Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

"Допущено до захисту"
Начальник кафедри управління інформаційною безпекою, д.т.н., доцент
полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
"____" _____2022 року

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНАНА РОБОТА

на тему **Дослідження методів захисту інформаційних ресурсів при використанні хмарних технологій на прикладі Microsoft Azure**

Виконав:
здобувач IV курсу, групи КБ-41
спеціальності (освітньої-професійної програми)
125 "Кібербезпека"
(Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої-професійної програми))
Дмитро ЛЕНЧУК
(ім'я та прізвище)
Керівник Орест ПОЛОТАЙ
(ім'я та прізвище)
Рецензент Ірина АРТИЩУК
(ім'я та прізвище)

Львів – 2022 року

АНОТАЦІЯ

Дмитро Ленчук “Дослідження методів захисту інформаційних ресурсів при використанні хмарних технологій на прикладі Microsoft Azure“. Бакалаврська кваліфікаційна робота за спеціальністю 125 “Кібербезпека” складається з текстової частини (пояснювальної записки), що містить 3 розділи, 69 с., 8 рис., 5 табл., 37 джерела. А також – графічної (презентації), що містить 11 слайдів.

Об’єкт дослідження – безпека інформації, яка передається, зберігається і обробляється при використанні хмарних обчислень.

Предмет дослідження – методи забезпечення інформаційної безпеки при використанні хмарних сервісів.

Мета роботи – підвищення інформаційної безпеки підприємств, що обробляють інформацію за допомогою хмарних технологій.

Бакалаврська кваліфікаційна робота спрямована на дослідження методів забезпечення інформаційної безпеки при використанні служби хмарних обчислень Microsoft Azure, побудована модель загроз для підприємства, де використовують хмарні технології.

Наведено порівняння витрат на впровадження локальної інфраструктури підприємства та аналогічної інфраструктури у хмарі.

Наукова новизна роботи полягає в дослідженні методів забезпечення інформаційної безпеки на підприємствах, де використовуються сучасні хмарні техноголії.

Напрямки подальших досліджень полягають у детальному аналізі доцільності застосування хмарних обчислень на підприємствах різних форм власності.

Ключові слова: ХМАРНІ ОБЧИСЛЕННЯ, ХМАРНІ ТЕХНОЛОГІЇ, MICROSOFT AZURE, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Dmytro Lenchuk "Research of methods of protection of information resources when using cloud technologies on the example of Microsoft Azure". Bachelor's thesis in the specialty 125 "Cybersecurity" consists of a text part (explanatory note), which contains 3 sections, 69 pages, 8 figures, 5 tables, 37 sources. And also - a graphic (presentation) containing 11 slides.

The object of research is the security of information that is transmitted, stored and processed using cloud computing.

The subject of research - methods of information security when using cloud services.

The purpose of the work is to increase the information security of enterprises that process information using cloud technologies.

The bachelor's qualification work is aimed at studying the methods of information security when using the cloud computing service Microsoft Azure, built a threat model for the enterprise, which uses cloud technologies.

A comparison of the costs of implementing the local infrastructure of the enterprise and similar infrastructure in the cloud.

The scientific novelty of the work lies in the study of methods of information security in enterprises that use modern cloud technologies.

Areas of further research are a detailed analysis of the feasibility of using cloud computing in enterprises of various forms of ownership.

Keywords: CLOUD COMPUTING, CLOUD TECHNOLOGIES, MICROSOFT AZURE, INFORMATION SECURITY.

ЗМІСТ

ВСТУП ……..….. 8

РОЗДІЛ 1. ОСОБЛИВОСТІ ХМАРНИХ ТЕХНОЛОГІЙ…….. 10

1.1. Побудова хмарних обчислень……..……... 10

1.2. Які технології можна назвати хмарними……. 11

1.2.1. Універсальність доступу…… 13

1.2.2. Самообслуговування за вимогою…….. 14

1.2.3. Спільне використання обчислювальних потужностей…… 15

1.2.4. Масштабування за потребою……. 16

1.2.5. Плачу за те що споживаю……... 17

1.3. IaaS, PaaS, SaaS як моделі обслуговування…….……. 18

1.4 Типи розгортання хмарних технологій…….…….. 23

Висновок до розділу …….. 26

РОЗДІЛ 2. МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ MICROSOFT AZURE……..……... 28

2.1. Вступ до Microsoft Azure…… 28

2.2. Особливості Microsoft Azure……. 31

2.3. Методи забезпечення інформаційної безпеки Microsoft Azure ……. 35

2.3.1. Загальна безпека Azure…… 35

2.3.2. Безпека сховищ…… 37

2.3.3. Безпека баз даних……. 38

2.3.4. Безпека мереж…….. 40

2.3.5. Керування доступами…….. 40

2.4. Побудова моделі загроз ……. 42

2.5. Побудова моделі порушника …… 50

Висновок до розділу …….. 52

РОЗДІЛ 3. ВИЗНАЧЕННЯ ВИТРАТ НА ВПРОВАДЖЕННЯ ЛОКАЛЬНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА ТА АНАЛОГІЧНОЇ ІНФРАСТРУКТУРИ У ХМАРІ MICROSOFT AZURE ……. 54

3.1. Розрахунок поточних витрат на впровадження хмарної інфраструктури підприємства…… 54

3.2. Розрахунок витрат на впровадження локальної інфраструктури підприємства …….. 57

3.2.1. Капітальні витрати……..…… 57

3.2.2. Поточні витрати……..…… 59

3.3. Економічне обґрунтування ……..... 60

Висновок до розділу 61

ЗАГАЛЬНІ ВИСНОВКИ ……..……... 63

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……..... 67

ЗАГАЛЬНІ ВИСНОВКИ

У першому розділі дипломної роботи розглядаються основні характеристики хмарних технологій за визначенням Національного інституту стандартів і технологій, а саме: самообслуговування за вимогою, повсюдність доступу, об’єднання ресурсів, масштабованість та облік споживання.

Самообслуговування на вимогу дає можливість споживачеві виконати всі необхідні дії для модернізації пропонованих йому послуг без звернення до постачальника хмарних послуг.

Універсальність доступу забезпечується широкою доступністю сервісу та підтримкою багатьох кінцевих пристроїв: персональних комп’ютерів, мобільних телефонів, смартфонів, інтернет-планшетів, з різними операційними системами та різними можливостями.

Колективна оренда та об'єднання ресурсів. Ресурси хмарних обчислень розроблено для підтримки моделі з кількома клієнтами. Колективна оренда дозволяє кільком клієнтам використовувати одні й ті ж програми або одну фізичну інфраструктуру, зберігаючи при цьому конфіденційність і безпеку своєї інформації.

Швидка еластичність і масштабованість. Однією з чудових переваг хмарних обчислень є можливість швидкого надання ресурсів у хмарі, оскільки вони потрібні виробничим організаціям. А потім видаляти їх, коли вони їм не потрібні. Ресурси хмарних обчислень можуть швидко збільшуватися або зменшуватися, а в деяких випадках це може відбуватись автоматично.

Облік використання. Використання ресурсів хмарних обчислень фіксується, і виробничі організації платять відповідно за те, що вони використали. Використання ресурсів можна оптимізувати, використовуючи можливості плати за використання. Це означає, що використання хмарних ресурсів — чи то екземпляри віртуального сервера, які працюють, чи сховище в хмарі — контролюється, вимірюється та повідомляється постачальником хмарних послуг.

На сьогодні можна вирізнити три основні моделі обслуговування хмарних технологій:

- інфраструктура як послуга (Infrastructure as a Service, скор. IaaS);
- платформа як послуга (Platform as a service, скор. PaaS);
- програмне забезпечення як послуга (software as a service, скор. SaaS).

Найвищим рівнем абстракції в хмарі є модель «програмне забезпечення як послуга» (SaaS).

У моделі SaaS хмарний постачальник пакує та надає бізнес-користувачу встановлений додаток. Програма зазвичай розміщується в хмарі та керується стороннім постачальником. Користувачі створюють облікові записи у провайдера, щоб отримати доступ до програми. Доступ до програми здійснюється через Інтернет через веб-браузер, і користувачеві не потрібно нічого встановлювати або підтримувати. Компанія стягує регулярну щомісячну плату залежно від кількості користувачів і функцій програми.

Нижчим рівнем абстракції у загальнодоступній хмарі є модель «платформа як послуга» (PaaS).

PaaS багато в чому схожий на SaaS. Але замість того, щоб мати хост-провайдер і надавати одну програму, доступний взаємопов’язаний набір програм та інструментів, до яких користувач може отримати доступ через Інтернет через веб-браузер. Ці інструменти можуть використовуватися багатьма користувачами і використовуватися для створення повного, повністю функціонального середовища розробки програмного забезпечення, гібридної хмари чи інших середовищ. Як і у випадку з SaaS, інструменти PaaS зазвичай розміщуються в хмарі та керуються третьою стороною.

Найнижчим рівнем абстракції у загальнодоступній хмарі є модель інфраструктури як послуги (IaaS), яка в основному працює як віртуальний центр обробки даних у хмарі.

IaaS розміщує програми та дані. IT-команди використовують IaaS для створення віртуальної інфраструктури хмарних ресурсів і сервісів, здатних керувати програмою та доступних для співробітників, бізнес-партнерів і

користувачів. Основною перевагою IaaS є зручність, яка дозволяє підприємствам відмовитися від дорогої інфраструктури локальних центрів обробки даних на користь гнучких хмарних ресурсів, які доступні та оплачуються лише за потреби.

Існує 4 основних типи хмарних обчислень: приватні хмари,загальнодоступні хмари, гібридні хмари та багатохмарні.

Публічні хмари — це хмарні середовища, які зазвичай створюються з IT-інфраструктури, що не належить кінцевому користувачеві. Деякі з найбільших постачальників загальнодоступних хмар включають Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud та Microsoft Azure. Усі хмари стають загальнодоступними, коли середовища розділені й перерозподілені між кількома клієнтами. Структури плати більше не є обов'язковими характеристиками загальнодоступних хмар, оскільки деякі постачальники хмар (наприклад, Massachusettes Open Cloud) дозволяють орендарям використовувати свої хмари безкоштовно.

Приватні хмари вільно визначаються як хмарні середовища, призначені виключно для одного кінцевого користувача або групи, де середовище зазвичай працює за брандмауером цього користувача або групи. Усі хмари стають приватними, коли базова IT-інфраструктура призначена для одного клієнта з повністю ізольованим доступом. Але приватні хмари більше не потрібно отримувати з локальної IT-інфраструктури. Зараз організації створюють приватні хмари в орендованих центрах обробки даних, що належать постачальникам, розташованих поза межами, що робить будь-які правила розташування та права власності застарілими.

Гібридна хмара — це, здавалося б, єдине IT-середовище, створене з кількох середовищ, підключених через локальні мережі (LAN), глобальні мережі (WAN), віртуальні приватні мережі (VPN) та/або API. .

Багатохмарне середовище може існувати навмисно (для кращого контролю конфіденційних даних або як надлишковий простір для зберігання для покращеного аварійного відновлення) або випадково (зазвичай це результат тіньових IT). У будь-якому випадку, наявність кількох хмар стає все більш

поширеним серед підприємств, які прагнуть покращити безпеку та продуктивність за допомогою розширеного портфоліо середовищ.

У другому розділі дипломної роботи були розглянуті особливості та послуги що надаються клієнтам Microsoft Azure:

- Загальні засоби безпеки Azure (Azure Defender for Cloud, Azure Key Vault);
- Засоби безпеки сховищ (Azure Storage Service Encryption)
- Засоби безпеки баз даних (Azure SQL Firewall, Azure SQL Transparent Data Encryption)
- Засоби безпеки мереж (Network Security Group, Web Application Firewall)
- Засоби керування доступом (RBAC, Azure Active Directory)

У третьому розділі дипломної роботи було визначено, що вартість інфраструктури на рік при використанні хмарної служби Microsoft Azure на 20% дешевше ніж при використанні локальної інфраструктури, при умові що вона експлуатується протягом 5 років.

В Україні використання хмарних обчислювальних систем регулюється загальними інформаційними законами та нормативними актами у сфері інформаційних технологій.

17 лютого 2022 року був прийнятий законопроект №2655, метою якого є створення умов для обробки та захисту даних при використанні технології хмарних обчислень, наданні хмарних послуг та визначенні особливостей використання хмарних послуг органами державної влади, а також більш ефективного використання державних ресурсів шляхом впровадження новітніх технологій. Також законопроект встановлює правові засади надання хмарних послуг та визначає умови договору про надання хмарних послуг. Ця подія створила правовий фундамент для розбудови якісно нової інформаційної інфраструктури країни [21].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України. Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

2. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

3. Довганич М. О. Методи та засоби захисту персонального інформаційного простору в контексті мережевої розвідки / М. О. Довганич, В. І. Ящук // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С. 79-81).

4. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

5. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 21–22.

6. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 52–54.

7. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

8. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

9. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.

10. Ориник С. Забезпечення безпеки використання хмарних сховищ для захисту персональних даних / С. Ориник, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

11. Полотай О., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у2 ч. Ч. 2. – Київ: Нац. акад. СБУ, 2016. – С. 204-205.

12. Рада ухвалила закон про хмарні послуги — УНІАН [Електронний ресурс] – Режим доступу : https://www.unian.ua/economics/other/rada-uhvalila-zakon-pro-hmarni-poslugi-ostanni-novini-11707906.html

13. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запроваджені концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного

захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 149–150.

14. Ящук В.І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктури матеріали Міжнародної науково-практичної конференції “Сучасні напрями розвитку економіки, підприємництва, технологій та їх правового забезпечення” 02-03 червня 2021 року м. Львів.

15. Assign Azure roles using the Azure portal - Azure RBAC | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current

16. Azure compliance documentation | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/compliance/

17. Azure Key Vault Overview - Azure Key Vault | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/key-vault/general/overview

18. Azure Security Services and Technologies | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/security/fundamentals/services-technologies

19. Azure Storage encryption for data at rest | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

20. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

21. CLOUD VS. ON-PREMISES COSTS [Електронний ресурс] – 5 с. – Режим доступу : https://codilime.com/pdf/faCloudOnPremisesFoundations.pdf

22. Control Engineering | Five characteristics of cloud computing [Електронний ресурс] – Режим доступу : https://www.controleng.com/articles/five-characteristics-of-cloud-computing/

23. Статистика зарплат програмістів, тестувальників і PM в Україні | DOU [Електронний ресурс] – Режим доступу : https://jobs.dou.ua/salaries/?period=2021-12&position=SysAdmin&experience=0-1

24. IP firewall rules - Azure SQL Database and Azure Synapse Analytics | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/azure-sql/database/firewall-configure

25. Microsoft Defender for Cloud - an introduction | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

26. Plan Azure virtual networks | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm

27. Pricing Calculator | Microsoft Azure [Електронний ресурс] – Режим доступу : https://azure.microsoft.com/en-us/pricing/calculator/

28. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Electronic resource] / Peter Mell, Timothy Grance – Special Publication 800-145 – 7 p. – Режим доступу : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

29. Total Cost of Ownership (TCO) Calculator | Microsoft Azure [Електронний ресурс] – Режим доступу : https://azure.microsoft.com/en-us/pricing/tco/calculator/

30. Transparent data encryption - Azure SQL Database & SQL Managed Instance & Azure Synapse Analytics | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview

31. Types of cloud computing [Електронний ресурс] – Режим доступу : https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

32. Understand cloud abstraction for your IT needs [Електронний ресурс] – Режим доступу : https://www.techtarget.com/searchcloudcomputing/tip/Understand-cloud-abstraction-for-your-IT-needs

33. What is Azure - A Complete Guide [Електронний ресурс] – Режим доступу : https://www.acronis.com/en-gb/blog/posts/what-is-microsoft-azure/

34. What is Azure Active Directory? | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

35. What is Azure web application firewall on Azure Front Door? | Microsoft Docs [Електронний ресурс] – Режим доступу : https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

36. What is Azure—Microsoft Cloud Services | Microsoft Azure [Електронний ресурс] – Режим доступу : https://azure.microsoft.com/en-us/overview/what-is-azure/