Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Наумовця Сергія Кириловича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методологія забезпечення кібербезпеки у віртуальних банківських системах*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст.викладач Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер				

Дніпро

2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Наумовцю Сергію Кириловичу*** **академічної групи** ***125м-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Методологія забезпечення кібербезпеки у віртуальних банківських системах*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 № 1036-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Аналіз актуальності, розвитку та загроз необанкінгу. Постановка задачі	30.10.2021
Розділ 2	Формування вимог щодо впровадження методів. Аналіз розподілу управління ризиками. Обґрунтування вибору хмарного провайдера.	30.11.2021
Розділ 3	Розрахунок економічних показників запропонованих рішень.	25.12.2021

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі:

Дата подання до екзаменаційної комісії:

Прийнято до виконання _____ Наумовець С.К.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 61 с., 6 рис., 9 табл., 3 додатка, 22 джерела.

Об'єкт дослідження: віртуальні банківські системи.

Предмет дослідження: реалізація вимог з кібербезпеки для віртуальних банківських систем.

Мета роботи: розробка рекомендацій щодо методів реалізації вимог з кібербезпеки для віртуальних банківських систем.

Методи дослідження: системний підхід, методи порівняння.

У першій частині описано актуальність технологічності необанкінгу сучасності. Принципи роботи необанків, динаміка розвитку та наведено порівняння загроз між класичним банком та необанком.

У спеціальній частині проаналізовано актуальні загрози та ризики про роботі у хмарному середовищу, запропоновано рекомендації щодо вибору надійного провайдера. Запропоновано вибір сервісів провайдера для впровадження в банківську систему. Запропоновано методи вирішення актуальних ризиків при роботі у хмарному середовищі.

В економічному розділі визначено: ефективність впровадження запропонованих методів забезпечення безпеки інформації при переході у хмару.

Практичне значення роботи полягає у дослідженні збереження технологічної відповідності стандартам та вимогам безпеки інформації в банківській установі при використані хмарних технологій.

Усі результати досліджень у дипломній роботі можуть бути використані для подальшого удосконалення систем безпеки банківських хмарних структур.

КЛЮЧОВІ СЛОВА: : АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ, ХМАРНІ ТЕХНОЛОГІЇ, ХМАРНА МОДЕЛЬ РОЗРАХУНКІВ, IaaS, SaaS, PaaS, ЗАГРОЗИ, SLA, УПРАВЛІННЯ РИЗИКАМИ, ХМАРНІ СЕРВІСИ.

ABSTRACT

Explanatory note: 61 pages, 6 figures, 9 tables, 3 appendices, 22 sources.

Object of research: virtual banking systems.

Subject of research: implementation of cybersecurity requirements for virtual banking systems.

Objective: to develop recommendations on methods of implementing cybersecurity requirements for virtual banking systems.

Research methods: system approach, comparison methods.

The first part describes the relevance of the manufacturability of modern neobank. Principles of operation of neo-banks, dynamics of development and comparison of threats between classical bank and neo-bank.

The special part analyzes the current threats and risks of working in a cloud environment, offers recommendations for choosing a reliable provider. The choice of provider services for implementation in the banking system is offered. Methods for solving current risks when working in a cloud environment are proposed.

The economic section defines: the effectiveness of the implementation of the proposed methods of information security during the transition to the cloud.

The practical significance of the work is to study the preservation of technological compliance with standards and information security requirements in the banking institution when using cloud technologies.

All research results in the thesis can be used to further improve the security systems of banking cloud structures.

KEY WORDS:: INFORMATION RISK ANALYSIS, CLOUD TECHNOLOGIES, CLOUD CALCULATION MODEL, IaaS, SaaS, PaaS, THREATS, SLA, GOVERNANCE MANAGEMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AKS – Azure Kubernetes Service

ACS – Azure Container Registry

AWS – Amazon Web Services

CISO – Chief information security officer

DoS/DDoS - Denial-of-service/Distributed Debial-of-service

EBS – Elastic Block Storage

EC2 - Elastic Compute

FIPS - Federal Information Processing Standards

IaaS – Infrastucture as a service

IEC - International Electrotechnical Commission

IOPS – Input/output operations per second

ISO – International Organization for Standardization

GDPR - General Data Protection Regulation

HSM - Hardware Security Module

KMS - Key Management Services

NIST - National Institute of Standards and Technology

PaaS – Platform as a service

PCI DSS – Payment Card Industry Data Security Standard

SaaS – Software as a service

SLA - Service Level Agreement

TLS - Transport Layer Security

ВМ – Віртуальна машина

НБУ – Національний Банк України

ПЗ – Програмне Забезпечення

СУІБ – Система управління інформаційною безпекою

СУБД – Система управління базами даних

СКС – Структурована кабельна система

ТЕО – Техніко-економічне обґрунтування

ЗМІСТ

ВСТУП

Необанки - це компанії, що спеціалізуються на фінансових технологіях (fintech), які пропонують цифровий фінансовий сервіс. Це означає, що клієнт може отримати доступ до банківських послуг за допомогою будь-якого смартфону, планшету, браузеру, тощо. Такий підхід допомагає оптимізувати банківський процес і зменшити витрати організації, що вирішила трансформуватися з класичного банку у необанк.

Основна відмінність між класичним банком і необанком в точці входу клієнта у продукт, що пропонує організація. Тобто, класичний банк примушує людину знаходитись фізично у відділені банку для відкриття рахунку, після чого його оригінали документів проходять перевірку співробітниками відділення, що по-перше займає багато часу, по-друге дає потенційну вірогідність змови між співробітником банку і потенційним шахраєм.

Аналізуючи динаміку розвитку необанкінгу можна зрозуміти, що все більше класичних банків почне переносити свої основні процеси у хмари. Безумовно це призведе до перегляду законодавчої бази, бо на сьогоднішній момент немає чітких правил щодо регулювання роботи необанків. Також зміниться вектор атак, що за собою несе створення нових методів забезпечення захисту, не враховуючи вже існуючі. Вплив необанків на ринок сьогодні з часом зробить їх існуючу систему обробки даних клієнтів стандартом серед всіх класичних банків.

Увесь процес адаптування сервісів під клієнта в необанках також призведе до виникнення нових вимог щодо забезпечення більш детального моніторінгу за подіями та додаткового шифрування даних як у гаджеті клієнта так і на стороні сервісів для забезпечення безпеки даних у банківській системі.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Принцип функціонування та переваги необанку

Необанкінг інтегрує в бізнес-процеси машинне навчання та технології штучного інтелекту для спрощення контролю ваших фінансів і тим самим скорочує документообіг з участю людини в банківських процесах оцифровуючи весь папер.

Як правило необанки існують як банківський продукт, що підкріплений до батьківського банку. Основною функцією необанкінгу є надання неперервності документообігу в цифровому вигляді таким чином, щоб не суперечити законодавству.

Основне різноманіття між класичним банком і необанком в точці входу клієнта у продукт, що пропонує організація. Тобто, класичний банк примушує людину знаходитись локально у відділені банку для відкриття рахунку, після чого його оригінали документів проходять перевірку співробітниками відділення, що по-перше займає багато часу, по-друге дає потенційну вірогідність змови між співробітником банку і потенційним шахраєм.

Необанк проводить процедуру надання клієнту послуг онлайн в часності в цьому допомагають хмарні технології, що нівелює ризик змови з шахраями на етапі перевірки його ідентифікаційних документів за допомоги штучного інтелекту. Проте в іншому механізм роботи з клієнтськими рахунками, даними, тощо - однаковий.

Необанки не мають фізичних приміщень для обслуговування клієнтів, всі сервіси існують всередині хмари, що дозволяє в значній мірі економити гроші компанії на оренді, наймі великої кількості персоналу, що буде знаходитись в приміщеннях та обслуговувати клієнтів, закупці технічних засобів і технічних спеціалістів для обслуговування цієї техніки.

Бізнес процес роботи з клієнтськими даними необанк закриває від очей для співробітника, бо всі дані клієнтів існують у окремих базах даних, це можна назвати розподілом зони відповідальності.

Відповідно, що не маючи фізичних точок для обслуговування, необанки пропонують свої послуги для клієнтів з мінімальними комісіями, оскільки технологія обробки даних автоматизована і не потребує втручання людини. Окрім того, необанк встановлює контроль за циркуляцією інформації в організації.

Необанки орієнтовані на клієнта, допомагаючи йому економити фінанси за допомогою участі технологій штучного інтелекту та Big Data в традиційному банківському обслуговуванні. Також інтерфейси додатків доволі прості, не

перегружені зайвою інформацією, що допомагає клієнту швидше освоїтись у просторі послуг необанку.

Послуги необанку не потребують великих витрат на його використання і можуть не потребувати плату за обслуговування клієнта взагалі. Необанк дозволяє клієнтам не витрачати свої кошти на зайві комісії під час транзакцій, що в свою чергу допомагає бути впевненими в тому, що клієнтські гроші не будуть інвестовані в інтереси організації.

Головною перевагою можна назвати актуальність технологій, що використовуються в необанках. Інтерфейси постійно адаптують під потреби клієнтів, технології обробки клієнтських даних завжди оптимізуються, коли класичний банк витрачає значну кількість часу на обробку паперу.

1.2 Аналіз динаміки розвитку необанкінгу

В останній час динаміка розвитку необанків тільки зростає. Вже на сьогоднішній день у світі зареєстровано не менш ніж 300 необанків і ще готується низка до запуску та отримання ліцензій для функціонування як необанк.[1,2]

На рис.1.1 наведено динаміку розвитку необанків у світі починаючи з 2010 року до сьогодні відповідно до [1]

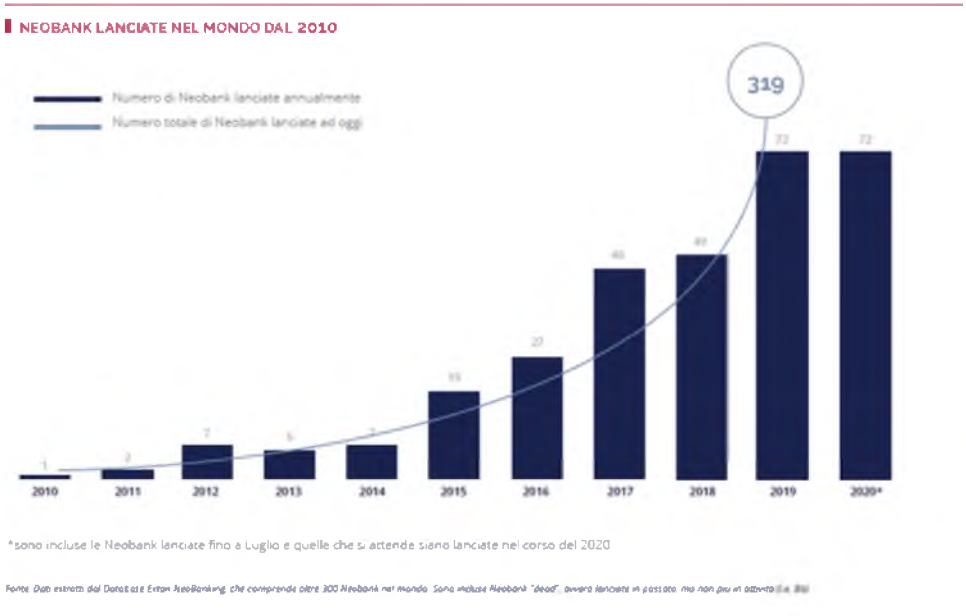

Рисунок 1.1 Динаміка розвитку необанкінгу в світі

Європа, як і раніше, залишається двигуном інновацій, де знаходяться три з п'яти найбільш розвинутих ринків: Великобританія як центр необанкінга, за нею йдуть Швеція і Франція. Слід зазначити, що тільки в Європі понад 50 млн осіб відкрили рахунки в необанках.

При цьому інші ринки швидко наздоганяють Європу — насамперед Південна Корея і Бразилія, а також США. На рис. 1.2 наведено крупних представників необанків по світу [1]

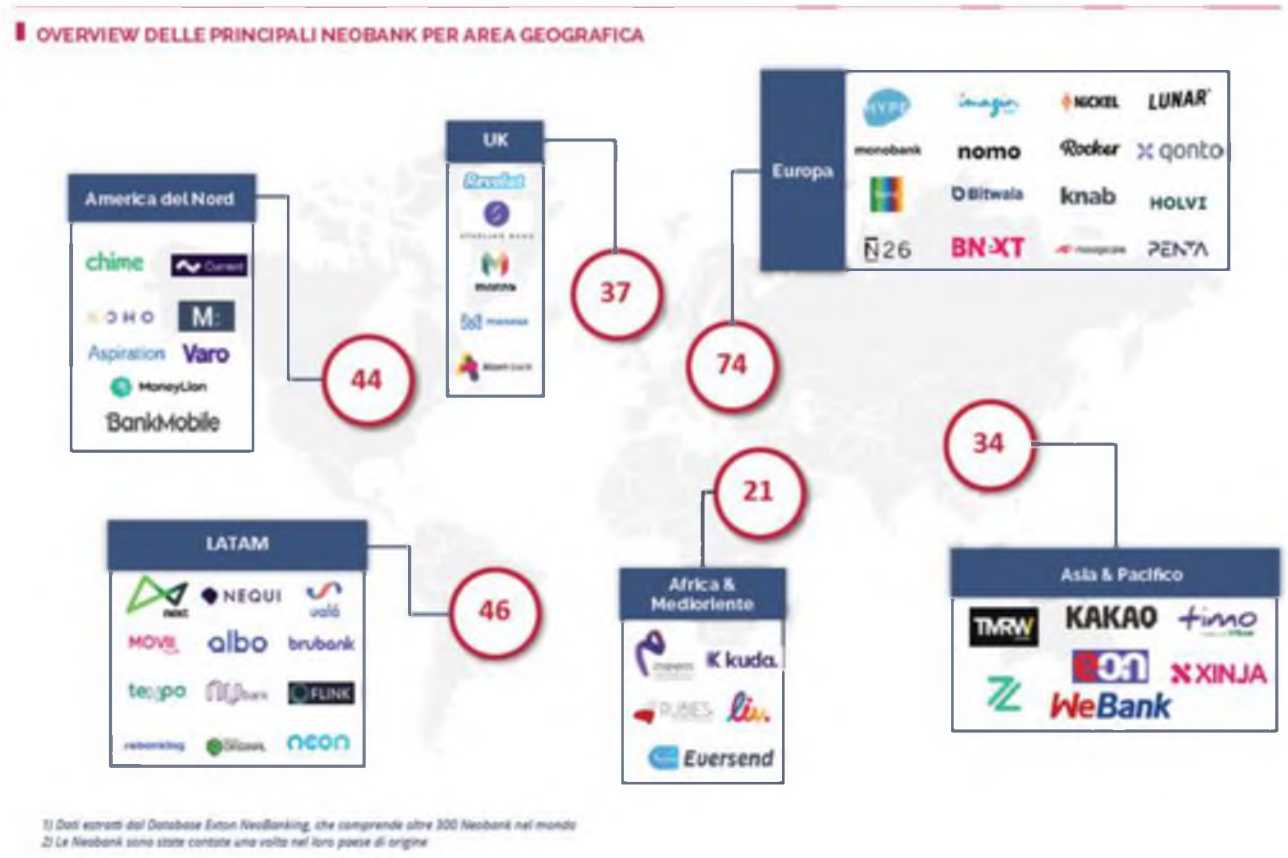

Рисунок 1.2. найкрупніші представники необанків світу за регіонами

Для нашої країни необанкінг це відносно нове поняття. Їх кількість поступово зростає, та їх позиції на ринку поступово закріплюються на ринку поруч з класичними банками.

Прикладом необанків України є:

Таблиця 1.1 Представники необанків в Україні

Назва	Лого
monobank	
izibank	

Продовження таблиці 1.1 Представники необанків в Україні

Назва	Лого
sport bank	
o.bank	
neobank	
todo bank	

На сьогоднішній день в Україні існує проблема щодо регулювання створення та розвитку нових необанків через достатньо консервативний підхід діючого законодавства, через що необанки не можуть існувати окремо від вже існуючого класичного банку України.

Як приклад можна взяти Monobank, що э необанком, але існує та обслуговує клієнтів за ліцензією UniversalBank. Тобто, реєструючись у додатку monobank людина стає клієнтом UniversalBank, але без прямого доступу до своїх послуг у його відділеннях. Монобанк – це просто портал в Інтернеті, що надає доступ до

банківських послуг. UniversalBank є фінансовим партнером та виконує прямі операції. [3]

1.3 Аналіз вимог із забезпечення інформаційної безпеки для банків України

Для забезпечення відповідності вимог законодавчих та нормативних документів в сфері щодо банківської діяльності щодо забезпечення інформаційної безпеки в банках України, необхідно аналіз основних вимог цих документів.

Для українських банків було видано постанову національним банком України "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" від 28.09.2017 № 95, що визначає основні та обов'язкові до виконання організаційні та технічні процеси щодо забезпечення безпеки інформації всередині банківської системи України.

Нажаль постанова була видана лише після крупного хакерского нападу на багату кількість банківських систем і не тільки, що призвело до великої кількості відмов у обслуговуванні та привела до величезних збитків організацій, що займаються банківською діяльністю.

Сам документ складається з 150 пунктів, пояснюючих необхідність впровадження організаційний та технічних методів для адекватно функціонуючого механізму захисту інформації, що буде циркулювати всередині банку. Виконано стислий аналіз змісту основних положень даного документу.

Перші сім пунктів описують сам документ, його призначення і область дії, а також використану термінологію в документі.

Восьмий пункт зазначає про необхідність банків у впроваджені власної системи управління інформаційною безпекою (СУІБ)

Як відомо, СУІБ це частина загальної системи управління, заснована на використанні методів оцінки бізнес-ризиків для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та покращення інформаційної безпеки банків. При створенні СУІБ рекомендується керуватися вимогами стандартів сімейства ISO 27000. Стандарти встановлюють вимоги щодо створення, впровадження, підтримки та постійного поліпшення системи безпеки організації. Метою СУІБ і

стандарту в цілому, є забезпечення захисту інформаційних ресурсів за рахунок ефективного управління ризиками пов'язаними з бізнес-процесами компанії.

Пункт дев’ятий зазначає необхідність впровадження процесного та ризик-орієнтованого підходу в організації. Процесний підхід являє собою відокремлення кожного бізнес-процесу для розглядання, що зв’язаний з іншими бізнес-процесами компанії. Ризик-орієнтований підхід дозволяє вибрати з величезної кількості вимог, розпоряджень та засобів захисту інформації ті, які дійсно необхідні організації та найкраще відповідають її потребам. Що дозволяє приймати усвідомлені, своєчасні та економічно-обґрунтовані рішення щодо застосування захисних заходів, базуючись на систематичному аналізі всіх факторів, що впливають на можливість здійснення загроз безпеці та ступені впливу цих загроз на бізнес.

Ризик-орієнтований підхід до вирішення завдань управління інформаційною безпекою лежить в основі всіх міжнародних та галузевих стандартів.

Пункт одинадцятий зазначає про необхідність банку в організації формування колективного керівного органу з питань впровадження та функціонування СУІБ, розробити становище, у якому визначити завдання, функції та обов'язки даного органу.

В таблиці 1.2 наведено вимоги щодо забезпечення впровадження СУІБ, заходи забезпечення інформаційної безпеки та криптографічного захисту інформації відповідно до постанови НБУ №95.

Таблиця 1.2 Стислий опис вимог постанови НБУ №95 від 28.09.2017

Пункт	Опис
17	Банк повинен розробити та запровадити політику інформаційної безпеки.
20	Банк зобов'язаний розробити та затвердити стратегію розвитку інформаційної безпеки.
23-24	При роботі з інформаційними системами НБУ необхідність в шифруванні інформації, слідкування за обліковими записами

	користувачів системи, тощо.
25	Банк зобов'язаний призначити особу відповідальну за інформаційну безпеку банку (Chief information security officer, CISO), яка має повноваження, достатні для прийняття управлінських рішень (посада не нижче за заступника голови правління банку).

Продовження таблиці 1.2 Стислий опис вимог постанови НБУ №95 від 28.09.2017

Пункт	Опис
26	Банк зобов'язаний сформувати підрозділ з інформаційної безпеки не менше ніж із двох працівників зі складу штатних працівників банку. Цей підрозділ безпосередньо підпорядковується відповідальному за інформаційну безпеку банку.
27-29	Описано регламент відносин відділів, відповідаючих за процеси пов’язані з інформаційною інформацією. (Підрозділ з інформаційної безпеки банку має здійснювати розробку вимог та здійснювати контроль за виконанням заходів щодо забезпечення безпеки інформації. Працівникам підрозділу ІБ та CISO(Chief Information Security Officer) забороняється мати повноваження щодо розробки, виробництва, адміністрування та експлуатації інформаційних систем банку, крім тих, що використовуються для забезпечення безпеки інформації. Підрозділу інформаційних технологій банку забороняється бути власником інформаційних систем банку, що безпосередньо забезпечують автоматизацію банківської діяльності.)

Продовження таблиці 1.2 Стислий опис вимог постанови НБУ №95 від 28.09.2017

Пункт	Опис
30-33	Зазначається, що працівники повинні бути ознайомлені з політикою інформаційної безпеки, яка розроблена у пункті 17. У контракті зі співробітником мають бути відображені обов'язки щодо дотримання ІБ. Також банк повинен ознайомлювати працівників із внутрішніми документами з ІБ та навчати їх у даному напрямку.
34-35	Регламентування роботи зі знімними носіями
36	Банк зобов'язаний розробити та затвердити внутрішні документи, що встановлюють вимоги щодо використання, надання, скасування та контролю доступу до інформаційних систем банку.
45	Банк повинен розробити та затвердити документи, що описують процес управління криптографічними ключами.
46-57	Визначення вимог щодо використання криптографічних алгоритмів в банку.
58-60	Вимоги до структурованої кабельної системи (СКС)
61-68	Вимоги до антивірусного програмного забезпечення (ПЗ) та його оновлень.
69-70	Операційні системи та ПЗ мають підтримуватися виробником, мати актуальні версії.
75	Банк повинен підтримувати у стані перелік ПЗ, що у банку.

Продовження таблиці 1.2 Стислий опис вимог постанови НБУ №95 від 28.09.2017

Пункт	Опис
77	Банк зобов'язаний розробити та затвердити процес управління оновленнями. Цей процес повинен містити такі стадії: – підготовка тестового середовища (тестових клієнтів); – підготовка переліку оновлень; – застосування оновлень у тестовому середовищі; – застосування оновлень на пілотній групі користувачів; – застосування протестованих оновлень.
78-82	Описують вимоги до ПЗ систем управління базами даних (СУБД) та серверів баз даних (БД).
83-88	Описують підвищені вимоги до робочих станцій та облікових записів (парольної політики) адміністраторів та інших привілейованих користувачів.
89-107	Описують вимоги до мережі, мережевого обладнання, кабельної системи, а також необхідність побудови єдиного місця управління мережею, підтримання документації в актуальному стані.
108	Банк зобов'язаний перевірити ефективність заходів захисту периметра мережі банку шляхом виконання періодичних тестів на проникнення.
109-111	Про використання електронного цифрового підпису лише від акредитованих центрів сертифікації ключів.
130-132	Описують порядок фіксації інцидентів безпеки інформації.

Останні пункти постанови визначають додаткові потреби щодо безпеки інформації, такі як:

- заборона використання радіотелефонів без шифрування;
- регламент з використання змінних носіїв;
- вимоги щодо застосування централізованих систем управління обліковими записами користувачів, оновлення безпеки для операційних систем, обліку інцидентів безпеки інформації;
- порядок маркування та документування елементів СКС;
- рекомендації щодо розподілу серверів та наявності проміжного сервера для ускладнення проникнення зловмисниками в мережу банку;
- необхідність боротьби з DoS/DDoS-атаками;
- вимоги до використання сертифікатів відкритих ключів.

Окрім постанови №95 НБУ також рекомендуються до використання наступні стандарти:

- ISO / IEC 27001 до: 2013 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги;
- ISO / IEC 27000 до: 2016 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів;
- ISO / IEC 27002 до: 2013 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки;
- ISO / IEC 27003: 2010 Інформаційні технології. Системи керування інформаційною безпекою. Настанова;
- ISO / IEC 27004: 2009 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання;
- ISO / IEC 27005: 2011 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;

- ISO / IEC 27006 до: 2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою;
- ISO / IEC 27007: 2011 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою;
- ISO / IEC 27008: 2011 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки;
- ISO / IEC 27011: 2008 Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002;
- ISO / IEC 27799: 2008 Інформаційні технології. Методи захисту. Настанова щодо управління інформаційною безпекою для організацій охорони здоров'я на основі ISO / IEC 27002.

Стандарти сімейства 27000 в першу чергу призначені для забезпечення захисту інформації в кіберпросторі та усунення проблем кібербезпеки, що виникають через наявність розбіжностей у підходах до організації методів безпеки в кіберпросторі.

Стандарт є технічним керівництвом націленим на реалізацію запобігання найбільш розповсюджених ризиків безпеки, включаючи:

- соціальну інженерію;
- злам;
- швидке розповсюдження злоякісного програмного забезпечення;
- шпигунське програмне забезпечення, потенційно небажане програмне;

Цей стандарт забезпечує пояснення основних положень кібербезпеки, пояснює зв'язок між кібербезпекою та іншими типами безпеки, дає визначення зацікавленим особам та опис їх ролі у кібербезпеці, керівництво з основних питань кібербезпеки, рекомендації з організації структури, за допомогою якої можна реалізувати співробітництво зацікавлених осіб для вирішення питань відносно забезпечення кібербезпеки.

Найголовнішою потребою для банку – має бути пройдена сертифікація PCI DSS, оскільки підприємство буде займатися обробкою платіжних карток. Стандарт безпеки даних індустрії платіжних карток (PCI DSS) – це пропрієтарний стандарт у сфері інформаційної безпеки. Він знаходиться під адміністративним управлінням Ради стандартів безпеки даних індустрії платіжних карток, заснованого компаніями American Express, Discover Financial Services, JCB International, MasterCard Worldwide та Visa Inc. Стислий перелік вимог стандарту наведено у таблиці 1.3

Таблиця 1.3 Стислий перелік вимог стандарту PCI DSS

Цілі	Вимоги
Створення та підтримка безпечних мереж та систем.	1. Встановлення та підтримка налаштувань брандмауера, необхідних для захисту даних власників карток. 2. Заміна встановлених на заводі системних паролів та інших параметрів безпеки за замовчуванням.
Захист даних власників карток.	3. Захист даних власників карток при зберіганні. 4. Шифрування даних власників карток при передачі по відкритих публічних мережах.
Реалізація програми контролю за вразливостями.	5. Захист усіх систем від шкідливого ПЗ та регулярне оновлення антивірусних програм. 6. Розробка та підтримка безпечних систем та додатків.

Продовження таблиці 1.3 Стислий перелік вимог стандарту PCI DSS

Цілі	Вимоги
Реалізація суворих заходів контролю доступу.	7. Обмежений доступ до даних власників карток, суворо в рамках практичної необхідності. 8. Ідентифікація та автентифікація доступу до компонентів системи. 9. Обмеження фізичного доступу до даних власників карток.
Регулярний моніторинг та тестування мереж.	10. Ідентифікація та моніторинг усіх звернень до мережевих ресурсів та даних власників карток. 11. Регулярне тестування систем та процесів, пов'язаних з безпекою.
Забезпечення політики інформаційної безпеки.	12. Забезпечення політики інформаційної безпеки щодо всіх працівників.

Таким чином, однією з основних умов переходу фізичної інфраструктури у хмару буде збереження відповідності всім законодавчим постановам і стандартам безпеки інформації, що організація була мати пройти на етапі функціонування з наземною інфраструктурою.

1.4 Хмарна модель необанку

Для оцінки доцільності переходу від класичного банку у необанк, необхідно порівняти між собою хмарні моделі, які пропонуються провайдерами та визначити ефективний варіант з точки зору контролю процесів організацією та безпеки даних відповідно до законодавства країни у якій класичний банк має намір перетворитись у необанк. Та почати треба з визначення хмарних технологій загалом.

Як відомо, хмарні технології надають обчислювальні послуги, включаючи сервери, сховище, бази даних, мережу, програмне забезпечення, аналітику та інтелект — через Інтернет («хмара»), щоб запропонувати швидші інновації, гнучкі

ресурси та економію масштабу. Зазвичай компанії платять лише за хмарні послуги, якими користуються, що допомагає знизити операційні витрати, ефективніше керувати інфраструктурою та розширюватися відповідно до змін бізнесу. [5]

На сьогодні багата кількість компаній розглядає хмарні технології в більшій частині лише як місце для збереження даних, але провайдери хмарних послуг мають дуже багату вибірку для організації бізнес-процесів компаній та забезпечення їх безпеки від загроз та атак зовні.

По-перше треба порівняти провайдерів хмарних технологій на ринку та обрати оптимальний за критерієм можливостей надання послуг на забезпечення безпеки даних замовника.

На ринку провайдерів хмарних технологій є три гіганти, це Google Cloud, Amazon Web Services та Azure від Microsoft.

Наряду з меншими представниками хмарних технологій ці троє займають провідне місце на ринках інфраструктури як послуги (IaaS) і платформи як послуги (PaaS)

IaaS (Infrastructure as a service) - це одна з послуг хмарних провайдерів, яка зосереджена на наданні інфраструктурних послуг на основі технології хмарних обчислень. IaaS використовується для заміни фізичних ресурсів, таких як сервери, віртуальними ресурсами, розміщеними та керованими провайдерами. Користувачі системи можуть запускати будь-яку операційну систему чи програму на цих орендованих серверах, не несучи ніяких додаткових зборів за обслуговування та експлуатацію. [5,6]

PaaS (Platform as a service) - це сервіс, який забезпечує розробникам основу для розробки додатків. У найпростішому сенсі сторонній постачальник надаватиме апаратні та програмні засоби користувачам через Інтернет, а користувачам потрібно буде займатися лише процесом проектування та розробки програми. Все апаратне та програмне забезпечення буде розміщено постачальником послуг PaaS на власній інфраструктурі. [5,6]

SaaS (Software as a service) - це програмне забезпечення як послуга (також зване веб-програмним забезпеченням, програмним забезпеченням на вимогу або

розміщеним програмним забезпеченням) є моделлю розповсюдження програмного забезпечення, програми якої розміщуються та доступні клієнтам через Інтернет. Використовуючи це рішення, замовник матиме доступ до програми, а також її безпеки, доступності та продуктивності, якими керує постачальник сервісу. [5,6]

Згідно зі звітом Synergy Research Group за 2020 рік, «зріст Amazon продовжує відображати загальне зростання ринку, тому він зберіг свою частку в 33% світового хмарного ринку. Друге місце в рейтингу Microsoft також зростає швидше, ніж ринок, його частка на ринку зросла майже на три відсоткові пункти за останні чотири квартали, досягнувши 18%». [4]

Microsoft особливо добре себе показує в SaaS, тоді як Google Cloud, з його потужністю в галузі штучного інтелекту, позиціонується для зростання в міру зростання ринку штучного інтелекту.

Завдяки величезному набору інструментів, який продовжує зростати в геометричній прогресії, можливості Amazon не мають собі рівних. Проте його структура витрат може бути складною у порівнянні з іншими провайдерами, а його зосередженість на загальнодоступній хмарі, а не на гібридній або приватній хмарі означає, що взаємодія з вашим центром обробки даних не є головним пріоритетом Amazon Web Service(AWS).

Близькgий конкурент AWS з надзвичайно потужною хмарною інфраструктурою - Azure. Azure наполегливо працює для взаємодії з користувацькими центрами обробки даних.

Google пізніше вийшов на ринок хмар і не має такої міри зосередженості на підприємстві, яка допомагає залучити корпоративних клієнтів. Але його технічний досвід є глибоким, а його провідні інструменти в галузі глибокого навчання та штучного інтелекту, машинного навчання та аналітики даних є значними перевагами. На рис. 1.3 представлено основних хмарних провайдерів існуючих на ринці сьогодні.

Рисунок. 1.3 Представники хмарних провайдерів

Як можна побачити на рис. 1.3, AWS займає домінуючу позицію у порівнянні з Microsoft Azure і Google Cloud Platform. Та з часом у лідерів ринку з'являться нові суперники, оскільки нішеві представники, такі як: Alibaba Cloud, IBM, Oracle та

Tencent Cloud не стоять на місці, а розвиваються і дуже швидко.

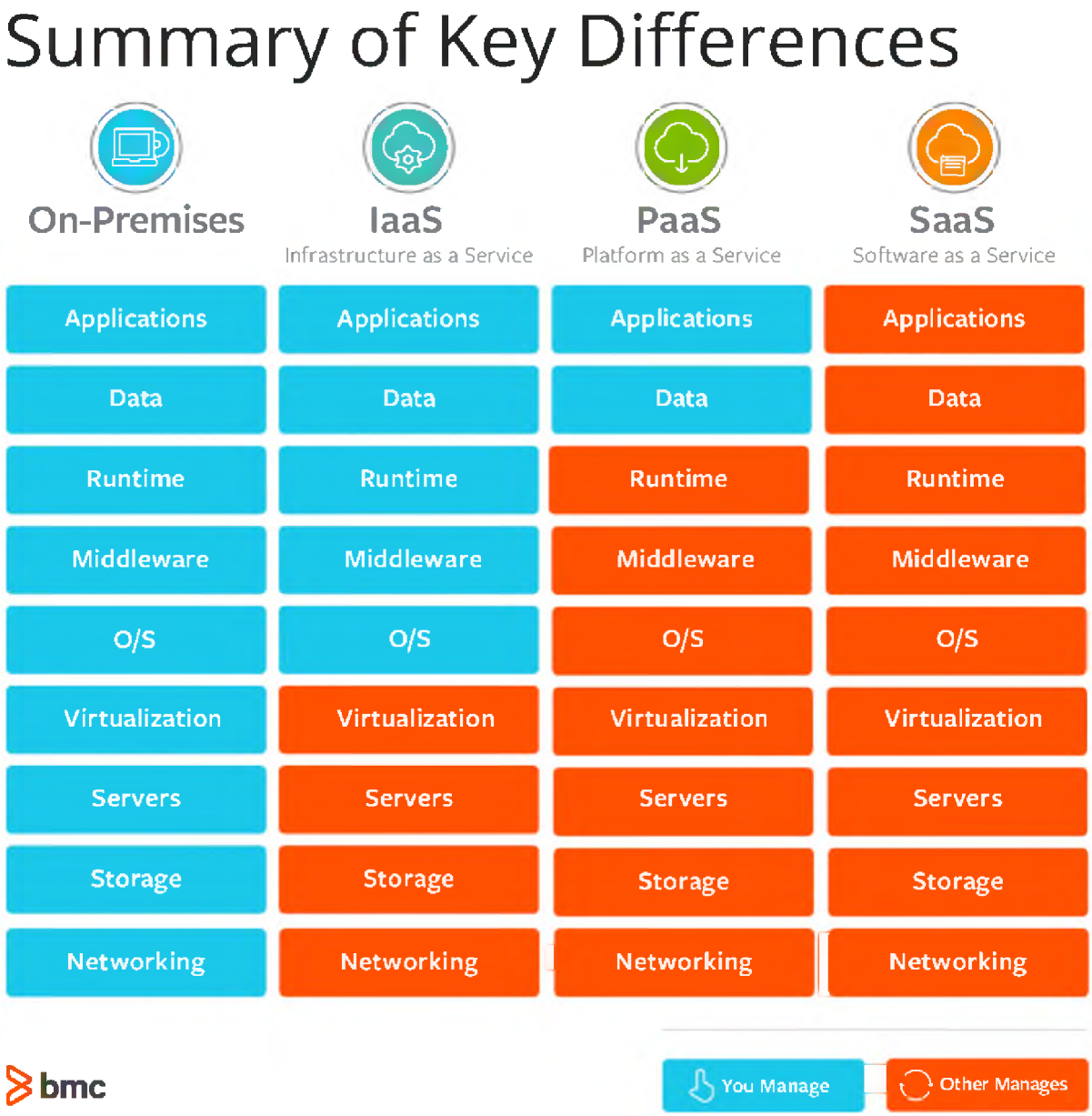

Рисунок 1.4 Порівняння ключових відмінностей розподілу відповідальності[6]

Як можна побачити, модель IaaS дає більше контролю за власними сервісами, що будуть розгорнуті всередині хмари.

По-друге необхідно порівняти який функціонал з забезпечення безпеки інформації можуть запропонувати провайдери-гіганти ринку.

Усі хмарні платформи надають можливість запускати віртуальні машини (ВМ), вибирати різні конфігурації для ВМ і вибирати клас ВМ. Диск, центральний процесор, пам'ять і операції введення/виводу в секунду
(IOPS) залежать від вибраного класу віртуальної машини.

Віртуальні машини та сховища є найбільш використовуваними сервісами на хмарній платформі. Максимальні параметри конфігурації обчислень однієї ВМ для хмарних платформ AWS та Azure та Google порівнюються в таблиці 1.4.

Таблиця 1.4 Конфігурації ВМ що пропонуються провайдерами до використання

	AWS	Azure	Google Cloud
CPU	1.6 GHz – 3.3 GHz	2.7 GHz – 3.7 GHz	2.0 GHz – 4.0 GHz
Maximum vCPUs	128	128	224
Maximum Memory	244 GB	208 GB	448 GB
Temporary Storage	48 TB	3 TB	4 TB
Maximum vGPUs	4	4	4

Також усі три хмарні платформи підтримують контейнерізацію, яка зараз надзвичайно популярна серед розробників додатків, що використовують мікросервіси. Google відіграє важливу роль у розробці Kubernetes для оркестрації контейнерів, і, як наслідок, Google Cloud Platform має гарну підтримку для контейнерів Kubernetes[7] і Docker[8]. Google Cloud Run[9] використовується для розробки та розгортання контейнерних додатків, які мають бути високомасштабованими. Amazon надає Amazon Elastic Container Registry[10], Amazon Elastic Container Service[11] та Amazon Elastic Kubernetes Service[12]. Служби контейнерів підтримують Kubernetes, контейнери Docker і служби Fargate (сервіс контейнерів Amazon

EC2)[13]. Azure має дві контейнерні служби: Azure Kubernetes Service (AKS)[14] і Azure Container Service (ACS)[15]. Для керування контейнерами використовуються Docker hub[16] і Azure Container Registry[17].

Популярність контейнерізація отримала завдяки своїм особливостям технологічним. Порівнюючи контейнери з віртуальними машинами можна зазначити перевагами наступне:

- Контейнер можна створити швидше, ніж ВМ. При цьому середовище контейнеризації для деяких завдань дає більше можливостей;
- Контейнер займає менше місця у сховищі, що зменшує накладні витрати;
- Є можливість слідкувати за версіями контейнерів, стежити за відмінностями між ними;
- Зазвичай контейнери створюються на основі відкритих стандартів. Тому з ними можна працювати у більшості дистрибутивів Linux, Microsoft, MacOS;
- Все, що відбувається всередині контейнера, залишається у контейнері. Контейнери не впливають один на одного або на операційну систему;

Хмарне сховище є ще одним важливим сервісом хмарної платформи, який широко використовується клієнтами по всьому світу. Кожна хмарна платформа надає різні типи хмарного сховища. У таблиці 1.5 наведено перелік доступних опцій для сховища у хмарі.

Таблиця 1.5 Перелік опцій для використання сховища у хмарі

Service	AWS	Azure	Google Cloud
Block Storage	Elastic Block Storage (EBS)	Azure Disk Storage	Google Persistent Disks
Object Storage	Simple Storage Service (S3)	Azure Blob Storage	Google Cloud Storage
File Storage	Elastic File System (EFS)	Azure Files	Google Cloud Files
Archive Storage	S3 Glacier Deep Archive S3 Infrequent Access	Azure Archive Storage Azure Cool Blob Storage	Google Cloud Storage Nearline, Coldline, and Archive
Bulk Data Transport	AWS Snow Family AWS Import/Export Service	Azure Data Box Azure Import/Export Service	Storage Transfer Service

Block storage (Блочне сховище) - постійний диск що є місцем сховищем для ВМ.

Object storage (Сховище об'єктів) - це сховище з функціоналом керування версіями та дозволами доступу, використовує сегменти для зберігання об'єктів.

File storage (Сховище файлів) - мережеве сховище файлів, яке використовується для зберігання, обміну та доступу до даних через мережу.

Archive storage (Архівне сховище файлів) - сервіс для створення резервних копій та збереження архівних даних

Bulk data transport (Переміщення масивних даних) - сервіс для оптимізації процесу переміщення великого об'єму даних

1.5 Особливості загроз та ризиків для віртуальних і класичних банків

Класичні банки вразливі через обмеженість наземною інфраструктурою, в якій існує можлива проблема дефіциту ресурсів, через що є ризик залишити організацію з відмовою в обслуговуванні.

Також вразливістю класичного банку є точка входу клієнта через наземну інфраструктуру.

Як приклад можна взяти нещодавній випадок одного з Українських банків, в якого виникла відмова в обслуговуванні через DDOS атаку на точку входу для клієнтів, через що сервіси відмовили в обслуговувані на декілька годин та клієнти залишились без можливості зробити хоча б якусь операцію. Це може призвести до втрати довіри до банку.

Одним з ризиків класичного банку є найм великої кількості персоналу забезпечуючого безпеку процесів.

Наприклад: Класичному банку необхідно шукати на ринку спеціаліста для налаштувать точок входу клієнтів і створення захисту для файрволу, коли необанк цю проблему нівелює хмарним сервісом, який пропонує вже готове рішення.

Класичному банку треба мати свою команду по забезпеченню обладнанням центрів для обробки і збереження даних, мати окремий відділ для налаштування резервного копіювання даних, коли необанк нівелює ці ризики використовуючи хмарові сервіси з готовими рішеннями.

Також класичний банк потребує фізичного захисту для своєї інфраструктури, за що необанк може не перейматися через те, що всі потужності хмарної

інфраструктури розкидані одразу у багатьох точках світу і складають собою один єдиний “пул” ресурсів для використання, на цій властивості додатково відпадає ризик відмови в обслуговуванні для необанка.

Хмарні сервіси завіряють у 99,9 service-level agreement (SLA), тобто ризик простою механізму і процесу необанку близиться до нуля.

Однакові ризики як для класичного так і для необанку можуть бути: DDOS-атаки, використання різноманітних систем зламу, використання вірусного програмного забезпечення, ризики технічного персоналу (наприклад, із компанії вилучається спеціаліст високого рівня, заміна якого може призвести до падіння продуктивності роботи відповідного відділу в компанії.), бекдор в програмному забезпеченні банку, комфорт персоналу (в приємній обстановці мотивація співробітника буде вища, вище продуктивність і відповідно якість продукту, за який співробітник відповідає.)

Основним джерелом ризиків для необанку є відсутність достатнього фінансування, оскільки більшу частину ризиків на себе бере вендор пропонуючий облачні сервіси організації та недостатня мотивація співробітників.

1.6 Висновок до першої частини

На сьогоднішній день хмарні технології являються дуже актуальним рішенням багатьох обчислювальних та організаційних проблем. Як можна було побачити по динамиці розвитку, все більше і більше організацій як банківських, так і будь-яких фінансових чи малого бізнесу, інтегруються у хмари через їх надійність, можливість надання безперервності роботи бізнесу та наданням надійного рівня безпеки до середовища, у якому будуть знаходитись сервіси організацій. Слід також зазначити, що через таку зміну технологій, також змінюються підходи до обробки даних, організаційні питання та інше.

Та не можна перекладати всю відповідальність за безпеку сервісів на одного провайдера. При переході у хмару для організації з’являються нові загрози та ризики, які та буде вимушена перекривати внутрішніми політиками безпеки. Не

дивлячись на всі зміни та засоби по усуненню вразливостей і загроз, всі методи повинні відповідати діючим нормативним документам.

Тому є необхідність проаналізувати для переносу фізичної інфраструктури до хмари при цьому зберігаючи відповідність стандартам безпеки та нормативним документам.

2. СПЕЦІАЛЬНА ЧАСТИНА

При вирішенні задачі з переносу треба враховувати вимоги державних нормативних документів та вимоги стандартів безпеки, такі як сімейство стандартів ISO 27000 і PCI DSS якщо ведеться мова про організацію, працюючою з платіжними картками. Також необхідно мати на увазі, що типові атаки на хмарні середовища можуть стати загрозою для будь-якого необанку.

Необхідно вибрати провайдера хмарних технологій, що може надати відповідні документи і сертифікати зазначаючі, що технології, які будуть використані, задовольняють потреби нормативних документів і політик безпеки організації для повноцінного функціонування.

2.1 Існуючі загрози хмарних обчислень

Основні з умов, які треба забезпечити при перенесені:

- Безпека від DoS/DDoS;
- Ізолювання доступу в мережі між сервісами;
- Контроль доступу користувачів до системи;
- Шифрування трафіку;
- Захист мережі;
- Можливість створення резервного копіювання;
- Надання ресурсів;

Перед початком впровадження застосунків для реалізації процесу переносу процесів класичного банку у хмару загалом, необхідно більш детально ознайомитись з можливими загрозами та ризиками при роботі у хмарі і методами їх усунення.

Контролювання 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 небезпеки, так як він пов'язаний з керованістю хмари, як з єдиною інформаційною системою і для неї загальний захист треба 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, безпека мережі в першу чергу являє собою побудову надійної моделі загроз, що включає захист від вторгнень і міжмережевий екран. Використання міжмережевого використовується з метою розмежування внутрішньої мережі ЦОД на підмережі з різним рівнем довіри. Це можуть бути окремі сервери, доступні з Інтернету або сервери із внутрішніх мереж.

2.2 Актуальні вразливості при роботі у хмарі

– Наявність віддаленого адміністрування;

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.

– Підвищення вірогідності ураження вимкнених ВМ

Коли віртуальну машину вимкнено, вона вразлива до зараження. Доступу до сховища образів віртуальних машин через мережу достатньо. На вимкненій віртуальній машині неможливо запустити захисне програмне забезпечення. У

цьому випадку повинен бути реалізований захист не тільки всередині кожної віртуальної машини, але і на рівні гіпервізора.

– Неоднорідність периметру

При використанні хмарних обчислень периметр мережі розмивається або зникає. Це призводить до того, що захист менш захищеної частини мережі визначає загальний рівень безпеки. Для розмежування сегментів з різними рівнями довіри у хмарі віртуальні машини повинні забезпечувати себе захистом, переміщуючи мережевий периметр до самої віртуальної машини. У таблиці 2.1 наведено перелік основних ризиків при використанні хмарних технологій та рекомендації щодо їх вирішення [18]

Таблиця 2.1 Ризики при роботі у хмарі та рекомендації щодо їх нейтралізації

Ризик	Характеристика	Управління
Атаки на гіпервізор	Ризик розподілу ресурсів, який може призвести до того, що одна віртуальна машина отримує несанкціонований доступ до пам'яті і ресурсів іншої віртуальної машини	Стандартизація процедур доступу до керуючих засобів хост-сервера; застосовування вбудованого брандмауера (програма, що здійснює захист комп'ютерних мереж) хоста віртуалізації
Атаки на системи управління	Ризик появи віртуальних машин-невидимок, які здатні блокувати роботу інших віртуальних машин	Застосування паролей, сертифікатів та кодів

Продовження таблиці 2.1 Ризики при роботі у хмарі та рекомендації щодо їх нейтралізації

Ризик	Характеристика	Управління
Стабільність з'єднання	Ризик погіршення (або відсутність) підключення до Інтернету	Кешування даних; розробка алгоритму переходу в режим повільного зв'язку
Залежність від постачальника (провайдера) «хмарних» технологій	Ризик відсутності можливості змінити постачальника «хмарних» технологій через відсутність на ринку інших провайдерів, коштів або часу	Ретельний підхід до вибору провайдера; робота з провайдером, який використовує відкриті стандарти
Банкрутство провайдера	Ризик зупинки надання «хмарних» рішень через банкрутство провайдера	Ретельний підхід до вибору провайдера; робота з декількома провайдерами; наявність плану дій із зміни провайдера

Продовження таблиця 2.1 Ризики при роботі у хмарі та рекомендації щодо їх нейтралізації

Ризик	Характеристика	Управління
Втрата зв'язку з провайдером	Ризик зупинки бізнес-процесів через відсутність доступу до сервісів провайдера	Вибір провайдера, що має дата-центри в декількох країнах; застосування супутникового інтернет-зв'язку; наявність резервної копії критичних систем у приватній «хмарі»
Перехоплення інформації при передачі	Ризик несанкціонованого доступу до інформації у процесі передачі даних	Використання криптографії при передачі інформації; навчання користувачів правилам інформаційної безпеки
Юридичний ризик	Ризик отримання штрафів та інших санкції з боку регулятора через порушення вимог чинного законодавства	Консультація з регулятором та зовнішніми аудиторами

Продовження таблиця 2.1 Ризики при роботі у хмарі та рекомендації щодо їх нейтралізації

Ризик	Характеристика	Управління
Втрата контролю над даними або інфраструктурою	Ризик відсутності можливості забезпечення належного рівня безпеки через втрату контроля над даними або інфраструктурою	Проведення аудиту безпеки провайдера; укладення угоди з провайдером щодо нерозголошення конфіденційних даних; моніторинг рівня сервісу та інцидентів порушення інформаційної безпеки
Неможливість знищення інформації	Ризик витоку інформації через неможливість знищення даних у «хмарних» технологіях	Шифрування даних в «хмарі»; маскування інформації; включення вимог з процедури знищення інформації в SLA (договір про рівень надання послуг)
Взлом інтерфейсів управління	Ризик шахрайства через взлом інтерфейсу управління «хмарними» технологіями	Двофакторна аутентифікація; шифрування переданих даних
DDOS-атаки	Ризик нападу на комп'ютерну систему з наміром зробити комп'ютерні	Вибір ddos-стійкого провайдера; робота з декількома провайдерами

	ресурси недоступними для користувачів	

Продовження таблиця 2.1 Ризики при роботі у хмарі та рекомендації щодо їх нейтралізації

Ризик	Характеристика	Управління
Діяльність інших користувачів «хмари»	Ризик несанкціонованого доступу до інформації та зупинка бізнес-процесів через діяльність інших користувачів «хмарних» технологій	Ретельний підхід до вибору провайдера; робота з декількома провайдерами

2.3 Рекомендації до заходів з управління ризиками

При перенесені процесів організації у хмару слід пам’ятати про розподіл ризиків організації замовника з провайдером. При використанні моделі IaaS треба зазначити, що основні ризики на себе приймає організація-замовник. В часності оновлення встановленого ПЗ у середовищі провайдера, будування архітектури додатків, налаштування коректності роботи сервісів, контроль утилізації ресурсів. Модель IaaS представляє собою видані ресурси користувачу у вигляді фізичних серверів, дискового сховища та мережеве обладнання, за котре відповідальність несе провайдер.

Організація – замовник несе відповідальність за роботу та захищенність своїх операційних систем, додатків та пов’язаних з ними даних. При тому в користувачів хмарного середовища є можливість використовувати програмні та технічні рішення провайдера для забезпечення безпеки як з точки фізичного захисту так і захисту віртуального середовища. Обраний провайдер для забезпечення необхідного рівня безпеки повинен пропонувати рішення як архітектурні так і програмні щодо

забезпечення безпеки даних всередині свої ЦОД, також не менш важливим критерієм буде наявність пройденого сертифікування за міжнародними стандартами безпеки, що може говорити про достатній рівень кваліфікації співробітників з забезпечення безпеки та налаштування інфраструктури в компанії провайдера.

2.4 Обгрунтування вибору провайдера

У першому розділі було зазначено про лідерство провайдера AWS на ринку хмарних технологій. З особливостей надання послуг слід зазначити, що AWS гарантує клієнтам контроль зберігання та доступу до інформації, що обробляється у хмарі. Пропонує автоматизовані процеси аналізу можливих загроз та вразливостей і методи їх усунення для безпечного масштабування інфраструктури організації. Окрім того, AWS гарантує шифрування всього потоку інформації на фізичному рівні всередині своїх центрів обробки даних: *"Усі дані, що протікають через глобальну мережу AWS, яка з'єднує наші центри обробки даних і регіони, автоматично шифруються на фізичному рівні, перш ніж покинуть наші захищені об'єкти."* [19] Додатковий рівень шифрування також існує наприклад у міжрегіональних VPC з'єднаннях (див. рис. 2.1)

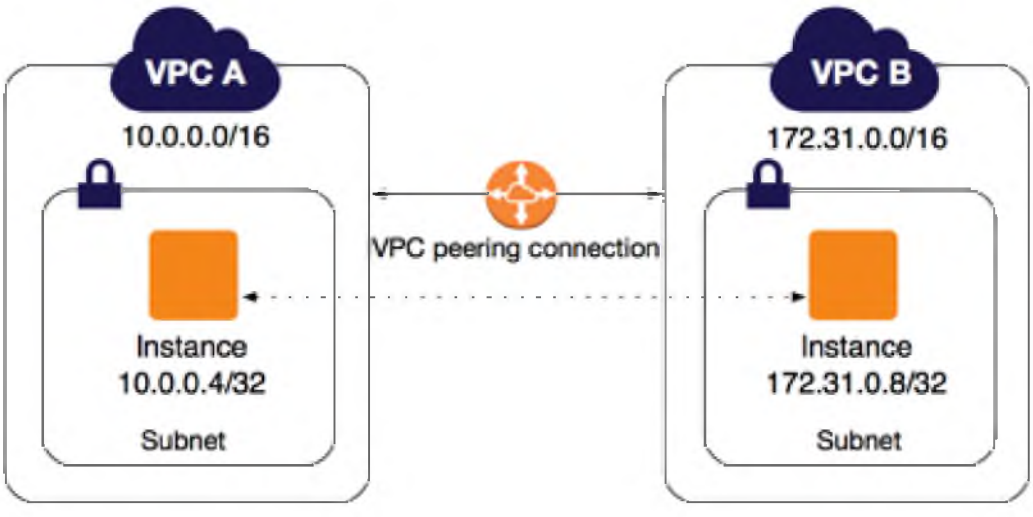

Рис 2.1 «Шифрування трафіку між розмежованими приватними мережами»

та у клієнтських service-to-service TLS з'єднаннях.

Також пропонуються засоби для шифрування клієнтської інформації самостійно за допомогою провайдерського KMS або через надання сервісу CloudHSM

для самостійного контролювання ключів шифрування що діє з використанням перевірених HSM за стандартом FIPS 140-2 [20]. AWS гарантує відповідність вимогам безпеки: *"AWS підтримує більше стандартів безпеки та сертифікатів відповідності, ніж будь-яка інша пропозиція, включаючи PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 і NIST 800-171, допомагаючи задовольнити вимоги до відповідності практично кожному регуляторному органу по всьому світу."*[20].

2.5 Обгрунтування вибору сервісів

Буде приведено перелік сервісів , для реалізації виконання потреб постанови НБУ №95 і стандарту PCI DSS при перенесені фізичної інфраструктури у хмару в реаліях Українського банку. Як відзначено вендором, всі перелічені нижче сервіси успішно пройшли сертифікацію ISO та відповідають вимогам PCI DSS.

Як було зазначено вище, AWS гарантує шифрування всіх даних на фізичному рівні, що виконує одну з вимог щодо забезпечення безпеки. Також для отримання більшого контролю за робочими станціями, всі запропоновані сервіси планується розглядати при використанні IaaS хмарної моделі (див. табл. 2.2).

Таблиця 2.2 Перелік запропонованих до впровадження сервісів

№	Сервіс	Опис	Реалізація	Сертифікація ISO	Сертифікація PCI DSS
1	AWS Elastic Load Balancing	Ефективно розподіляє мережевий трафік між віртуальними машинами.	Безпека від DoS/DDoS-атак.	+	+
2	Amazon Route 53	Створення зон та записів в DNS без керування власними DNS-	Створення тестової мережі, розмежування	+	+

		серверами та програмним забезпеченням.	доступів до продових систем.		
3	AWS Certificate Manager (ACM)	Дозволяє надавати, керувати та розгортати загальнодоступні і приватні сертифікати рівня безпечних сокетів/транспортного рівня (SSL/TLS) для використання зі службами AWS та внутрішніми підключеними ресурсами.	Надання додаткового шифрування трафіку між сервісами.	+	+
4	Amazon Virtual Private Cloud (VPC)	Надання керованості мережевих служб та додаткової ізоляції між сервісами.	Контроль доступу	+	+
5	Amazon S3 и Amazon S3 Glacier	Надання резервного копіювання будь-яких типів даних	Резервне копіювання	+	+
6	AWS EC2	Видача ресурсів та створення віртуальних серверів для виконання бізнес-процесів організації	Робочі ресурси	+	+
7	AWS EBS	Надання блочних пристроїв зберігання	Робочі ресурси	+	+

8	AWS ECS	Керування кластерами контейнерів для об’єднання їх в кластери	Розподіл ресурсів	+	+
9	AWS WAF	Захистит програм та вебсайтів від відмови в обслуговуванні та веб-атак.	Брандмауер	+	+
10	AWS CloudHSM	Апаратний модуль безпеки (HSM), який дає змогу легко створювати та використовувати власні ключі шифрування в AWS Cloud.	Шифрування даних	+	+
11	Wazuh	Збирання та аналіз даних журналів про інфраструктуру.	Ідентифікація та моніторинг усіх звернень	+	
12	OpenVAS	Неаутентифіковане та аутентифіковане тестування, реалізація будь-якого типу тестування уразливостей.	Регулярне тестування систем та процесів, пов'язаних з безпекою.	+	
13	AWS Identity and Access Management (IAM)	Авторизація користувачів	Ідентифікація та автентифікація доступу до компонентів системи.	+	

Таким чином, можна зробити висновок, що запропоновані на сьогоднішній день готові рішення хмарного провайдера та пара рішень відкритого доступу у більшій частині задовольняють вимоги постанови та стандартів безпеки. Проте деякі дані потребують більш детального вивчення перед впровадженням в систему банку.

Загалом запропонований провайдер дозволяє банківській організації бути впевненою в достатньому рівні захисту даних клієнтів як на фізичному рівні, так і у програмному середовищі.

Структурне відображення використання сервісів для переносу та початку роботи у хмарі наведено на рис 2.2

Схематичне відображення взаємодії користувача з банківськими сервісами представлено у додатку Б.

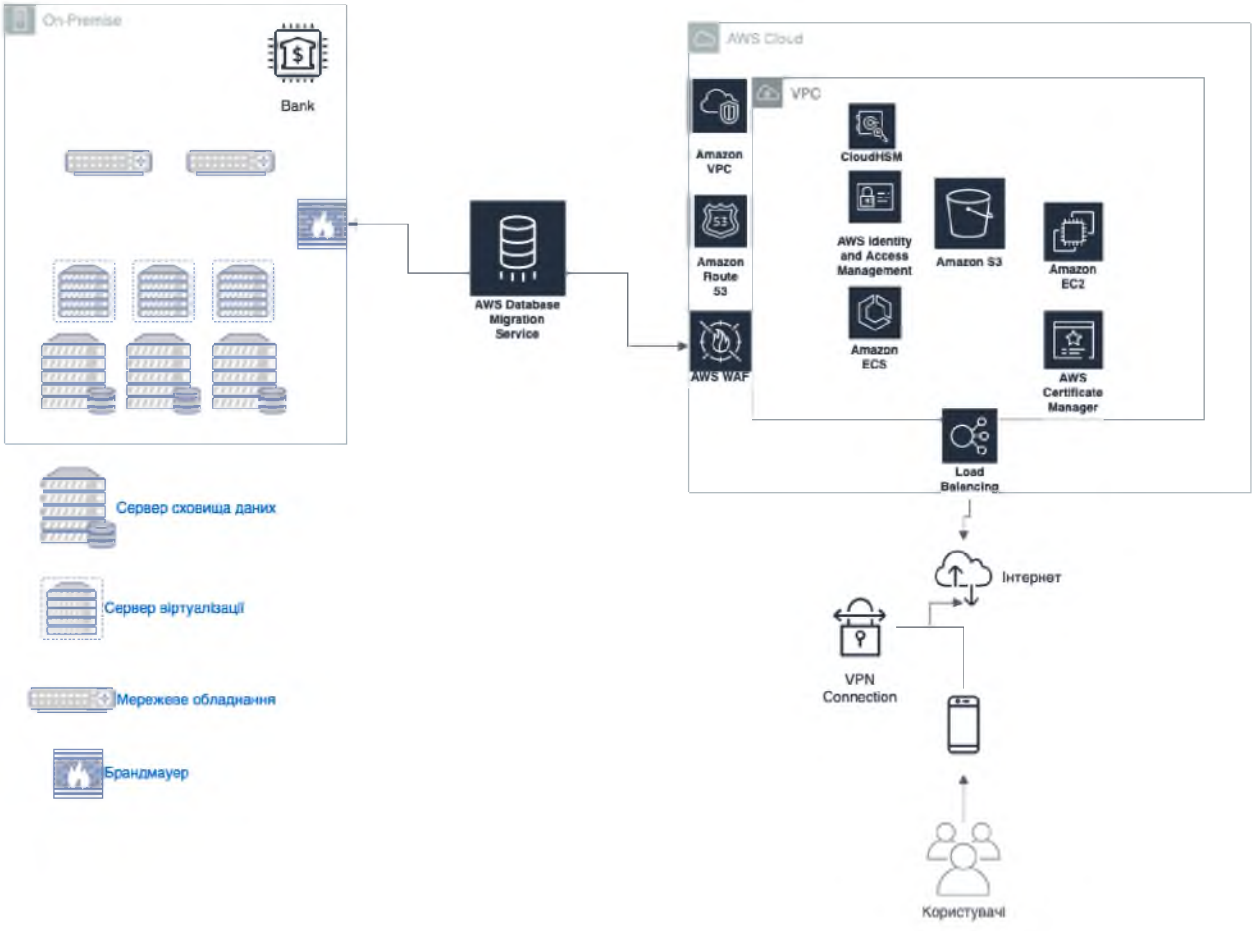

Рисунок 2.2 Схема сервісів та їх використання з боку користувачів сервісів організації як розробник/адміністратор

2.6 Висновок до другого розділу

В даному розділі були розглянуті актуальні загрози та ризики для банківських організацій, що мають намір перевести свої робочі процеси у хмарне середовище.

Надано рекомендації щодо запобігання ризикам і загрозам, пов'язаних з роботою у хмарі.

Було запропоновано використання послуг одного з надійніших провайдерів ринку, та рекомендовано сервіси провайдера, які можуть забезпечити організації відповідність стандартам, що потребуються для проведення фінансової діяльності в рамках України.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

У даному розділі кваліфікаційної роботи наводиться техніко-економічне обґрунтування(ТЕО) впровадження хмарних сервісів/технологій, які були наведені у спеціальному розділі.

Техніко-економічне обґрунтування (ТЕО) – це обов'язкова складова частина будь-якого інвестиційного проекту, тобто проекту, що потребує певних фінансових витрат. Основна мета розробки ТЕО – дати фінансову оцінку передбачуваних витрат та одержуваного корисного результату, а також оцінити прибутковість проекту і, в кінцевому підсумку, економічну доцільність його розробки та впровадження.

Для успішного проведення техніко-технічного обґрунтування необхідно виконати наступні дії:

– Виконати розрахунок капітальних витрат на придбання і налагодження програмного і апаратного забезпечення для реалізації методів, які наведені у спеціальному розділі;

– Розрахувати річні експлуатаційні витрати на утримання і обслуговування програмного та апаратного забезпечення;

– Визначити річний економічний ефект від реалізації методів захисту;

– Визначити та провести аналіз показників економічної ефективності запропонованих у спеціальному розділі методів;

– Сформулювати висновок щодо економічної доцільності обраних методів захисту смарт-контракту.

3.2 Виконання розрахунків

3.2.1 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат відносяться витрати на методи забезпечення збереження безпеки інформації при переході від фізичної інфраструктури до хмарної, які визначаються виходячи з трудомісткості впровадження цих методів.

Трудомісткість реалізації запропонованих методів визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного з спеціалістів інформаційної безпеки).

Трудомісткість визначається за наступною формулою:

$$t = tmз + tв + ta + tозб + tр + tд \qquad (3.1)$$

де *tmз* – тривалість складання технічного завдання на впровадження методів;

tв – тривалість вивчення ТЗ, літературних джерел за темою тощо;

ta – тривалість проведення аудиту запланованих до впровадження сервісів спеціалістом безпеки;

tозб – тривалість вибору основних рішень з забезпечення безпеки при переході с фізичної інфраструктуру у хмарну;

tр – тривалість реалізації впровадження;

tд – тривалість документального оформлення методів.

Визначено, що, враховуючи особливості запропонованих методів, наведені вище величини становлять: *tmз* = 48 годин, *tв* = 72 години, *ta* = 48 годин, *tозб* = 72 годин, *tp* = 168 години, *tд* = 24 години.

Відповідно,

$$t = 48+72+48+72+168+24 = 432 \text{ } годин$$

Розрахунок витрат на впровадження сервісів

При використані хмарних технологій, замовник лишає турботу за тарифи на використання і обслуговування технічного обладнання та на використання електроенергії на плечі хмарного провайдера.

Оплата сервісів AWS потребує наявності точної кількості наявних в організації ресурсів для міграції, оскільки ціна варіюється в залежності від використаних ресурсів провайдера на даний момент.

Для прикладу буде взято середню конфігурацію технічного обладнання для опрацювання невеликої кількості даних.

У таблиці 3.1 приведено ціни за використання гігабайту сховища. [21]

Таблиця 3.1 тарифи AWS за використання сервісу сховища

S3 Standart	Вартість
Перші 50 ТБ/місяць	$0.023 за гігабайт
Наступні 450 ТБ/місяць	$0.022 за гігабайт
Більш ніж 500ТБ / місяць	$0.021 за гігабайт

Розрахунок за тарифами AWS

Стандартна пам'ять S3: 120 ТБ на місяць x 1024 ГБ в ТБ = 122880 ГБ на місяць

Розрахунки цін:

Ціна для: 122880 ГБ

51200 ГБ x 0,0230000000 USD = 1177,60 USD

71680 ГБ x 0,0220000000 USD = 1576,96 USD

Загальна вартість: 1177,60 USD + 1576,96 USD = 2754,5600 USD (Стандартна вартість зберігання S3)

10 000 000 запитів PUT для S3 Storage x 0,000005 USD за запит = 50,00 USD (вартість стандартних запитів S3 PUT)

10 000 000 запитів GET на місяць x 0,0000004 USD за запит = 4,00 USD (вартість запитів S3 Standard GET)

2 754,56 USD + 4,00 USD + 50,00 USD = 2 808,56 USD

S3 Стандартна вартість (щомісячно): 2 808,56 USD

За курсом валют на момент 20.01.22 (28.33 грн) вартість впровадження сервісу для збереження/резервування даних на місяць буде складати: 2 808,56 * 28,33 = 79566,5 грн

Для виконання впровадження сервісів, потрібні розрахункові потужності

Як приклад було взято параметри на один сервер, що провайдер може виділити з характеристиками: 20 фізичних процесорів, 32 віртуальних процесори.

Розрахунок за тарифами AWS

1 одиниця x 2,218 USD на годину x 730 годин на місяць = 1619,1400 USD

Вартість виділеного хосту Amazon EC2 (щомісячно): 1619,14 USD

Для роботи EC2 хостів, їм потрібно мати місце для зберігання та опрацювання актуальної інформації та даних в реальному часі. 10 ТБ сховища з пропускною здатністю 1гб/сек на кожний логічний розділ масиву коштує за тарифом AWS:

10 240 ГБ x 1 x 0,096 USD = 983,04 USD (вартість зберігання у EBS)

Вартість EBS Storage: 983,04 USD

1000 МБ/с - 125 МБ/с безкоштовно = 875,00 МБ/с, що оплачується

875,00 Мб/с = 875,00 оплачувана пропускна здатність (МБ/с)

875,00 МБ/с / 1024 МБ на ГБ = 0,8545 оплачувана пропускна здатність (Гб/с)

0,8545 Гб/с x 1 екземпляр x 49,152 USD = 42,00 USD (вартість пропускної спроможності EBS gp3)

983,04 USD + 42,00 USD = 1 025,04 USD (Загальна вартість зберігання EBS)

Ціна Amazon Elastic Block Storage (EBS) (щомісячно): 1 025,04 USD

Вартість виділеного хосту Amazon EC2 (щомісячно) = 1619,14 USD

Ціни Amazon Elastic Block Storage (EBS) (щомісячно) = 1 025,04 USD

Загальна місячна вартість за впровадження = 2 644,18 USD

Вартість впровадження сервісу для виконання розрахунків та обробки даних на місяць буде складати: 2 644,18 * 28,33 = 74910 грн

Ціни за впровадження сервісів вказаних у розділі 2.5 наведено у таблиці 3.2 з використанням середніх конфігурацій.

Таблиця 3.2 ціна впровадження додаткових сервісів для функціонування

Назва сервісу	Ціна впровадження за місяць
AWS Elastic Load Balancing	23.36 USD = 661.8 грн
AWS Route 53	220.50 USD = 6246,8 грн
AWS WAF	~200 USD = 5666 грн
AWS VPC	~1000 USD = 28330 грн
AWS CloudHSM	1518USD = 43005 грн

Приблизна вартість впровадження:

79566,5 + 74910 + 661.8 + 6246,8 + 5666 + 28330 + 43005 = 238386,1 грн*

*Ціни змінюються в залежності від необхідної кількості ресурсів замовника

Заробітна плата виконавця/виконавців враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, тощо) і визначається за формулою:

$$Ззп = t*Зпр = 432*56,6 = 24451,2 \text{ грн} \quad (3.2)$$

де t – загальна тривалість розробки методів захисту смарт-контракту, годин;

Зпр – середньогодинна заробітна плата технічного інженера з нарахуваннями, грн/година.

Витрати на впровадження запропонованих методів *Кпз* складаються з витрат на заробітну плату виконавця *Ззп* і вартості необхідних для впровадження сервісів *Змч*:

$$Кпз = Ззп + Змч = 24451,2 + 238386,1 = 262837,2 \text{ грн} \quad (3.3)$$

Оскільки обрані сервіси від провайдера відмічені як сертифіковані продукти відповідно стандартів ISO 27001 та PCI DSS, додаткові витрати на аудит не потребуються.

Капітальні витрати на впровадження сервісів для збереження рівня безпеки інформації організації становитиме:

$$*К = Кпз = 262837,2 \quad (3.4)$$

*Оскільки забезпечення електроживлення та обслуговування технічного обладнання не лежить на плечах замовника хмарного середовища.

3.2.2 Розрахунок річних експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об‘єкта проектування за календарний рік, визначений у грошовій формі.

До поточних витрат відносяться наступні витрати:

– вартість Upgrade-відновлення й модернізації системи(*Св*);

– витрати на керування системою(*Ск*);

– витрати, викликані активністю користувачів системи(*Сак*).

Під «витратами на керуванням системою» маються на увазі витрати, пов’язані з керуванням і адмініструванням серверів та інших компонентів системи. До цієї статті витрат відносяться наступні витрати:

– навчання адміністративного персоналу й кінцевих користувачів;

– амортизаційні відрахування від вартості обладнання та ПЗ;

– заробітна плата обслуговуючого персоналу;

– аутсорсинг;

– навчальні курси та сертифікація обслуговуючого персоналу;

– технічне й організаційне адміністрування й сервіс

Через особливості використання хмарних технологій, витрати на підтримку працездатності сервісів будуть складатись лише з оплати щомісячного тарифу та адміністрування сервісів зсередини командами IT відділів організації.

Отже витрати на керування проектом протягом одного року складати

$$Ск = Кпз * 12 = 262837,2 * 12 = 3154046,4 \text{ грн} \quad (3.5)$$

Таким чином, річні поточні витрати банківської організації на функціонування хмарної інфраструктури для своїх сервісів та процесів складатиме 3154046,4 грн.

3.2.3 Визначення річного економічного ефекту

Кінцевим результатом впровадження заходів щодо забезпечення безпеки інформації є величина відвернених втрат, що розраховується виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього.

В даному випадку, при використані хмарного простору, при успішній атаці на хмарного провайдера чи при тимчасовій відмові в обслуговуванні сервісів провайдера, вся банківська система зупинить свої процеси, що приведе до величезних збитків та втраті іміджу компанії.

Величина можливих збитків компанії визначається за формулою:

$$B = \Sigma_i \Sigma_n \text{U} \text{ грн}, \quad (3.6)$$

де i – кількість вузлів, n – кількість атак, U – упущена вигода простою

$$U = П_п + П_в + V, \quad (3.7)$$

де Пп – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\Sigma Зс}{F} * t_п , \quad (3.8)$$

Де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 год).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} , \quad (3.9)$$

Де Пви – витрати на повторне уведення інформації, грн;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітньої плати співробітників атакованого вузла або сегмента

корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:ё

$$П_{ви} = \frac{ΣЗс}{F} * t_{ви} , \quad (3.10)$$

Витрати на відновлення вузла або сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки tв і розміром середньогодинної заробітньої плати обслуговуючого персоналу (адміністраторів)

$$Ппв = \frac{ΣЗо}{F} * t_{в} , \quad (3.11)$$

Витрати від зниження очікуванного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} * (t_{п} + t_{в} + t_{ви}) , \quad (3.12)$$

де Fг – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Отже, Пп = (24451,2 * 2 / 176) * 24 = 6668,5 грн;

Пви = (24451,2 * 2 / 176) * 4 = 1111,4 грн;

Ппв = (24451,2 * 2/ 176) * 2 = 555,7 грн;

V = (15000000/2080) * $(t_{п} + t_{в} + t_{ви})$ = 216346,2 грн;

Пв = 1111,4 + 555,7 = 1667,1 грн

U = 6668,5 + 1667,1 + 216346,2 = 224681,8 грн

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = 10 * 12 * 224681,8 = 26961816 \text{ грн.}$$

Загальний ефект від впровадження сервісів для збереження безпеки даних:

$$E = B * R - C, \text{ грн} \quad (3.13)$$

Де B – загальний збиток від реалізації атаки на хмаровий сервіс, грн;

R – вірогідність успішної реалізації атаки на сервіс (R = 20%);

C – щорічні витрати на експлуатацію системи

Загальний ефект від реалізації складає:

$$E = 26961816 * 0,2 - 3154046,4 = 2238317 \text{ грн}$$

3.2.4 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи:

$$ROSI = \frac{E}{K}, \text{ частки одиниці} \quad (3.14)$$

де E – загальний ефект від реалізації захисних методів, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI дорівнює:

$$ROSI = \frac{2238317}{262837,2} = 8,5 \text{ частки одиниці}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (Nдеп – Nінф) / 100 \quad (3.15)$$

Де Nдеп – річна депозитна ставка (11%);

Nінф – річний рівень інфляції (10%)

Розрахункове значення коефіцієнта повернення інвестицій:

$$8,5 > (11 - 10) / 100 = 8,5 > 0,01$$

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від реалізації впровадження хмарних сервісів на заміну існуючих фізичних серверів компанії:

$$То = \frac{К}{Е} = \frac{1}{ROSI} = \frac{1}{8,5} = 0,1 \text{ роки} \quad (3.16)$$

3.3 Висновок третього розділу

При проведенні техніко-технічного обґрунтування було визначено, що розмір капітальних витрат на впровадження сервісів для переходу фізичної інфраструктури у хмару складає 262837,2 грн, річні поточні витрати на функціонування системи складають 3154046,4 грн.

Впровадження сервісів є економічно доцільним, оскільки коефіцієнт повернення інвестицій складає 8,5 грн/грн, що означає отримання 8,5 грн економічного ефекту на кожну гривню капітальних вкладень на впровадження сервісів хмарних технологій, термін окупности при цьому складатиме 0,1 роки (приблизно 36 днів).

Розрахунки в даному розділі були виконані відповідно до методичних вказівок [22]

ВИСНОВОК

Можна сказати, що на даному етапі існування хмарних технологій, перехід до їх використання майже необхідний, оскільки все більше компаній застосовують такий підхід до опрацювання даних. Хмарні технології надають достатній рівень безпеки, майже нескінчену можливість до динамічного масштабування ресурсів організації.

Також вони мають в наявності готові рішення для запобігання багатої кількості атак, та попри все перелічене, хмарні технології не можуть запропонувати захист від людського фактору, який може послугувати причиною як неправильно сконфігурованого взаємозв'язку між сервісами, так і недостатньо надійно налаштованого мережевого захисту в приватній мережі. Хмарні технології можуть допомагати організаціям зменшити ризик допустити помилки як організаційні, так і технічні, надаючи ті самі готові рішення.

В Україні, нажаль, досить мала частка компаній згодна повністю переходити у хмари через доволі високу ціну за використання послугами та не дуже прогресивну нормативну законодавчу базу, що не дозволяє використовувати хмарні технології в будь-яких цілях компаній.

Та все одно технологія дуже швидко розвивається і є надія на те, що Україна зможе подолати законодавчі питання з організації та експлуатації хмар як у приватних організаціях країни, так і у державних.

Таким чином в роботі було обгрунтовано актуальність необанкінгу, актуальність використання хмарних технологій, проаналізовано актуальні ризики та загрози при роботі у хмарі.

Було сформовано рекомендації щодо впровадження сервісів хмарного провайдера, обгрунтовано вибір хмарного провайдера та розраховано економічну доцільність впровадження рекомендованих методів для збереження достійного рівня забезпечення безпеки даних клієнтів організації при переході у хмару.

ПЕРЕЛІК ПОСИЛАНЬ

1. Nebanks made in Ukraine URL: https://blog.liga.net/user/yubarabash/article/42329

2. Кількість необанків у світі прагне до 300 URL: https://minfin.com.ua/ua/2020/12/24/57548026/
3. Розвиток банківського бізнесу в умовах цифрової економіки URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/83574/1/Krukhmal_neobank.pdf;jsessionid=4CFF805DF2A5CE673A453B50C53E805D
4. Incremental growth in cloud URL: https://www.srgresearch.com/articles/incremental-growth-cloud-spending-hits-new-high-while-amazon-and-microsoft-maintain-clear-lead-reno-nv-february-4-2020
5. What is cloud computing URL: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/.
6. Types of cloud computing URL: https://aws.amazon.com/types-of-cloud-computing/
7. Production-Grade Container Orchestration URL: https://kubernetes.io/
8. Docker URL: https://www.docker.com/
9. Cloud Run URL: https://cloud.google.com/run/
10. Amazon Elastic Container Registry URL: https://aws.amazon.com/ecr/
11. Amazon Container Service URL: https://aws.amazon.com/ecs/
12. Amazon Elastic Kubernetes Service URL: https://aws.amazon.com/eks/
13. AWS Fargate URL: https://aws.amazon.com/fargate/
14. Azure Kubernetes Service URL: https://azure.microsoft.com/en-us/services/kubernetes-service/
15. Container Services URL: https://azure.microsoft.com/en-us/product-categories/containers/
16. Docker Hub URL: https://hub.docker.com/
17. Azure Container Registry URL: https://azure.microsoft.com/en-us/services/container-registry/
18. Наукова стаття *Управління ризиками «Хмарних» технологій у системі ризик-менеджменту банку* текст наукової статті з спеціальності «*Економіка і бізнес*» (Бобиль В.В.)

19.AWS Cloud Security URL:https://aws.amazon.com/security/?nc1=f_cc

20.FIPS 140-2 Security Requirements for Cryptographic Modules URL: https://csrc.nist.gov/publications/detail/fips/140/2/final

21.AWS Calculator URL: https://calculator.aws/#/createCalculator/S3

22. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Уппорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі.	23	
6	А4	Спеціальна частина.	12	
7	А4	Економічний розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	2	

ДОДАТОК Б. Схематичне відображення використання сервісами зі сторони клієнта банківським додатком.

ДОДАТОК В. Відгук

Відгук
на кваліфікаційну роботу магістра на тему:
«Методологія забезпечення кібербезпеки у віртуальних банківських системах»
студента групи 125м-20-2
Наумовця Сергія Кириловича

Мета роботи – розробка рекомендацій із забезпечення виконання вимог з кібербезпеки для віртуальних банківських систем.

Тема роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – обґрунтовувння використання, впровадження та аналізу кращих світових стандартів, практик з метою розв'язання складних задач в галузі інформаційної безпеки та/або кібербезпеки.

Задачі роботи (обґрунтування актуальності роботи, аналіз основних законодавчих та нормативних актів, що регламентують захист інформації в банківських системах, аналіз актуальних загроз та ризиків, аналіз типових структур віртуальних банківських систем, формування та формалізація вимог до розробки, обґрунтування вибору методів реалізації кібербезпеки) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність запропонованих рішень полягає у їх адаптованості до вимог як національних так і міжнародних законодавчих та нормативних документів в сфері банківської діяльності.

Практичне значення результатів проектування полягає в можливості забезпечення вимог чинних нормативних документів із використанням технічних рішень, які є доступними на ринку «хмарних» технологій.

До недоліків дипломної роботи відносяться:

– недостатньо структуровано наведений аналіз актуальних загроз для віртуальних банківських систем;
– не в повному обсязі виконана формалізація вимог до розробки;

– недостатньо обґрунтовані правові аспекти передачі ризиків на провайдера послуг;

– відсутність даних про практичну перевірку ефективності запропонованих рішень.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог положення про систему виявлення та запобіганню плагіату.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Наумовець С.К. виявив себе фахівцем, здатним самостійно, на достатньо високому рівні вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи магістра, заслуговує оцінки “добре”, а Наумовець С.К. присвоєння йому кваліфікації магістр з кібербезпеки, освітньо-професійна програма «Кібербезпека».

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.т.н., професор _____ В.І. Корнієнко