УДК 681.518.54

Кириченко О.А., студент гр. 125-22-2
Науковий керівник: Олішевський І.Г., асистент;
(Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна)

ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ПРИ ХМАРНИХ ОБЧИСЛЕННЯХ

Хмарні обчислення (англ. cloud computing) — це модель забезпечення повсюдного та зручного мережевого доступу на вимогу до загального пулу конфігуруємих обчислювальних ресурсів (наприклад, мереж передачі даних, серверів, пристроїв зберігання даних, додатків і сервісів - як разом, так і окремо), які можуть бути оперативно надані і звільнені з мінімальними експлуатаційними витратами і / або зверненнями до провайдера.

Переваги:	**Недоліки:**
не потрібні великі обчислювальні потужності ПК - по суті будь-який смартфон, планшет і т.д., при відкритті вікна браузера отримує величезний потенціал	хмарні послуги надаються якоюсь компанією, тому збереження даних користувача залежить від цієї компанії
висока швидкість обробки даних	необхідність бути завжди в мережі
економія на покупці софта – всі необхідні програми вже є в сервісі, де будуть працювати додатки	небезпека хакерських атак на сервери
всі дані зберігаються в мережі	можлива подальша монетизація ресурсу

Таблиця 1 – Порівняння переваг та недоліків хмарних обчислень

Основні характеристики хмарних обчислень

- **Самообслуговування за запитом;**
- **Вільний доступ через мережу Інтернет;**
- **Об’єднання ресурсів;**
- **Швидка масштабованість.**

Проблеми, пов'язані з безпекою у хмарі.

Є ряд питань / проблеми, пов'язані з безпекою хмарних обчислень, але ці питання діляться на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг і питання безпеки, з якими стикаються їх клієнти. Для того, щоб зберегти ресурси, скоротити витрати, та зберегти ефективність, провайдери хмарних послуг часто зберігають більше одного разу дані клієнта на тому ж сервері.

Управління безпекою у хмарі. Архітектура безпеки хмари є ефективною, тільки якщо правильно реалізовано захист на місці. Ефективна архітектура безпеки хмари визначає проблеми, які виникатимуть з керуванням безпеки. Управління безпеки усуває проблеми пов'язані з контролем безпеки. Існує багато типів управління архітектурною безпекою хмари, вони зазвичай можуть бути знайдені в одній з наступних категорій:

- **Стримуюче управління;**
- **Профілактичне управління;**
- **Коригуюче управління;**
- **Детективне управління.**

Безпека та приватність

- **Управління ідентифікацією;**

- **Фізична безпека;**
- **Безпека персоналу;**
- **Доступність;**
- **Безпека додатків;**
- **Приватність.**
- **Безпека хмарних моделей**

Рівень ризику в трьох хмарних моделях сильно відрізняється, та шляхи вирішення питань безпеки також відрізняються в залежності від рівня взаємодії. Вимоги до безпеки залишаються однаковими, але в різних моделях, SaaS, PaaS або IaaS, рівень контролю над безпекою змінюється. В моделі **SaaS** клієнт не керує мережею, серверами, операційними системами, зберіганням даних і навіть деякими можливостями додатків, тому основний обов'язок щодо забезпечення безпеки практично повністю лягає на постачальників.

Як і в моделі SaaS, в моделі **PaaS** клієнт не може управляти або контролювати інфраструктуру - мережі, сервери, операційні системи або системи зберігання даних - але має контроль над розгортанням додатків.

У моделі **IaaS** клієнти мають контроль над операційними системами, зберіганням даних і розгортанням додатків і, можливо, обмеженим контролем над вибором мережевих компонентів.

Висновок

Сьогодні ми не можемо собі уявити виконання якоїсь роботи, або діяльність з метою розваг без потужних пристроїв, типу ПК, планшетів або смартфонів. Але інколи ці пристрої створюють деякі незручності, наприклад, наш накопичувач зламався і не піддається ремонту, тому уся інформація виявляється знищеною. Або, через відсутність потрібного додатку ми не можемо виконати якусь частину роботи. Або, зараз немає доступу до смартфону, на якому зберігаються важливі проекти.

Проблем може бути багато і не завжди їх можна вирішити, тому я вважаю тему хмарних технологій дуже актуальною. Вони допомагають нам тримати потрібні дані “під рукою”, до яких ми можемо звернутися у будь-який момент часу, або хмарному сервісі є додаток, який потрібен для виконання проекту, або його зберігання. Наприклад, Google Drive - повний офісний пакет з хмарним зберіганням.

Але не менш актуальною є тема захисту цих даних. Необхідно забезпечити захист даних на високому рівні, не наражаючи на небезпеку ні клієнтів, ні компанію, що надає доступ до хмарних сервісів. Це можна зробити за допомогою локального резервного копіювання, шифрування даних, встановлення надійного паролю для запобіганню розкрадання даних та встановлення антивірусного програмного забезпечення.

Перелік посилань:

1. https://bankchart.com.ua/finansoviy_gid/groshi_rodini/statti/porivnyannya_hmarnih_shovisch_onedrive_dropbox_google_drive_i_box#3;
2. https://worldvision.com.ua/luchshie-6-sovetov-dlya-predpriyatiy-po-zashchite-dannykh-v-oblake/;
3. https://naurok.com.ua/urok-hmarni-tehnologi-188869.html;
4. https://ukrbukva.net/93548-Informacionnaya-bezopasnost-v-oblachnyh-vychisleniyah-uyazvimosti-metody-i-sredstva-zashity-instrumenty-dlya-provedeniya-audita-i-rassledovaniya-incid.html;
5. https://onbiz.biz/cloud-computing-models/.