аутсорсингові послуги. Однак вони забезпечують безпеку наших хмарних програм, даних та операцій, а не надають нам доступ до інструменту або платформи. Розглянемо переваги безпеки як послуги (рис.1.10).

Рисунок 1.10 Переваги безпеки як послуги

1) Гнучкість та швидше виділення ресурсів

Можливість негайно надати нашим користувачам доступ до цих інструментів – один із найкращих аспектів рішень «як послуга». Крім того, рішення SECaaS доступні на запит, де і коли вони нам потрібні, і можуть масштабуватися в міру необхідності. Це означає, що більше немає двозначності щодо розгортання або оновлень, оскільки наш постачальник SECaaS зробить все за нас і зробить все це очевидним через веб-панель керування.

2) Поліпшена видимість

Наш бізнес може бачити, що весь його трафік, використовувані програми та будь-які зламані пристрої IoT, загрози та порушення політики зупинені. І багато іншого в режимі реального часу завдяки хмарній безпеці як

послузі. Інтегроване хмарне рішення пропонує централізоване представлення всіх дій у службах кібербезпеки, включаючи брандмауер, пісочницю, безпечний веб-шлюз, розширений захист від загроз, запобігання втраті даних, контроль смуги пропускання та багато іншого. Це нагадує систему управління інформацією та подіями безпеки (SIEM).

3) Менше вразливості

Зловмисники все більше уваги приділяють мобільним користувачам та використовують мобільні пристрої як плацдарм для атак на бізнес-системи. Оскільки зловмисники сьогодні знають, що застаріла система безпеки у центрі обробки даних не може захистити цих користувачів. Якщо ми не можемо захистити кожне посилання, захист нашої мережі наражається на ризик. Діри в корпоративній безпеці, створені користувачами поза мережею та людьми, які безпосередньо підключаються до хмарних програм та загальнодоступного Інтернету, заповнюються мережевою безпекою як послугою.

4) Визволення ресурсів

Наші IT-команди можуть зосередитись на тому, що критично важливо для нашої компанії, коли забезпеченням безпеки керують ззовні. SECaaS вивільняє ресурси та забезпечує повну прозорість за допомогою панелей керування. Група аутсорсингових експертів з безпеки вправно керує нашою IT-безпекою, гарантуючи нам її ефективне керування.

Ми також можемо делегувати керування процедурами безпеки свого IT-персоналу. Ми можемо надати своїм IT-фахівцям можливість контролювати процеси безпеки та керувати всіма змінами політики та системи через веб-інтерфейс.

5) Економія витрат

Здатність фірми економити гроші одна із основних переваг підходу «цінний папір як послуга». Хмарна служба часто пропонується на рівні підписки з різними можливостями оновлення. Це дозволяє фірмі платити за те, що їй потрібно зараз. Крім того, експертиза є необов'язковою.

6) Доступ до фахівців з безпеки

Коли ми використовуємо SECaaS, ми отримуємо досвідчених, кваліфікованих експертів з безпеки замість нашої внутрішньої команди, яка може потребувати більш спеціалізованих знань або бути перевантаженою іншими завданнями та нездатною приділити необхідну увагу кібербезпеці.

Проблеми безпеки в хмарі є для всіх рішень безпеки. При використанні аутсорсингового рішення для забезпечення безпеки необхідно враховувати декілька таких питань, як такі: усунення застарілого обладнання за допомогою міграції, ризик неправильної конфігурації, підзвітність.

2. FWaaS (firewall as a service, «фаервол як сервіс») - надання міжмережевого екрану в хмарній інфраструктурі за передплатою. FWaaS - це хмарна система безпеки, яка також надає брандмауер нового покоління, що гіпермасштабується. Служба брандмауера – це пропозиція преміум-акаунту, яка використовує брандмауер для захисту мережі компанії від атак. Іноді краще створити власну безпекову інфраструктуру.

FWaaS знаходиться між нашим пристроєм та Інтернетом, (Рис.1.11). Система FWaaS перевіряє трафік, коли він намагається увійти до нашої системи, щоб виявляти та усувати ризики. Інспекція перевіряє дані, що містяться в заголовку кожного пакета, отримуючи уявлення про те, звідки було відправлено пакет, а також про інші дії, які можуть вказувати на його зловмисність.

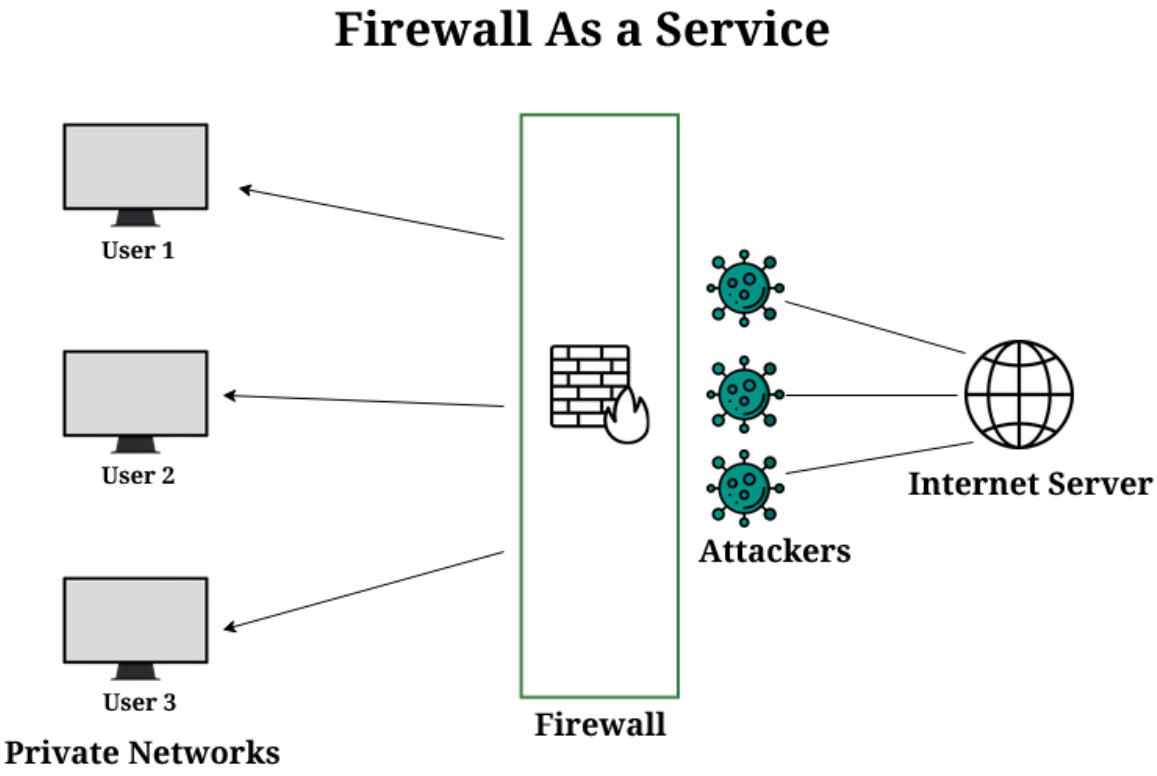


Рисунок 1.11 Фаервол як сервіс

Робота брандмауера як послуги (FWaaS):

- Брандмауер як рішення фільтрує мережну активність, щоб захистити бізнес як від внутрішніх, так і зовнішніх загроз.
- На додаток до функцій брандмауера з відстеженням стану він включає фільтрацію пакетів, мережну безпеку, протокол управління передачею/інтернет-шифрування, рівні сокетів безпеки, що забезпечують сумісність з VPN і зіставлення IP-протоколу.
- FWaaS також включає більш глибокі можливості аналізу контенту, такі як здатність виявляти атаки шкідливих програм, кібератаки та інші віруси.
- Деякі варіанти FWaaS включають NGFW (брандмауер нового покоління) для живлення системи. Ви також можете отримати технології машинного навчання з NGFW, які можуть виявляти інноваційні атаки нульового дня, яких раніше не було.
- Це досягається шляхом оцінки поведінки цифрових даних та перевірки на наявність ненормальної та потенційно небезпечної активності.

Переваги:

Для компаній, які шукають гнучке рішення для забезпечення безпеки, FWaaS пропонує багато суттєвих переваг. Щоб зберегти гнучкість, багато підприємств відмовляються від традиційного внутрішнього вибору і довіряють безпеку мережі постачальнику FWaaS.

Ось список переваг FWaas:

- Простіше розгортання та обслуговування. Впровадження нового локального засобу захисту від шкідливих програм або просто окремого продукту безпеки може вимагати значних зусиль та ресурсів. Все, що нам потрібно зробити з FWaaS, це повідомити службу про те, що нам потрібно. У них вже є ресурси, і їхня команда може впоратися з усіма проблемами конфігурації.
- Підвищена масштабованість. Розширити систему FWaaS неважко. Нам потрібно лише уточнити нові вимоги у нашого провайдера. Однак вони можуть порадити нам покладатися на цілі нашої компанії. Крім того, при масштабуванні за допомогою FWaaS досить просто повернутися до попереднього налаштування, якщо нове рішення виявиться зайвим або надмірним.
- Підвищена адаптивність: ми можемо визначити, коли та де розгортати безпеку за допомогою FWaaS залежно від процедур та ресурсів, які ми бажаємо захистити. Ми також можемо вибрати, де наші засоби захисту повинні бути розміщені у хмарному інформаційному ланцюжку. FWaaS також можна використовувати для захисту баз даних, програмного забезпечення або CRM-систем. Ми також можемо змінити налаштування кожної опції на свій розсуд.

Недоліки:

- Міжмережні екрани вимагають значних витрат, залежно від типу. Апаратні брандмауери значно дорожчі за програмні брандмауери. Крім того,

апаратні брандмауери вимагають встановлення та управління, що може бути дорогим.

- Брандмауер, однак, має кілька обмежень, таких як його нездатність зупинити атаки вірусів та шкідливих програм, для яких знадобилися б додаткові програми на рівні окремих машин. Для обслуговування та модернізації брандмауера потрібні додаткові сили та ресурси.

3. MaaS (malware as a service, «шкідливе ПЗ як сервіс») -термін, придуманий зловмисниками для позначення того, що одні зловмисники розробляють шкідливі інструменти і надають доступ до них за підпискою іншим зловмисникам, які потім використовують їх у своїх атаках. Наприклад, якщо використовується вірус-здирник, цей метод називається "програма-вимагач як послуга"(RaaS).

Програма-виконавець як послуга (RaaS) — це бізнес-модель свого роду, яка імітує концепцію «Програмне забезпечення як послуга (SaaS)». Це дозволяє афільованим особам надати хакерам та іншим кіберпреступникам готові інструменти, що виконують сценарії програм-виконавців. Партнери, які розробляють скрипт програми-виконавця і встановлюють його в програмне забезпечення, отримують якийсь відсоток від суми викупу. Згідно зі статтею Bank Info Security, в кінці 2019 року кількість випадків програм-вимагачів зросла до 33%, серед яких афілійовані особи отримували в середньому 80% виплат викупу.

Для забезпечення кібербезпеки в різних хмарних інфраструктурах на ринку пропонуються спеціалізовані рішення:

1. CASB (cloud access security broker) - брокери безпеки хмарного доступу, що забезпечують ІБ в хмарі за допомогою аутентифікації користувачів (в т.ч. мультифакторній), контролю за наданням доступу до даних, логування дій, надання звітності, а також шляхом контролю програмного API-доступу з боку додатків і сервісів.

Рішення CASB забезпечують додатковий рівень захисту для співробітників компанії, які отримують доступ до хмарних програм.

Програмне забезпечення також забезпечує дотримання політик безпеки та діє як шлюз між співробітниками та хмарними сервісами. Це дозволяє організаціям розширити локальні засоби керування безпекою за межі своєї локальної мережі чи інфраструктури.

На практиці типовим рішенням CASB є хмарне або локальне програмне забезпечення, яке знаходиться між користувачем хмарної програми та постачальником хмарних послуг. Звідси рішення захищає хмарні програми, користувачів та дані, застосовуючи політики безпеки бізнесу.

Сьогодні все більше і більше організацій покладаються на хмарні програми через економію коштів, зручність та підтримку розподіленої робочої сили. На жаль, доступ до хмарних програм пов'язаний з цілою низкою загроз безпеці.

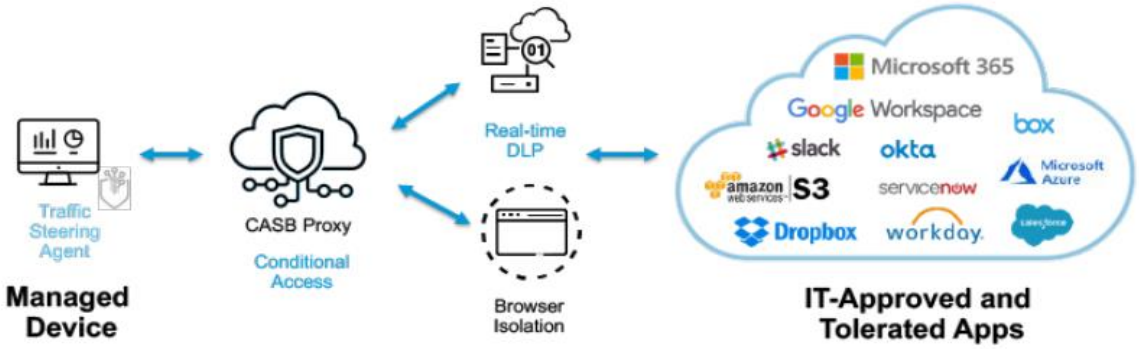


Рисунок 1.12 Захист хмарних додатків за допомогою CASB

Як правило, традиційний захист периметра, що забезпечує локальний захист, не підходить для хмарних додатків, тому виникає необхідність додаткового захисту, наприклад, той, який пропонують рішення брокера безпеки доступу до хмари.

Зазвичай роль рішення CASB полягає у виявленні загроз безпеки та порушень нормативних вимог щоразу, коли користувачі та пристрої отримують доступ до хмарних програм та даних. Крім зниження ризиків безпеки,

програмне забезпечення CASB також відстежуватиме системи на предмет будь-якої незвичайної поведінки та дій. При виявленні будь-яких відхилень інструменти мають в ідеалі реагувати та попереджати адміністраторів.

Інструменти CASB дозволяють організаціям:

- Підвищити безпеку затверджених користувачів та хмарних програм. Це також допомагає виявляти несанкціоновані хмарні служби, несанкціонований доступ та підозрілі дії.
- Відстежувати та керувати діями користувачів, керованими та некерованими пристроями.
- Отримувати уявлення про стан безпеки організації та ризики відповідності.
- Розширення можливостей виявлення загроз та реагування на них для хмарних служб.
- Захистіть користувачів хмарних сервісів, дані та хмарні програми.

2. CSPM (cloud security posture management) - системи управління станом хмарної безпеки, що допомагають проаналізувати кіберризики на основі даних про налаштування хмарної інфраструктури, які проводять оцінку відповідності поточних налаштувань хмарних систем вимогам законодавства і рекомендацій вендорів, що допомагають візуалізувати стан ІБ в Cloud-інфраструктурі.

CSPM забезпечує організаціям кращу видимість їх хмарних середовищ та покращує їхнє управління та виявлення ризиків та загроз. Він виявляє такі проблеми, як відсутність шифрування, неправильне керування ключами шифрування та додаткові дозволи облікового запису.

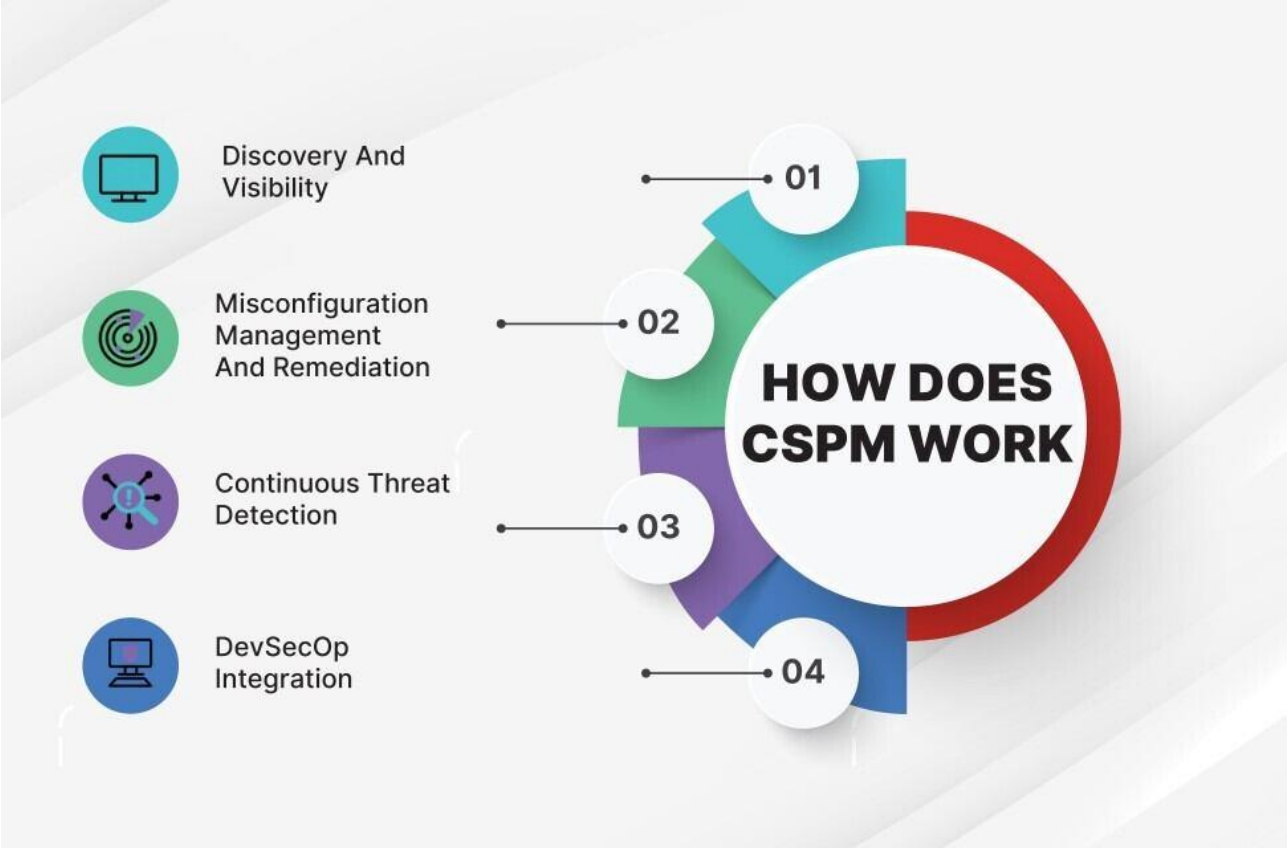


Рисунок 1.13 Принцип роботи CSPM.

CSPM працює за допомогою таких підходів:

1) Виявлення та видимість: CSPM забезпечує видимість хмарних активів та конфігурацій. Він встановлює єдине джерело достовірної інформації для всіх хмарних середовищ, що гарантує, що організації можуть автоматично виявляти дії, пов'язані з метаданими, неправильними конфігураціями, змінами мережі та безпеки. Він також дозволяє керувати політиками безпеки для облікових записів, проектів, регіонів та віртуальних мереж за допомогою єдиної консолі.

2) Керування неправильною конфігурацією та виправлення: важлива роль, яку відіграє CSPM, полягає у усуненні та усуненні ризиків безпеки у хмарі. Це досягається шляхом порівняння змін хмарних додатків з еталонними показниками галузі та організації, що дозволяє швидко виявляти та усувати порушення. Це допомагає організаціям виявляти проблеми, такі як неправильні конфігурації, відкриті порти та несанкціоновані модифікації, які можуть

призвести до вразливості хмарних ресурсів та знижує ймовірність дорогих помилок розробників. CSPM також відстежує місця зберігання даних, перевіряє наявність відповідних рівнів дозволів та гарантує, що всі екземпляри бази даних, що відповідають за резервне копіювання, шифрування та високу доступність, включені.

3) Безперервне виявлення загроз: CSPM використовує цілеспрямований підхід до виявлення загроз та управління ними, що дозволяє організаціям завчасно виявляти потенційні загрози. Він фокусується на областях, на які зловмисники, швидше за все, націляться, що скорочує кількість попереджень, встановлює пріоритети вразливостей на основі хмарного середовища та запобігає попаданню вразливого коду на виробничу стадію. CSPM також постійно відстежує хмарні середовища на наявність потенційно шкідливих дій та подій несанкціонованого доступу через виявлення загроз у реальному часі.

4) Інтеграція DevSecOps: CSPM знижує накладні витрати організацій та усуває складності та тертя, пов'язані з керуванням багатохмарними обліковими записами та постачальниками. Він забезпечує хмарний та безагентний процес управління станом, який забезпечує централізований контроль та прозорість усіх хмарних ресурсів. Це дає спеціалістам DevOps та службам безпеки єдине уявлення, що дозволяє їм запобігти переміщенню скомпрометованих активів протягом життєвого циклу їхніх програм. Організації також можуть інтегрувати CSPM зі своїм інструментом управління інформацією та подіями безпеки (SIEM), який забезпечує додаткову інформацію та більшу видимість порушень політик та неправильних конфігурацій. Крім того, інтеграція наборів інструментів DevOps з CSPM забезпечує швидке виправлення та реагування.

Переваги CSPM: виявлення неправильно настроєного мережного підключення, оцінка ризику даних, виявлення надмірно ліберальних дозволів облікового запису, безперервний моніторинг хмарного середовища, автоматичне виправлення неправильних конфігурацій у деяких випадках.

3. CWPP (cloud workload protection platform) - хмарні системи захисту сервісів, які здійснюють контроль налаштувань розміщених в хмарі елементів (серверів, контейнерів, додатків), аналіз їх вразливостей, сегментацію на мережевому рівні, контроль активності, усунення загроз.

CWPP – це високорозподілений інструмент безпеки, який захищає всі робочі навантаження, забезпечуючи чітке уявлення про локальні та хмарні середовища. Більшість компаній використовують рішення CWPP для захисту своїх програм, контейнерів, мережевих ресурсів, фізичних серверів, віртуальних машин (ВМ) та безсерверних робочих навантажень.

4. SASE (secure access service edge) - прикордонні сервіси безпечного доступу, що надають користувачам зручний і безпечний доступ до корпоративних хмарних ресурсів з використанням засобів мультифакторної аутентифікації, з перевіркою пристрою, який подключається, на відповідність вимогам компанії (т.зв. «posturing»), із застосуванням функціоналу систем виявлення/запобігання вторгнень і контролем мережевого трафіку.

1.3.3 Результати аналізу сфери хмарної кібербезпеки

Хмарні обчислення комерційно доступні вже 20 років і застосовуються практично повсюдно: близько 95% компаній зазначають, що вони мають хмарну стратегію. Хоча постачальники хмарних послуг значно вдосконалили свої системи безпеки, користування такими сервісами досі пов'язані з ризиками. На щастя, ці ризики можна знизити до мінімуму за допомогою наведених нижче передових практик:

- Слід визначити, яка інформація є найбільш вразливою. Хоча повсюдне впровадження захисту найвищого рівня, звичайно, буде зайвим, компанії мають убезпечити свої конфіденційні дані — інакше вони наражаються на ризик втрати інтелектуальної власності та накладення нормативних штрафів. Тому перш за все необхідно визначити, яка саме

інформація підлягає захисту. Для виявлення та класифікації даних зазвичай використовують спеціальний механізм. Необхідно встановити комплексне рішення, яке зможе виявити та захистити конфіденційну інформацію у вашій мережі, на кінцевих пристроях та у хмарі, і при цьому забезпечить необхідний рівень гнучкості та мобільності для вашої організації.

- Доступ до даних та їх зберігання. Незважаючи на те, що конфіденційні дані можна зберігати у хмарі, така можливість не є чимось очевидним. За даними звіту McAfee за 2022 р. «Про впровадження хмари та ризики» (Cloud Adoption and Risk Report), 37% усіх файлів у хмарі містять конфіденційну інформацію. Експерти відзначають зростання цього показника, порівняно з минулим роком. Хоча більша частина цієї інформації зберігається в корпоративних хмарних сервісах типу Box, Salesforce і Office365, що добре зарекомендували себе, важливо розуміти, що жодне з цих рішень не гарантує 100% безпеки. Зважаючи на це, важливо вивчити дозволи та контекст доступу до даних у нашому хмарному середовищі та внести необхідні коригування. У деяких випадках доведеться видалити конфіденційні дані, які вже розміщені в хмарі, або помістити їх у карантин.

- Обмін конфіденційними даними. Порівняно з попереднім роком, обсяги обміну конфіденційними даними збільшилися більш ніж на 50%. Якою б продуманою не була наша стратегія зниження загроз, не можна лише реагувати на інциденти: ризики такого підходу занадто великі. Необхідно розробити політику контролю доступу та забезпечити її застосування ще до потрапляння даних у хмару. Можливість редагувати документи має бути лише у невеликої кількості співробітників, більшості буде достатньо їх перегляду. Аналогічно, не всім користувачам, які мають доступ до певних даних, слід дати дозвіл на обмін ними. Необхідно створити групи та налаштувати права, щоб пересилати таку інформацію могло лише вузьке коло осіб із відповідними повноваженнями. Це суттєво обмежить поширення конфіденційних даних.

- Шифрування хмарного сервісу. Комплексне шифрування на рівні файлів має бути основою всіх заходів щодо забезпечення безпеки у хмарі. Хоча шифрування даних постачальниками хмарних послуг захищає їх від третіх сторін, у провайдерів з'являється доступ до ключів шифрування. Для максимального захисту компаніям необхідно впровадити сучасні криптографічні рішення із власними ключами та застосовувати їх до завантаження даних у хмару.

1.3.3.1 Усунення внутрішніх загроз хмарної безпеки

Використання хмари співробітниками.

Навіть якщо в нашій організації діє корпоративна стратегія хмарної безпеки, наші співробітники можуть користуватися хмарою на власний розсуд. Більшість людей заводять облікові записи або використовують онлайн-сервіси для конвертації файлів без попередньої консультації з фахівцями IT. Щоб оцінити потенційні ризики роботи співробітників зі хмарою, слід перевірити журнали проксі-сервера, брандмауера та системи управління інформацією про безпеку та події безпеки (SIEM). Це дозволить отримати повне уявлення про те, які хмарні сервіси використовуються, та визначити їхню цінність для співробітників/організації в порівнянні з ризиками повного або часткового розгортання систем у хмарі. Також слід пам'ятати, що тіньове використання - це не тільки доступ до нових або недозволених сервісів з кінцевих кінцевих пристроїв. Компаніям також потрібна стратегія боротьби з переміщенням даних із довірених хмарних рішень на неконтрольовані ними смартфони, планшети та ноутбуки. Оскільки в хмарний сервіс можна зайти з будь-якого підключеного до Інтернету пристрою, неконтрольована особиста техніка створює пробіл у будь-якій безпеці. Щоб обмежити завантаження файлів на несанкціоновані пристрої, можна зробити перевірку безпеки обов'язковою попередньою умовою такого завантаження.

Важливість ролі кінцевих пристроїв.

Більшість користувачів застосовують для доступу до хмари веб-браузер, тому компаніям необхідно впровадити ефективні інструменти для захисту клієнтської сторони та забезпечити своєчасне оновлення браузерів, щоб запобігти експлуатації їх вразливостей. Це є ключовими компонентами хмарної безпеки. Для повноцінного захисту пристроїв кінцевих користувачів необхідно встановити сучасні спеціалізовані рішення, наприклад, брандмауери, особливо якщо наша компанія працює за моделлю IaaS або PaaS.

Захист від необережних користувачів та зловмисників.

Серед загроз безпеки, з якими компанії стикаються щомісяця, з вини персоналу трапляються в середньому 15 інцидентів. У 95% організацій внутрішньосистемні небезпеки з'являються як мінімум раз на місяць. Вони неминучі: питання лише тому, коли ця проблема торкнеться нас. Загрози такого роду включають як ненавмисне розкриття (тобто, скажімо, випадкове пересилання документа з конфіденційними відомостями), так і власне шкідливу активність — наприклад, коли менеджер з продажу скачує повну версію клієнтської бази перед відходом до конкурентів. І необережні співробітники, і зломщики можуть чинити дії, що вказують на зловмисне використання хмарних даних. Для відстеження аномальних явищ і запобігання внутрішнім та зовнішнім витокам даних, слід використовувати рішення з технологіями машинного навчання та аналізу поведінки користувачів.

1.3.4 Аналіз ринку інструментів захисту хмарних середовищ

Глобальна галузь засобів захисту хмарних середовищ (SSE) у 2022 році зросла у грошовому вираженні приблизно на $1 млрд, або на 38% порівняно з попереднім роком. Таку оцінку зробила компанія Dell'Oro Group, яка оприлюднила результати дослідження 15 березня 2023 року.

Інструменти SSE (Security Service Edge) є частиною мережевої моделі SASE (Secure Access Service Edge) – прикордонного сервісу безпечного

доступу. Це комбінація технологій SWG (засоби захисту на рівні шлюзів), CASB (брокер безпечного доступу в хмару), FWaaS (хмарний брандмауер) та ZTNA (рішення для мережного доступу з нульовою довірою), а також мережевих технологій SD-WAN (програмно-визначені глобальні мережі) та VPN (віртуальна приватна мережа). Фактично SASE - це набір нових і раніше використовуваних рішень. Ця платформа надає захисні засоби користувачеві, пристрої або вузлу граничних обчислень.

Аналітики Dell'Oro Group кажуть, що пандемія COVID-19 підвищила потребу у хмарних програмах на тлі розвитку концепцій віддаленої роботи та дистанційного навчання. А тому компанії та організації стали активніше впроваджувати кошти SSE. На світовому ринку такі рішення пропонують понад 20 постачальників. У трійку провідних гравців входять Cisco, Broadcom/Symantec та Zscaler: 2022-го вони отримали приблизно 58% від загального розміру виручки. У сегменті брандмауерів різного типу витрати показали зростання на двозначні числа відсотків: найбільший попит мали рішення Cisco, Fortinet і Palo Alto Networks.

Якщо розглядати ринок SASE в цілому, то, за даними Dell'Oro Group, його обсяг у 2022 році перевищив $6 млрд. Зростання по відношенню до 2021-го склало приблизно 34%. У трійку найбільших постачальників за розміром виручки увійшли Cisco, Zscaler та Broadcom/Symantec: разом вони контролювали трохи більше 40% галузі. При цьому Cisco припала на частку 17%, тоді як Zscaler відстала менш ніж на 1%.

Комплекти SASE від одного постачальника за підсумками 2022-го займали 45% від загальних поставок: найбільш популярними виявилися продукти Cisco, Fortinet і Palo Alto Networks. До трійки найбільших постачальників уніфікованих SASE по виручці увійшли Versa Networks, VMware та Cato Networks.

У мережевому сегменті SD-WAN виторг у 2022 році зріс на 30% порівняно з попереднім роком. До трійки найбільших гравців у цій сфері за

обсягом виручки увійшли Cisco, Fortinet та VMware – разом вони зайняли майже половину ринку. З технологічного погляду рішення SSE за підсумками 2022-го зайняли майже 60% глобального ринку SASE у плані доходу. Ще 40% припало на платформи SD-WAN.

Зазначається, що у зв'язку з цифровою трансформацією бізнесу, збільшенням кількості віддалених робочих місць та використанням хмарних сервісів все більш важливим стає забезпечення безпеки у хмарі, а тому попит на SASE-продукти швидко зростає. Такі рішення забезпечують ефективний захист як усередині, так і поза традиційним периметром мережі.

2 ОХОРОНА ПРАЦІ

Згідно з ч. 1 ст. 13 Закону України «Про охорону праці» роботодавець зобов'язаний створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ЕОМ. Велике значення має раціональна конструкція і розташовує елементів робочого місця, що важливе для підтримки оптимальної робочої пози людини-оператора. В процесі роботи з комп'ютером необхідно дотримувати правильний режим праці і відпочинку.

Дотримання норм охорони праці є спільним завданням як роботодавця, так і працівника. У вирішенні питань з охорони праці можна звернутися до законодавства України з охорони праці.

Метою данного розділу дипломного проекту є визначення оптимальних умов праці програміста та обов`язків з охорони праці.

1.Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу

На робочому місці розробника програмного забезпечення: підвищений рівень отримуваного електромагнітного випромінювання, статична електрика, високий рівень шуму, несприятливі умови мікроклімату, підвищена напруга на зір та мозок тощо.

Під час робочого процесу програміст піддається впливу великої кількості шкідливих та небезпечних факторів, а саме: шуми, вібрації, інфрачервоне випромінювання, електромагнітне випромінювання, електричний струм, емоційне та нервове навантаження, сидяче положення тіла протягом

дового часу. Тому дуже важливо забезпечити правильний нормований графік та організувати робочий процес так, щоб мінімізувати вплив усіх перелічених раніше небезпечних та шкідливих факторів.

2 Гігієнічні вимоги до виробничого середовища.

Вимоги, що пред'являються до умов праці на виробництві, визначаються необхідністю забезпечення таких умов праці на робочому місці, при яких виключено несприятливий вплив на працездатність і здоров'я працюючих і можуть бути забезпечені оптимальні границі поділу і кооперації праці, а в кінцевому підсумку підвищення ефективності та якості праці.

2.1 Вимоги до приміщення

Обємно-планувальні рішення будівель та приміщень для роботи з ВДТ мають відповідати вимогам ДСанПІН 3.3.2.007-98. Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше 6,0 $м^2$, а об’єм – не менше ніж 20,0 $м^3$. У приміщеннях слід щоденно робити вологе прибирання. Вони повинні бути оснащені аптечками першої медичної допомоги. При приміщеннях мають бути обладнанні побутові приміщення для відпочинку.

Для стін і робочих поверхонь використовують мало насичені (основні) кольори, для невеликих помешкань або ділянок, що рідко потрапляють у поле зору працюючих, а також для створення контрастності – кольори середньої насиченості (допоміжні), для маленьких по площі поверхонь – насичені (акценти) – як функціональне фарбування. Стелі у всіх приміщеннях повинні бути білими. Поверхні устаткування в приміщеннях повинні бути матовими або напівматовими для виключення випадку відблисків світла в очі працюючого, а стіни бути пофарбованими фарбами пастельних тонів.

2.2 Освітлення

Відповідність характеристик систем освітлення нормативним вимогам гарантує не тільки збереження здоров'я, а й високі продуктивність і якість

праці. На підприємствах використовується природне і штучне освітлення. Перше призначено для роботи в денний час, а друге - у вечірній, коли природного освітлення недостатньо. Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення, відповідно до ДБН В.2.5-28:2018 « Природне і штучне освітлення».

Для штучного освітлення у приміщенні використовуються люмінесцентні лампи типу ЛБ, які в порівнянні з лампами розжарювання мають ряд істотних переваг: за спектральним складом світла вони близькі до природного світла, мають підвищену світлову віддачу (у 2-5 разів вищу, ніж у ламп розжарювання); мають триваліший термін служби – до 10 тис годин.. Допускається застосування ламп розжарювання у світильниках місцевого освітлення.

2.3 Шум

Рівні шуму та вібрації на робочих місцях осіб, що працюють з ПК, визначаються відповідно до ДСанПіН 3.3.2.007-98.

Для забезпечення дотримання допустимих рівнів шуму на робочих місцях застосовуються засоби звукопоглинання, вибір яких обґрунтовується спеціальними інженерно-акустичними розрахунками (п. 3.3.3 ДСанПіН 3.3.2.007-98).

2.4 Мікроклімат

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря – ДСН 3.3.6.042-99 «і норми мікроклімату виробничих приміщень».

Параметри мікроклімату	значення параметрі	
	Взимку	влітку
Температура, C^0	22-24	23-25
Відносна вологість, %	40-60	40-60
Швидкість руху повітря, м/с	0,1	0,1-0,2

Нормалізація параметрів мікроклімату у виробничих приміщеннях здійснюється за допомогою систем опалення. Ці системи поділяються на водяні парові та повітряні. Кількість теплоти, що генерується системою опалення, має відповідати втрат теплоти в приміщенні (через будівельні конструкції, на нагрів повітря в приміщенні, технологічні тепловтрати, нагрів надходять матеріалів і напівфабрикатів). Основними засобами захисту від теплових випромінювань є екранування та теплоізоляція, а також пристрій місцевих припливних систем вентиляції. При природній вентиляції (за допомогою вікон) повітря надходить у приміщення і видаляється з нього внаслідок різниці температур і тиску.. Механічна вентиляція забезпечується вентиляторами, що забирають повітря зовні і направляє його до будь-якого робочого місця. або устаткування, а також видаляють забруднене повітря

2.4 Вимоги до організації робочого місця працівника

До самостійної роботи на комп'ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочому місці один раз на півріччя, періодичні медичні огляди один раз на два роки

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео термінала, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.

Робочий стіл повинен регулюватися по висоті в границях 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля Рекомендовані розміри столу: висота 725 мм, ширина 600-1400 мм, глибина 800-1000 мм. Робочий стілець повинен бути оснащений підйомно-поворотним пристроєм для регулювання висоти сидіння і спинки, а також кута її нахилу. Регулювання кожного параметра повинне вироблятися легко, бути незалежним і надійно фіксуватися.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом $+30^0$ до нормальної лінії погляду працюючого.

Клавіатуру слід розташовувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого.

3 Пожежна безпека

Під пожежною безпекою розуміють систему державних і суспільних заходів, спрямованих на охорону від вогню людей і власності. Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки (негорючі речовини й матеріали в холодному стані).

 Куріння у не відведених для цього місцях	 Порушення правил користування електроприладами	 Необережне поводження з вогнем

Всі приміщення повинні бути забезпечені первинними засобами пожежогасіння: пожежним водопостачанням (пожежні крани ПК), пожежні щити з набором пожежного інструменту, вуглекислотними або порошковими вогнегасниками. У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефону 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації і приступити до ліквідації пожежі.

ВИСНОВКИ

Завданням дослідження в галузі хмарних технологій був аналіз існуючих сучасних хмарних сервісів. Досліджено та проаналізовано існуючі методи безпеки в хмарних сервісах з точки зору компонентів технології, можливих загроз та способів протидії атакам. Запропоновано найбільш підходящі сервіси відповідно до потреб користувача. Також були розглянуті переваги та недоліки використання хмарних технологій і типи послуг, що пропонуються хмарними сервісами. Завдяки історичним даним та ключовим факторам розвитку, доповненим кількісними значеннями, було виявлено стабільний розвиток та зростання ринку хмарних сервісів, що підтверджує обґрунтованість проведеної роботи. Для того, щоб зрозуміти функціональність технології, було представлено послуги, які пропонуються користувачам, та визначено класифікацію хмарних сервісів.

У другій частині були досліджені загрози та можливі атаки на кожен компонент хмарних сервісів, щоб повністю зрозуміти небезпеки, з якими стикаються користувачі хмарних сервісів. На основі цих загроз представлено новітні методи захисту вразливостей кожного компонента хмарних сервісів, щоб запобігти будь-яким небажаним наслідкам, таким як втрата даних користувачів, перехоплення повідомлень або недоступність сервісів з різних причин. Визначено те що, необхідно в першу чергу ретельно захистити сервер управління, приділивши особливу увагу автентифікації та правам доступу, що може бути ефективно досягнуто шляхом використання додаткового програмного забезпечення, спеціально розробленого для віртуальної інфраструктури. Доступ до хмарних серверів повинен здійснюватися за захищеними протоколами, а адміністративний доступ повинен бути обмежений за IP-адресою. Також важливо логічно і фізично відокремити середовище управління віртуальною інфраструктурою від виробничого середовища віртуальних машин, щоб запобігти несанкціонованому втручанню.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 17788 – 2014. Information technology – Cloud computing – Overview and vocabulary. – Publ. 2014-10-15. – Geneva: ISO, 2014. – 10 p.
2. NIST Special Publication 800-39, Managing Information Security Risk. Organization, Mission, and Information System View. Information security. – 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
3. ПРО ЗАТВЕРДЖЕННЯ Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України від 29.03.2006 р. № 373 // Законодавчі та нормативні документи України у сфері інформації, видавничої та бібліотечної справи: темат. Добірка. - К., 2007. - Ч.1. - С.74-77.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
5. Закон України «Про захист персональних даних»;
6. Закон України «Про доступ до публічної інформації»;
7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Постанова Кабінету Міністрів України від 29.03.06 № 373);
8. Концепція технічного захисту інформації в Україні (Постанова Кабінету Міністрів України від 8.10.97 №1126);
9. Положення про технічний захист інформації в Україні (Указ Президента України від 27.09.99 № 1229/99).
10. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: http://www.uk.xlibx.com/4yuridicheskie/1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php.

11. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплек- сної системи захисту інформації в інформаційно-телекомунікаційній системі”. [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

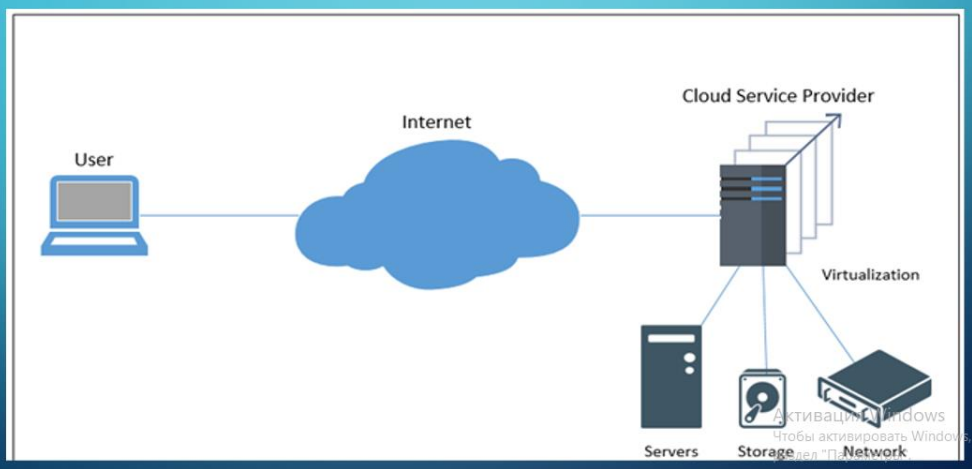
12. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с

ДОДАТОК Б

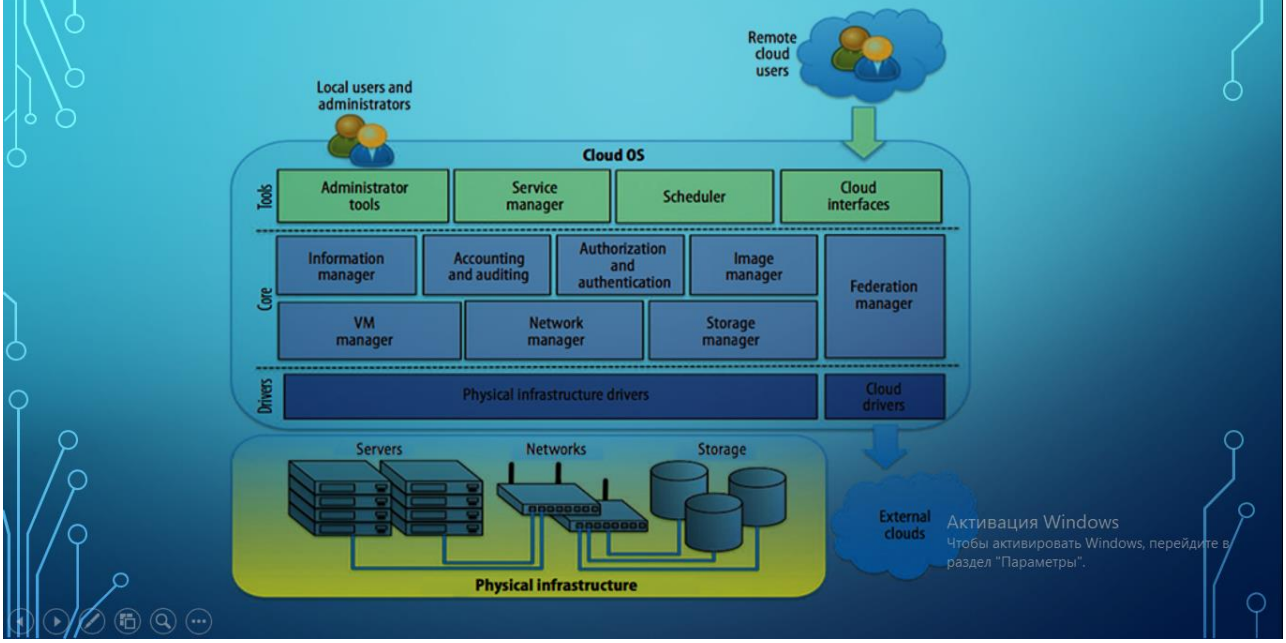
Слайди мультимедійної презентації

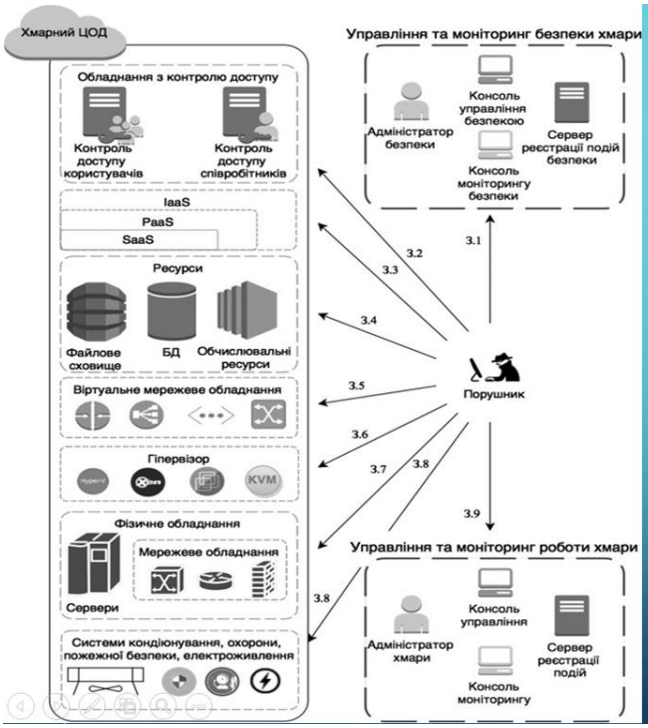
Моделі хмарних служб

ПРИКЛАД ІНФРАСТРУКТУРИ IAAS

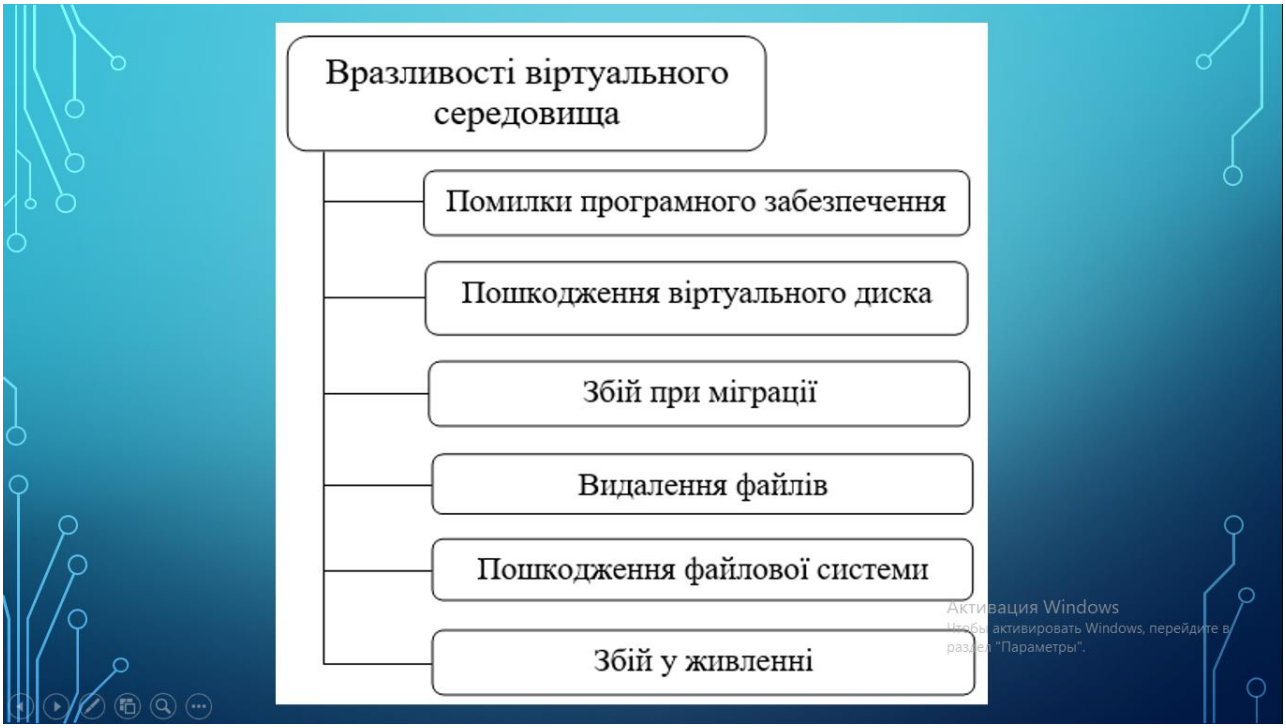


АРХИТЕКТУРА IAAS ОБЛАКА



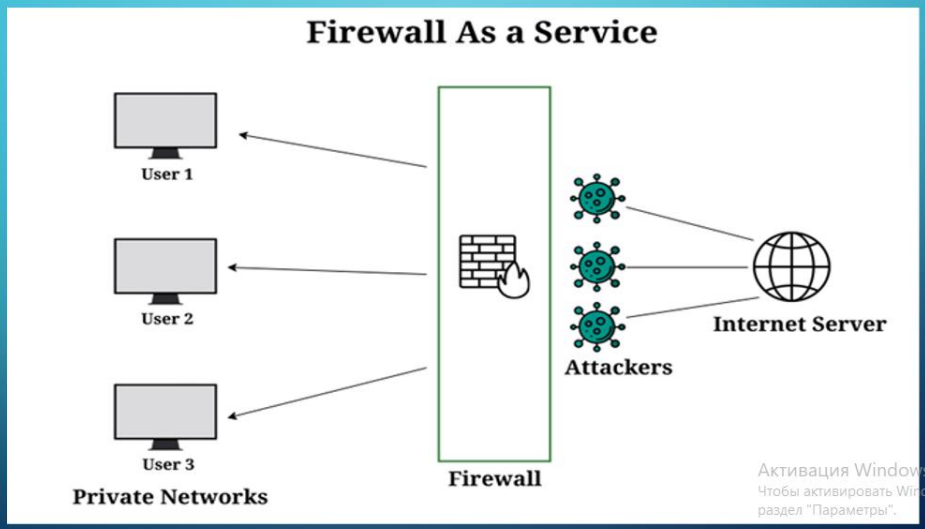


Модель загроз хмарного кіберпростору

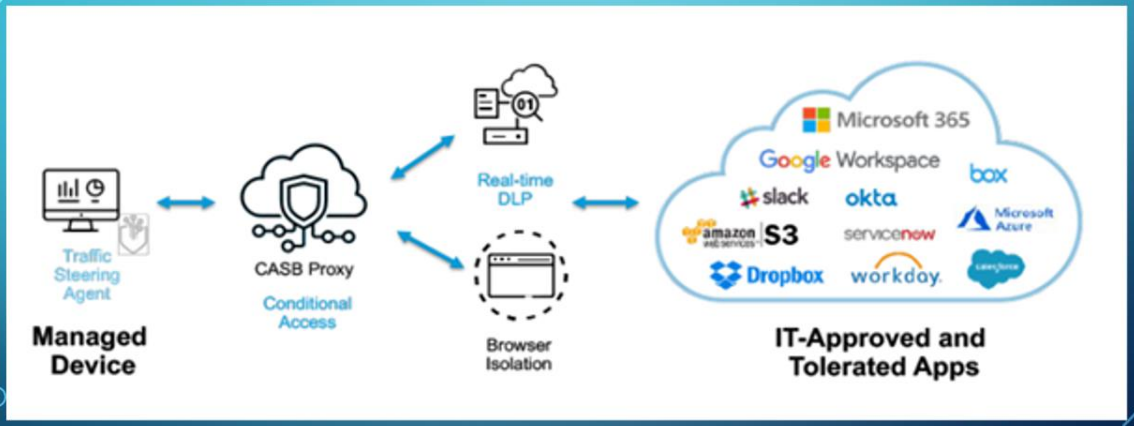


ПЕРЕВАГИ БЕЗПЕКИ ЯК ПОСЛУГИ

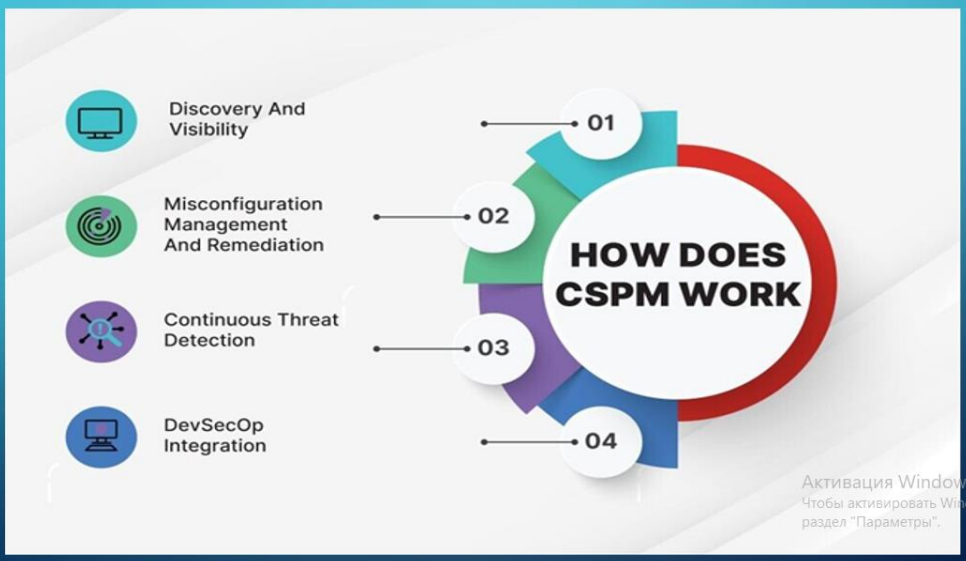
ФАЕРВОЛ ЯК СЕРВІС



ЗАХИСТ ХМАРНИХ ДОДАТКІВ ЗА ДОПОМОГОЮ CASB



ПРИНЦИП РОБОТИ CSPM



UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015582966

Дата перевірки:
13.06.2023 12:41:11 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.06.2023 12:42:57 EEST

ID користувача:
100011688

Назва документа: 2БКС-27 Студзінський Д.С.

Кількість сторінок: 55 Кількість слів: 10830 Кількість символів: 84486 Розмір файлу: 1.23 MB ID файлу: 1015232689

24.4%
Схожість

Найбільша схожість: 6.43% з Інтернет-джерелом (https://softico.ua/uk/news/top-hmarnih-zagroz-z-yakimi-neobhidno-b...

24.4% Джерела з Інтернету | 437 ..... Сторінка 57

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 69

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Студзінський Дмитро Сергійович,
здобувач освіти гр. 4ФКГ-06, та

Харченко Роман Юрійович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз загроз кібербезпеці хмарних сервісів та методів боротьби з ними»

(автор роботи – Студзінський Д.С., керівник роботи – Харченко Р.Ю.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Студзінський Д.С./

Керівник _____ / Харченко Р.Ю./

« 12 » _____06_____ 2023 р.

ВСП «Одеський технічний фаховий коледж ОНТУ»

ВІДГУК

керівника про випускну роботу бакалавра

Студзінського Дмитра Сергійовича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Тема випускної роботи Аналіз загроз кібербезпеці хмарних сервісів та методів боротьби з ними

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки) Випускна робота виконана відповідно технічному завданню. Пояснювальна записка до випускної роботи містить 72 сторінки. У пояснювальній записці проведено аналіз загроз кібербезпеки хмарних сервісів та методів боротьби з ними. Розглянуті моделі кібербезпеки. Графічна частина складається з 14 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра, розробку виконано у повному обсязі.

б) Самостійність роботи

Протягом виконання випускної бакалаврської роботи Студзінський Д.С. поступово та послідовно виконував всі етапи, проявив ініціативу у створенні загальної концепції та реалізації випускної роботи. Всі роботи він виконував самостійно, з оглядом на рекомендації керівника.

в) Теоретична підготовка здобувача освіти

Студзінський Д.С. під час роботи над випускною бакалаврською роботою вивчив достатню кількість літературних джерел за даною тематикою.

Вважаю, що теоретична підготовка здобувача освіти добра і він готовий до захисту роботи.

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва

Під час виконання роботи Студзінський Д.С. мав змогу самостійно приймати окремі рішення з виконання програмної частини роботи та показав вміння організовано працювати над поставленою задачею, користуючись сучасними комп'ютерними програмними засобами.

Оцінка розрахункової частини

Оцінка графічної частини Добре

Загальна оцінка Добре

Прізвище, ім`я, по батькові *Добре*

Харченко Роман Юрійович к.т.н.

Місце роботи і посада керівника роботи

доцент каф. "Морського радіозв'язку" НУ «Одеська Морська академія»

Підпис

«12» серпня 2023р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на випускну роботу бакалавра здобувача освіти
відділення комп'ютерних систем

Студзінського Дмитра Сергійовича

(прізвище, ім`я та по батькові)

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **Обслуговування комп'ютерних систем та мереж**

Керівник дипломного проекту (роботи) **Шевцов Юрій Сергійович**

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи)

Аналіз загроз кібербезпеці хмарних сервісів та методів боротьби з ними

Обсяг розрахунково-пояснювальної записки 74 сторінок

Обсяг графічної (презентаційної) частини 14 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Дипломний проект повністю відповідає завданню до дипломного проектування. Графічна частина складається з окремих слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра.

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Пояснювальна записка дипломного проекту виконана якісно, у повному обсязі. В дипломному проекті здобувачем проаналізовано загрози кібербезпеки хмарних сервісів та методів боротьби з ними. Розглянуті технічні та програмні методи боротьби з загрозами. В дипломному проекті в останніх розділах проаналізовано економічні показники та питання охорони праці.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) _____

Презентаційні матеріали виконані якісно, демонстративно та відповідають вмісту теоретичного матеріалу

г) перелік позитивних якостей дипломного проекту (роботи)_____

Здобувачем проаналізовані загрози кібербезпеки хмарних сервісів та методів боротьби з ними, що є дуже актуальною тематикою в наш час. Розглянуті технічні та програмні методи боротьби з загрозами і ефективність їх застосування.

д) основні недоліки дипломного проекту (роботи) _____

Серед недоліків роботи варто вказати, відсутність посилань на перелік використаних джерел та наявність орфографічних помилок в тексті пояснювальної записки

Оцінка розрахункової частини *4 (добре)*

Оцінка графічної частини *5 (відмінно)*

Загальна оцінка *4 (добре)*

Прізвище, ім'я, по батькові рецензента *Василіу Євген Вікторович*

Місце роботи і посада рецензента *Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки*

Підпис: _____

« 16 » червня 2023 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ ДУІТЗ

ВІДДІЛ КАДРІВ