Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА
## Пояснювальна записка

*другий (магістерський)*
(рівень вищої освіти)
Дослідження інфокомунікаційних складових платіжних систем
(тема)

Виконав: студент 2 курсу, групи *ІМЗзм-19-2*
*Дерев'янко В.В.*
(прізвище, ініціали)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-науковий*
Освітня програма *Інформаційні мережі зв'язку*

Керівник *к.т.н., доц. Золотарьов В.А.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *проф. Безрук В.М.*
(підпис) (прізвище, ініціали)

2021 p.

Не містить відомостей, заборонених до відкритого публікування

Студент_____ Дерев’янко В.В.

Керівник_____ Золотарьов В.А.

Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
Тип програми *освітньо-наукова*
Освітня програма *Інформаційні мережі зв'язку*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«25» березня 2021 р.

# ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Дерев'янку Володимиру Віталійовичу
(прізвище, ім'я, по батькові)

1.Тема роботи: *Дослідження інфокомунікаційних складових платіжних систем*
затверджена наказом по університету від 25 *березня* 2021 р. № *33 стз*
2. Термін подання студентом роботи до екзаменаційної комісії *16 травня 2021* р.
3. Вихідні дані до роботи: *Об'єкт дослідження – інфокомунікаційна система платіжної банківської системи. Дослідити: основні засади функціонування ЕПС, сучасні АІБС, хмарні технології; сервіси хмарної інфраструктури платіжних систем; хмарне середовище для обміну даними; обліково-операційні хмарні сервіси; управління платежами у хмарах; шаблонні додатки на основі розподілених реєстрів; RegTech-сервіси; можливості хмари з надання фінансових послуг; торгові додатки хмарних послуг; інформаційні ризики платіжним системах у хмарах. Провести SWOT аналіз Інтернет банкінгу. Розробити модель платформи хмарних технологій для Інтернет-банкінгу. Дослідити можливості хмарних сервісів із захисту паролів, проаналізувати найкращі менеджери паролів 2021 р. за платформами, браузерами, алгоритмами шифрування, складені вимоги для вибору менеджерів паролів. Виявити найнебезпечніші кібератаки на платіжні системи, розташованих у хмарах*

4. Перелік питань, що потрібно опрацювати в роботі: *Перелік умовних скорочень. Вступ. 1. Дослідження основних засад функціонування платіжних систем в Україні. 2. Дослідження інфокомунікаційних банківських платіжних систем. 3. Дослідження особливостей застосування хмарних технологій у платіжних системах. 4. Дослідження інформаційних ризиків платіжним системам у хмарних технологіях Висновки. Перелік використаних джерел. Додаток А: слайди презентації*

5. Перелік графічного матеріалу із зазначенням комп'ютерних ілюстрацій (слайдів)

Слайди у форматі Power Point: *мета роботи; ключові елементи платіжної інфраструктури України, основні блоки платіжних систем, SWOT аналіз Інтернет банкінгу; порівняння можливостей хмарних технологій; найкращі менеджери паролів; E cloud; Визначення найнебезпечніших атак на платіжні системи в хмарах*

6. Консультанти розділів роботи

| Найменування розділу | Консультант (посада, прізвище, ім'я, по батькові) | Позначка консультанта про виконання розділу | |
|---|---|---|---|
| | | підпис | дата |
| *Основна* | *доц. Золотарьов В.А.* | | |

**КАЛЕНДАРНИЙ ПЛАН**

| № | Назва етапів роботи | Терміни виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | *Ознайомлення із завданням. Уточнення ТЗ.* | 26.03.2021 | |
| 2 | *Аналіз завдання та літературних джерел.* | 01.04.2021 | |
| 3 | *Написання першого розділу* | 08.04.2021. | |
| 4 | *Написання другого розділу* | 15.04.2021 | |
| 5 | *Написання третього розділу* | 28.04.2021 | |
| 6 | *Написання четвертого розділу* | 08.05.2021 | |
| 7 | *Написання вступу та висновків* | 11.05.2021 | |
| 8 | *Оформлення презентаційного матеріалу та підготовка до захисту у ДЕК* | 12.05.2021 | |

Дата видачі завдання 25 березня 2021 р.

Студент_____ Дерев'янко В.В.
(підпис) (прізвище, ініціали)

Керівник роботи_____ к.т.н., доц. Золотарьов В.А.
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 94 сторінок, 20 рисунків, 22 таблиць, 74 джерел, 1 додаток

ПЛАТІЖНА СИСТЕМА, АВТОМАТИЗОВАНА БАНКІВСЬКА СИСТЕМА, ХМАРНІ ТЕХНОЛОГІЇ, КІБЕРАТАКИ, МЕНЕДЖЕРИ ПАРОЛІВ

Об'єкт дослідження – інфокомунікаційна мережа платіжної системи.

Мета роботи – аналіз інфокомунікаційних складових сучасних платіжних систем;

Досліджені основні тенденції розвитку інфокомунікацій у складі платіжних та банківських систем. Сервіси хмарної інфраструктури платіжних систем.

Проаналізовані менеджери паролів хмарних систем, Визначені найнебезпечніші кібератаки на платіжні системи у хмарах.

# ABSTRACT

Explanatory note: 94 pages, 20 figures, 22 tables, 74 sources, 1 appendix

PAYMENT SYSTEM, AUTOMATED BANKING SYSTEM, CLOUD TECHNOLOGIES, CYBER ATTACKS, PASSWORD MANAGERS

The object of study - the telecommunication network of the payment system. The purpose of the work - analysis of telecommunication components of modern payment systems;
The main trends in the development of telecommunications in the payment and banking systems are studied. Cloud infrastructure services of payment systems. Analyzed password managers of cloud systems, identified the most dangerous cyber attacks on payment systems in the cloud.

ЗМІСТ


| | | |
|---|---|---|
| ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ | | 9 |
| ВСТУ | | 1 |
| П | | 1 |
| 1 | ДОСЛІДЖЕННЯ ОСНОВНИХ ЗАСАД ФУНКЦІОНУВАННЯ ПЛАТІЖНИХ СИСТЕМ В УКРАЇНІ | 1<br>3 |
| 2 | ДОСЛІДЖЕННЯ ІНФОКОМУНІКАЦІЙНИХ БАНКІВСЬКІХ ПЛАТІЖНИХ СИСТЕМ | 2<br>1 |
| 2.1 | Банківська автоматизована інформаційна система | 2<br>1 |
| 2.2 | Узагальнена структура БАІС | 2<br>4 |
| 2.3 | Дослідження ролі Інтернет-банкінгу в розвитку платіжних систем | 2<br>9 |
| 2.4 | Передумови використання банками хмарних технологій | 3<br>1 |
| 3 | ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У ПЛАТІЖНИХ СИСТЕМАХ | 3<br>3 |
| 3.1 | Поняття хмарних технологій та опис підходів до їхнього застосування | 3<br>3 |
| 3.1.1 | Інфраструктура як послуга (IaaS) | 3<br>3 |
| 3.1.1.1 | Поширені бізнес-сценарії IaaS | 3<br>4 |
| 3.1.1.2 | Переваги IaaS | 3<br>5 |
| 3.1.2 | Платформа як послуга (PaaS) | 3<br>6 |
| 3.1.2.1 | Поширені сценарії PaaS | 3<br>7 |
| 3.1.2.2 | Поширені сценарії PaaS | 3<br>7 |
| 3.1.3 | Програмне забезпечення як послуга: SaaS (Software as a Service) | 3<br>8 |
| 3.1.4 | Бізнес як сервіс BaaS (Bank / Business as a Service) | 3<br>8 |
| 3.2 | Сервіси хмарної інфраструктури платіжних систем | 4<br>2 |
| 3.2.1 | Інфраструктурні послуги | 4<br>2 |
| 3.2.2 | Інформаційна безпека як послуга | 4 |

| | | |
|---|---|---|
| 3.2.3 | Захист платежів | 350 |
| 3.3 | Хмарне середовище для обміну даними | 51 |
| 3.4, 3.5 | Обліково-операційні сервіси в хмарних технологіях | 56 |
| 3.5, 3.6 | Керування платежами у хмарах | 56 |
| 3.6, 3.8 | Шаблонні додатки на основі технології розподілених реєстрів | 58 |
| 3.7 | RegTech-сервіси | 58 |
| 3.8 | Хмара як супермаркет фінансових послуг | 61 |
| 3.9 | Торгова площадка хмарних послуг | 62 |
| 4 | ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ ПЛАТІЖНИМ СИСТЕМАМ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ | 64 |
| 4.1 | Інформаційні ризики хмарних технологій | 64 |
| 4.1.1 | Неправильна конфігурація параметрів безпеки | 64 |
| 4.1.2 | Відмова в обслуговуванні | 65 |
| 4.1.3 | Витік даних | 65 |
| 4.1.4 | Злом акаунтів | 66 |
| 4.1.5 | Небезпечні API-інтерфейси | 66 |
| 4.1.6 | Шкідливі програми | 66 |
| 4.1.7 | Крос-хмарні атаки | 67 |
| 4.1.8 | Атака по боковому каналу | 67 |
| 4.1.9 | Незаконне використання обчислювальних ресурсів | 67 |

4.2 Визначення найнебезпечніших атак на платіжні системи в хмарах 68
ВИСНОВКИ 74
ПЕРЕЛІК ПОСИЛАНЬ 75
Додаток «А» Слайди презентації 84

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АБС – автоматизована банківська система
АІС – автоматизована інформаційна система
АРМ – автоматизоване робоче місце
АТ – акціонерне товариство
БД – база даних
ЄБС – єдина біометрична система
ЄС - євросоюз
ЕД – електронні документи
ЕП – електронний платіж
ЕПД – електронні платіжні документи
ЕПС – електронна платіжна система
ІБ – інформаційна безпека
ІС – інформаційна система
ЗІ – захист інформації
ЗУ – Закон України
НБУ – Національний Банк України
НСД – несанкціонований доступ
ОБД – операційний день банку
ОС – операційна система
ПЗ – програмне забезпечення
ПК – персональний комп’ютер
ППД – паперові платіжні документи
ПТК – програмно-технічний комплекс
ПрАТ – приватне акціонерне товариство
СЕП – система електронних платежів
СЗІ – система захисту інформації
СЗД – система зберігання даних
СУБД – система управління базою даних
ТОВ – товариство з обмеженою відповідальністю
ФАРМ – функціональне автоматизоване робоче місце
API - *Application Programming Interface – прикладний програмний інтерфейс*

BaaS - Bank / Business as a Service - Бізнес як сервіс

IaaS - Infrastructure as a service - Інфраструктура як послуга

HDD – шпиндельний магнітний диск

KYC - Know Your Client - ідентифікація користувачів

PaaS - Platform as a service - Платформа як послуга

PCI DSS - Payment Card Industry Data Security Standard - Стандарт безпеки даних індустрії платіжних карток

SaaS - Software as a Service - Програмне забезпечення як послуга:

SWIFT - Society for Worldwide Interbank Financial Telecommunications, - *Товариство всесвітніх міжбанківських фінансових телекомунікацій*

VDC – віртуальний дата центр

# ВСТУП

Раціональна організація роботи платіжних систем сприяє безперебійному функціонуванню фінансового сектору країни у цілому і прискорює здійснення платежів у міжнародних і національних напрямках. Надійні й ефективні платіжні системи є гарантією стабільного функціонування як банківської системи країни, так і економіки у цілому. Крім того, за допомогою окремих платіжних систем здійснюються значні обсяги переказів коштів, тому порушення в їхній роботі можуть викликати системні ризики і негативно позначитися не тільки на фінансовій стабільності, а й у цілому на економічній безпеці держави. Саме тому поступовий та стабільний розвиток, контролювання та регулювання цієї сфери діяльності мають бути у фокусі уваги уряду нашої країни [74].

У першому розділі атестаційної роботи розглянуті основні принципи функціонування платіжних систем в Україні, перераховані основні нормативно-правові документи, які забезпечують їхню діяльність. Наведено: класифікацію платіжних систем за важливістю для держави та ключові елементи платіжної інфраструктури України; виділені основні блоки платіжних систем. З'ясовані основні переваги впровадження безготівкових розрахунків для різних об'єктів і суб'єктів господарської діяльності.

Головною складовою платіжних систем є автоматизовані банківські системи, тому у другому розділі атестаційної роботи висвітлені особливості застосування інфокомунікаційних систем в банківській діяльності. З'ясовані базові принципи застосування інформаційних технологій в банківських системах, досліджено склад забезпечувальної частини банківської АІС, наведено структуру АІС комерційного банку та описано її функціональну частину. Докладно описані задачі, що покладаються на модулі автоматизованої банківської системи та встановлені функціональні зв'язки між ними. Особлива увага приділена дослідженню Інтернет-банкінгу в платіжних системах, проведено його SWOT аналіз. З'ясовані передумови застосування в банках хмарних обчислень.

Використання хмарних технологій є головним трендом у розвитку сучасних платіжних систем. У третьому розділі атестаційної роботи були

досліджені сучасні хмарні технології за єдиною схемою: бізнес-сценарії та переваги застосування. Складено проект платформи з застосуванням хмарних технологій для Інтернет-банкінгу. Проаналізовані та докладно описані сервіси хмарної інфраструктури платіжних систем: інфраструктурні послуги; послуги безпечного доступу; алгоритми захисту платежів; хмарне середовище обміну даними. Досліджені можливості хмарних сервісів із захисту паролів, проаналізовані 9 топ менеджерів паролів 2021 р. за платформами, браузерами, алгоритмами шифрування, складені вимоги для вибору менеджерів паролів. Докладно описані можливості E-Cloud та описана його структура.

У четвертому розділі описані основні вразливості хмарних технологій, проаналізовані 10 найпопулярніших кібератак на хмари,

# 1 ДОСЛІДЖЕННЯ ОСНОВНИХ ЗАСАД ФУНКЦІОНУВАННЯ ПЛАТІЖНИХ СИСТЕМ В УКРАЇНІ

Згідно з статтею 1.29 Закону України «Про платіжні системи та переказ коштів в Україні» « платіжна система - платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. Проведення переказу коштів є обов'язковою функцією, що має виконувати платіжна система» [2]. Це визначення не редагувалося з 2001 р., тому сьогодні фахівці з права трактують платіжну систему в широкому та вузькому смислі [17].

Таблиця 1.1 – Трактування терміну «Платіжна система»

| Платіжна в широкому смислі | Платіжна система в узькому смислі |
|---|---|
| це сукупність інституційно-правових та інфраструктурних елементів, платіжних інструментів, договірних відносин і законодавчих норм, основне призначення яких полягає у реалізації інтересів суб'єктів господарського і цивільного обігу шляхом забезпечення організації та здійснення діяльності з надання платіжних послуг крізь призму виконання таких функцій, як:<br>1) формування умов для здійснення операцій з переказу коштів;<br>2) формування умов для здійснення учасниками платіжних систем діяльності з надання платіжних послуг та інших видів діяльності в межах платіжних систем;<br>3) задоволення потреб користувачів платіжних систем у наданні та реалізації відповідних платіжних послуг | це одна зі складових частин фінансово-кредитної системи держави, яка являє собою впорядковану,<br><br>законодавчо регульовану сукупність окремих платіжних систем, організацій, що забезпечують постійний рух коштів та сприяють реалізації цілей грошово-кредитної політики центрального банку |

Сьогодні виділяють шість основних вимог, яким мають задовольняти сучасні платіжні системи (рис.1.1)


Рисунок 1.1 – Вимоги до сучасних платіжних систем

Основними нормативно-правовими документами функціонування платіжної системи в нашій країні є Закони України "Про Національний банк України" [1], "Про платіжні системи та переказ коштів в Україні" [2], "Про захист інформації в інформаційно-телекомунікаційних системах" [3], "Про інформацію"[4], "Про електронні документи та електронний документообіг" [5], "Про основні засади забезпечення кібербезпеки України" [6], "Про електронні довірчі послуги" [7], Указ Президента України від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [8], проєкт постанови правління НБУ «Про затвердження Положення про захист інформації та кіберзахист в платіжних системах» [9].

Національний банк створив державну систему електронних платежів - СЕП - для забезпечення розрахунків банків та їх клієнтів у гривні в межах України. Національний банк є платіжною організацією та розрахунковим банком СЕП. СЕП забезпечує високий рівень безпеки і надійності переказу коштів між банками. СЕП обслуговує 96% міжбанківських платежів у державі, тому вона визнана системно важливою платіжною системою України. СЕП належить до системи валових розрахунків у режимі реального часу (за міжнародною класифікацією – RTGS). СЕП дає змогу відправляти платежі в одному з двох режимів: реального часу і файловому. В режимі реального часу кошти потрапляють на рахунок банка-отримувача миттєво; у файловому режимі час проходження платежу від банка-відправника до банка-отримувача в середньому складає від 10 до 20 хвилин. Учасниками СЕП є Національний банк, банки України та Державна

казначейська служба України. У середньому в день СЕП обробляє 1,5 млн платежів на суму близько 173 млрд грн. Проте потенціал СЕП значно більший - запас пропускної спроможності СЕП дозволяє щоденно обробити практично у 10 разів більше документів, ніж теперішні обсяги [22].


Рисунок 1.2 – СЕП НБУ

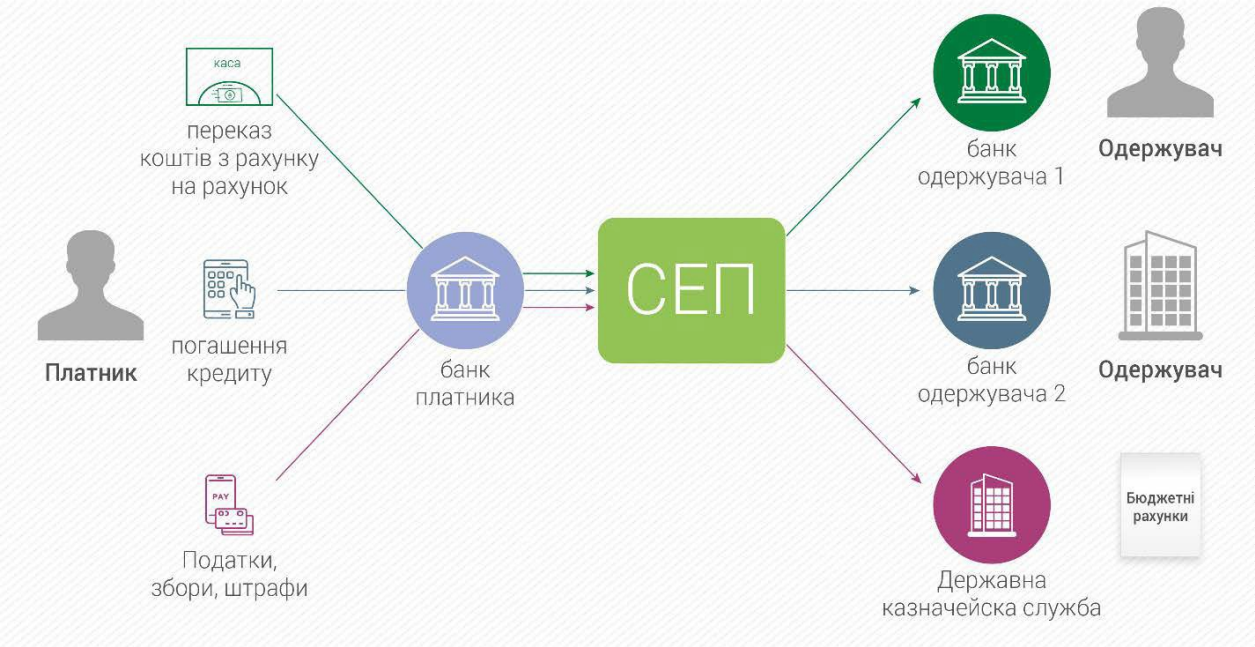


Рисунок 1.3 – Дорожня карта платежу

Розподіл платіжних систем за категоріями важливості здійснюється регулятором згідно з міжнародною практикою для приведення діяльності значущих платіжних систем, які займають значну частку на ринку, у відповідність до міжнародних стандартів оверсайта [18]

Таблиця 1.2 – Важливість платіжних систем

| | |
|---|---|
| Системно важливі | 1) платіжна система забезпечує проведення міжбанківських переказів, частка яких становить більше ніж 10% від загальної суми переказів, виконаних у країні системами міжбанківських розрахунків та через кореспондентські рахунки банків, відкриті в інших банках України;<br>2) платіжна система здійснює перекази коштів за правочинами з державними цінними паперами на відкритому ринку;<br>3) платіжна система забезпечує врегулювання зобов'язань учасників, які виникають в інших платіжних системах |
| Соціально важливі | 1) платіжна система здійснює внутрішньодержавні перекази коштів та транскордонні перекази коштів, частка яких перевищує 10% від загальної суми переказів, виконаних системами переказу коштів, створених резидентами та нерезидентами;<br>2) платіжна система здійснює операції з використанням електронних платіжних засобів, частка яких перевищує 10% від загальної суми операцій, виконаних системами роздрібних платежів на території України |
| Важливі | 1) платіжна система забезпечує проведення міжбанківських переказів, частка яких становить від 5 до 10% від загальної суми переказів, виконаних у країні системами міжбанківських розрахунків та через кореспондентські рахунки банків, відкриті в інших банках України;<br>2) платіжна система здійснює внутрішньодержавні перекази коштів та транскордонні перекази коштів, частка яких становить від 5 до 10% від загальної суми переказів, виконаних системами переказу коштів, створеними резидентами та нерезидентами;<br>3) платіжна система здійснює операції з використанням електронних платіжних засобів, частка яких становить від 5 до 10% від загальної суми операцій, виконаних системами роздрібних платежів на території України;<br>4) платіжна система здійснює внутрішньодержавні перекази коштів, частка яких становить більше ніж 5% від загальної суми внутрішньодержавних переказів коштів, виконаних системами переказу коштів, створеними резидентами та нерезидентами;<br>5) платіжна система здійснює транскордонні перекази коштів, частка яких становить більше ніж 5% від загальної суми транскордонних переказів, виконаних системами переказу коштів, створеними резидентами та нерезидентами. |

Таблиця 1.3 – Перелік системно важливих, соціально важливих і важливих систем в Україні, визначених НБУ у 2020 р. [18]

| Категорія важливості | Платіжні системи |
|---|---|
| Системно важливі | Система електронних платежів (СЕП) Національного банку України. |
| Соціально-важливі | - MasterCard", MasterCard International Incorporated, США;<br>- "Visa", Visa International Service Association, США;<br>- "Western Union", Western Union Financial Services Inc. США/Western Union Network, SAS, Франція;<br>- "FORPOST" (на сьогодні – Nova Pay), ТОВ "Пост Фінанс";<br>- "Поштовий переказ", ПАТ "Укрпошта |
| Важливі | - "Фінансовий світ", ТОВ "Українська платіжна система";<br>- "MoneyGram", Money Gram Payment Systems Inc. США;<br>- "City 24", ТОВ "Фінансова Компанія "Фенікс";<br>- "FLASHPAY", ПрАТ "Банк Фамільний";<br>- "RIA", Continental Exchange Solutions Inc, США.;<br>- "INTELEXPRESS", АТ Мікрофінансова організація "Інтелекспрес", Грузія |

Виділяють чотири основні блоки платіжних систем: інформаційний, технічний, нормативно-правової та фінансовий.

*Інформаційного блок* складається з програмно-технічного захисту; нормативно-правового захисту інформації; адміністративно-правових засобів захисту; включаючи гарантії, що надаються законодавчою базою України.

До *технічного блоку* входять автоматизовані програми, вузли зв'язку і телекомунікаційні системи, технічні прилади, допоміжні технічні та експлуатаційні пристрої.

У *нормативно-правовому блоці* знаходиться вся законодавча база регіонального і державного масштабу, яка регулює і визначає відносини всіх взаємодіючих сторін в рамках організації платіжної системи та участі в ній.

*Фінансовий блок* включає в себе порядок і правила здійснення бухгалтерського обліку, надання обов'язкової звітності, операційне супроводження перерахувань, що забезпечують економічно прозору модель функціонування платіжної системи та можливість контролю за виконанням операцій і процедур безготівкових розрахунків.

Таблиця 1.4 – Категорії ЕПС, внесених до реєстру НБУ

| № | Характеристика | Особливості категорії |
|---|---|---|
| 1 | Внутрішньодержавні та міжнародні ЕПС, платіжною організацією яких є резидент | ЕПС призначені для організації переказу коштів на користь фізичних та юридичних осіб. Учасниками ЕПС є банки та фінансові установи |
| 2 | Міжнародні ЕПС, платіжною організацією якої є нерезидент | Компанії-нерезиденти представлені в Україні 11 платіжними системами. Чотири з них – це карткові системи (Visa, Mastercard, AMEX і UnionPay International). Вони забезпечують обробку платежів за банківськими картками. Ще сім – міжнародні сервіси грошових переказів, наприклад Western Union і MoneyGram, ін. |
| 3 | Внутрішньобанківські платіжні системи | Десять українських банків створили внутрішні системи переказу коштів у національній валюті без відкриття рахунків. Скористатися ними можна тільки у відділеннях конкретного банку, який надає послугу |
| 4 | Оператор послуг платіжної інфраструктури | Оператор послуг платіжної інфраструктури призначений для організації надання послуг процесингу, клірингу, операційних інформаційних та інших технологічних функцій, які стосуються переказу коштів |

Таким чином, до основних елементів платіжної інфраструктури в Україні можна віднести складові фінансової системи, що зображені на рис. 1.3


Рисунок 1.4 – Ключові елементи платіжної інфраструктури в Україні

Наведений рисунок характеризує лише ключові елементи платіжної інфраструктури нашої держави.

Таблиця 1.5 – Переваги впровадження в Україні безготівкових розрахунків

| Об’єкт | Перевага |
|---|---|
| Держави | декриміналізація та детінізація економіки; оптимізація витрат, пов’язаних із обслуговуванням готівкового обігу; зростання бази оподаткування за рахунок підвищення прозорості бізнесу |
| Банки | скорочення операційних витрат (на перерахунок, експертизу пошкоджених та сумнівних банкнот, охорону, інкасацію тощо); зростання комісійних доходів; поліпшення показників ліквідності; розширення клієнтської бази, зокрема за рахунок перехресних продажів послуг; мінімізація ризиків, пов’язаних із безпекою зберігання, інкасації, транспортування готівки |
| Фізичні особи | зручність у користуванні; отримання доступу до додаткових можливостей та сервісів; легалізація процесу отримання доходу шляхом поступового відходу від заробітних плат «у конвертах»; мінімізація ризику шахрайства шляхом отримання підроблених банкнот, крадіжки, пограбування тощо |
| Торгівельні організації | мінімізація ризику шахрайських дій (підроблені банкноти, пограбування тощо); зростання обсягів продажу (за рахунок психологічного ефекту, адже фізична особа при готівкових розрахунках не може використати більше готівки, ніж фізично має, проте при користуванні кредитною картою зазвичай користується овердрафтом) |

# 2 ДОСЛІДЖЕННЯ ІНФОКОМУНІКАЦІЙНИХ БАНКІВСЬКІХ ПЛАТІЖНИХ СИСТЕМ

## 2.1 Банківська автоматизована інформаційна система

Термінологія, яка застосовується в платіжних системах, не поспіває за вимогами часу і тому в наукових працях та законодавчій базі досі використовуються дещо застаріли терміни.

Так в постанові «Про затвердження Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України" від 17 червня 2004 року N 265 визначається, що інформаційні системи банку - це комплекси програмно-апаратних засобів, призначені для вирішення банками та їх філіями власних завдань у сфері автоматизації, технічної й технологічної підтримки діяльності Центру сертифікації ключів банку та взаємодії з інформаційними системами Національного банку. До цих систем належать система автоматизації банку, внутрішньобанківська міжфілійна платіжна система, інформаційна система Центру сертифікації ключів банку тощо [22] .

Автоматизована Банківська Система (АБС) це комплекс апаратно-програмних засобів, що реалізують мультивалютну інформаційну систему, що забезпечує сучасні фінансові та управлінські технології в режимі реального часу при транзакційній обробці даних. Термін «автоматизована» означає, що в деякій системі відбувається часткова автоматизація ряду бізнес-процесів, однак немає повної автоматизації, тобто система працює в діалозі з людиною, який є особою, яка приймає остаточні рішення.

Існує термін «автоматична», який означає, що в цій системі все бізнес-процеси повністю автоматизовані і можуть виконуватися без присутності людини. Автоматизація банківської діяльності завжди передбачає участь людини, тому повністю автоматичних банківських систем бути не може. Замість терміну «автоматизована» розробники використовують термін «інформаційна банківська система» або «інфокомунікаційна банківська система». В атестаційній роботі ми будемо використовувати більш сучасну абревіатуру Банківська автоматизована інформаційна система (БАІС).

Таблиця 2.1 – Склад забезпечувальної частини банківської АІС

| Забезпечення | Функції |
|---|---|
| Інформаційне | це сукупність уніфікованих форм первинних документів, систем класифікації і кодування та методів їх застосування у банківській діяльності, а також файли даних, що зберігаються у базі даних і використовуються для автоматизованого вирішення функціональних задач |
| Технічне | це комплекс технічних засобів, який включає до свого складу обчислювальну техніку та засоби збору і передачі даних для інформаційного обміну як всередині банку, так і при взаємодії з іншими банками та клієнтами |
| Програмне | сукупність програм, які реалізують мету та задачі АІС і забезпечують функціонування технічних засобів (загальне і спеціальне) |
| Математичне | сукупність алгоритмів та економіко-математичних моделей, які характеризують процедури обробки даних та формування бухгалтерської статистичної звітності |
| Лінгвистичне | включає до свого складу мовні засоби, що використовуються у системі: мови програмування, інформаційно-пошукові мови, мови опису метаданих, мови запитів і спілкування користувачів з системою й інші мовні засоби |
| Правове | сукупність нормативно-правових документів та інструктивних і методичних матеріалів, які регламентують права й обов’язки спеціалістів та визначають технологічний порядок функціонування БАІС і юридичний статус результатів такого функціонування |
| Організаційне | сукупність методів і засобів, що дозволяють удосконалювати організаційну структуру об’єктів, управління та функції, яка визначає штатний розмір та чисельність кожного підрозділу, розробити посадові інструкції персоналу управління в умовах функціонування системи обробки даних |

| | |
|---|---|
| Методичне | сукупність документів, які описують технологію функціонування ІС, методи вибору і застосування технологічних прийомів (технологічне забезпечення) |
| Ергономічне | сукупність методів і засобів для створення оптимальних умов високоефективної роботи в умовах АІС для людей. Найсприятливіші умови праці |

Забезпечувальна частина (табл.2.1) об’єднує всі види ресурсів, необхідних для повноцінного функціонування БАІС [23].

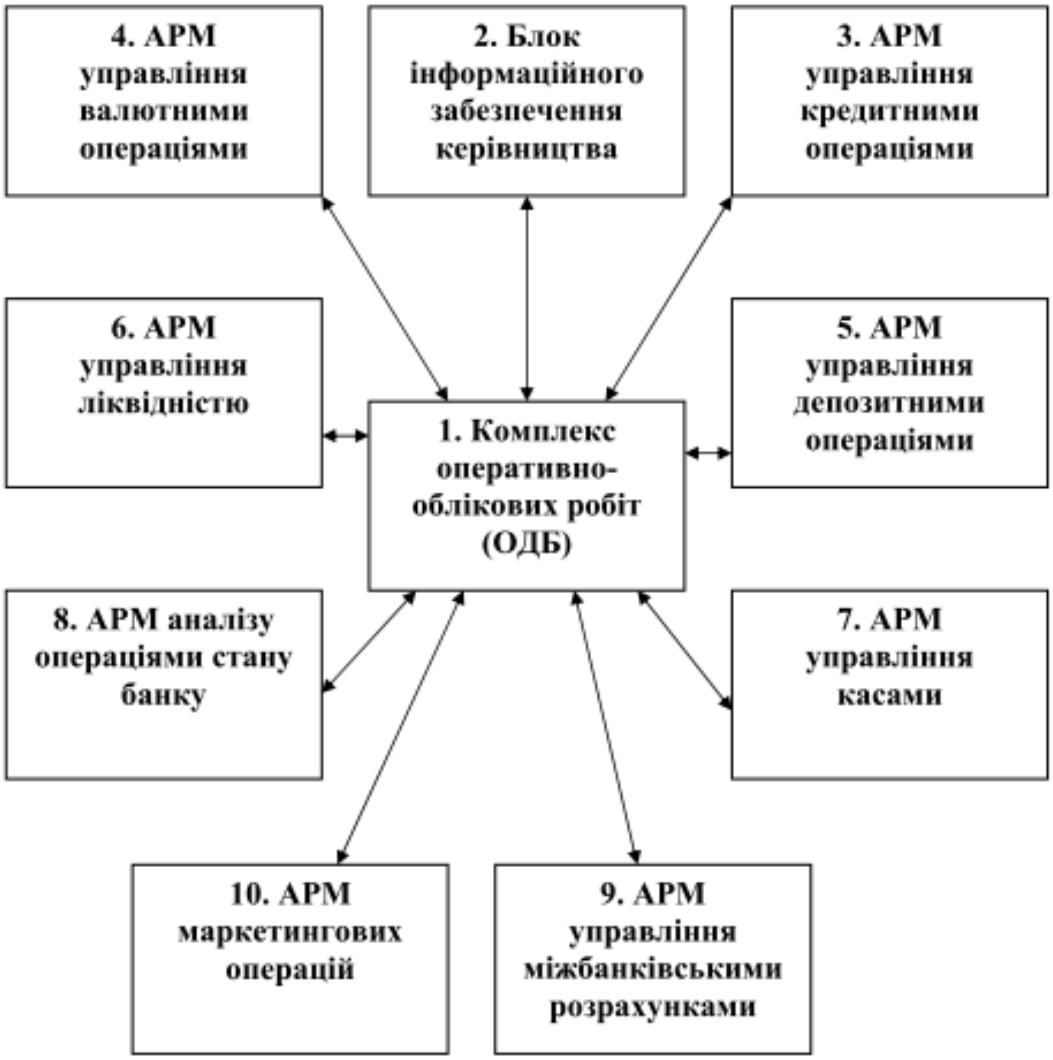


Рисунок 2.1 – Структура функціональної частини АІС комерційного банку

Функціональна частина БАІС об’єднує так звані автоматизовані робочі місця (АРМ) – програмно-технічні комплекси, які реалізують банківські функції.

Пояснимо термін «платформа» БАІС. Насамперед, платформи - це обладнання, яке включає і комп'ютери, і програмне забезпечення, і додаткове обладнання, на якому може функціонувати БАІС. Іноді уточнюють поняття «платформа» і вживають терміни «апаратна платформа» та «програмна платформа» або «апаратно-програмна платформа».

При описі платформ, на яких реалізуються БАІС, посилаються на системне програмне забезпечення, до якого відносяться мережева операційна система, яка встановлена на сервері і забезпечує узгоджену роботу всіх комп'ютерів і всіх користувачів в мережі, і локальна операційна система, яка встановлена на конкретних робочих місцях. В загальному випадку це можуть бути різні операційні системи. Крім того, до системного або базового програмного забезпечення при розгляді БАІС часто відносять СУБД. Пройшли ті часи, коли розробники БАІС використовували саморобні СУБД. В даний час міцно склався ринок професійних СУБД і практично всі сучасні АБС використовують для своєї реалізації ту чи іншу промислову (таку, яка поставляється і продається її розробниками) СУБД.

Оскільки в нашому світі все постійно розвивається, і особливо це стосується інформаційних технологій, при описі конкретної БАІС можуть бути використані терміни «сімейство операційних систем» або «версія СУБД». Під «сімейством» розуміємо операційні системи, що поставляються однією фірмою-розробником, а під «версією СУБД» - конкретну реалізацію.

## 2.2 Узагальнена структура БАІС

Слід зазначити, що БАІС є складною багатофункціональною системою і найбільш складним програмно-апаратним комплексам. Як і будь-яка складна система, БАІС може бути розглянута з різних точок зору.

Базові принципи застосування інформаційних технологій в банківських системах:

- модульний принцип побудови;
- принцип єдності інформаційного простору;
- принцип забезпечення безпеки;
- принцип ефективності;
- принцип взаємодії окремих програмних компонент;
- узгодженість всіх видів забезпечення.

Модульний принцип передбачає поділ інформаційної банківської системи на ряд елементів за функціональним або об'єктному принципом. Ці елементи прийнято називати модулями, блоками або компонентами. Наприклад, при розподілі за функціональною ознакою можна виділити: операційний день

банку, розрахунково-касове обслуговування, кредитування, депозитарний облік; по об'єктному принципом - модуль головного банку, модуль філії, модуль відділення і т. п. [23]

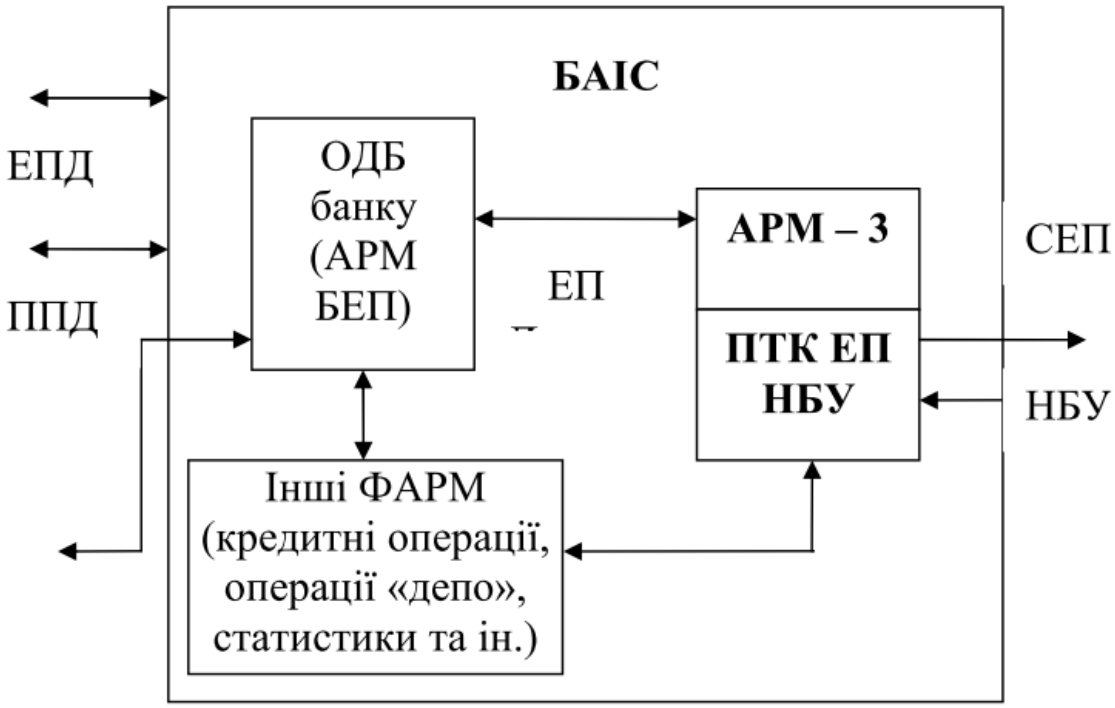


Рисунок 2.2 – Загальна структура АІС стандартного комерційного банку

На рис. 2.2 наведено стандартну структуру АІС комерційного банку. Скороченнями позначено: ЕПД – електронні платіжні документи; ППД – паперові платіжні документи; БЕП – банківський електронний платіж, СЕП – система електронних платежів, ФАРМ – функціональні автоматизовані робочі місця, ЕП – електронний платіж; ОДБ – операційний день банку; ПТК – програмно-технічний комплекс [23].

Операційний день (funds transfer business day) – частина робочого дня банку або іншої установи - учасника платіжної системи, протягом якої приймаються від клієнтів документи на переказ і документи на відкликання та можна, за наявності технічної можливості, здійснити їх обробку, передачу та виконання. Тривалість операційного дня встановлюється банком або іншою установою - учасником платіжної системи самостійно та закріплюється в їх внутрішніх нормативних актах [2].

Традиційно при описі БАІС виділяють три взаємодіючих шари обробки інформації: фронт-офіс (Front office), бек-офіс (Back office) і розрахункове ядро (Accounting).

*Front office* - верхній рівень утворюють модулі, що забезпечують швидкий і зручний введення інформації, її первинну обробку і будь-який зовнішній взаємодія банку з клієнтами, іншими банками, НБУ, інформаційними та торговими агентами (програмними системами з обробки інформації).

*Back office* - середній рівень складають спеціальні функціональні додатки, які відповідають різним напрямкам внутрішньобанківської діяльності та внутрішніми розрахунками (робота з кредитами, депозитами, цінними паперами, пластиковими картками і т. п.).

Accounting - нижній рівень утворюють модулі, які виконують базові функції бухгалтерського обліку або складають бухгалтерське ядро.

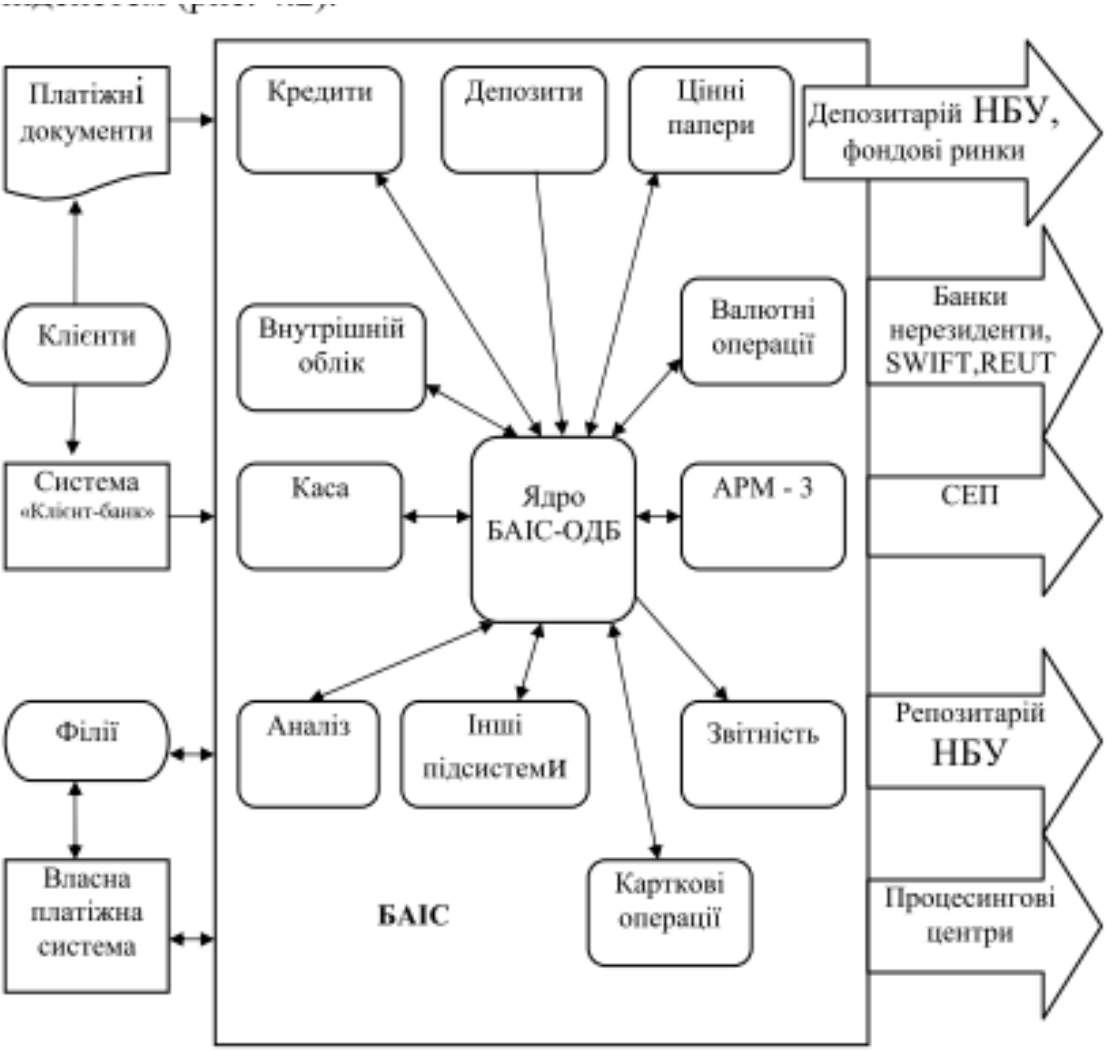


Рисунок 2.3 – Функціональний зв’язок модулів АІБС

*Модуль розрахунково-касового обслуговування*:

- облік даних про клієнтів банку, укладених договорах банківського обслуговування, відкриття і ведення розрахункових і валютних рахунків клієнтів;
- обробка банківських документів різних видів, у тому числі платіжних доручень в гривнях і валюті, касових, конверсійних, меморіальних, позабалансових і термінових документів;
- проведення гривневих розрахунків через розрахункову мережу Національного Банку України, валютних розрахунків через мережу S.W.I.F.T;

- автоматизоване ведення картотек документів, в тому числі позабалансових картотек і карток документів, що надійшли на рахунки нез'ясованих сум;
- автоматичний розрахунок і стягнення комісії за проведення операцій;
- формування бухгалтерської звітності відповідно до вимог НБУ.

*Модуль обліку касових операцій:*

- облік готівки валютно-обмінних операцій в касах банку;
- автоматичний облік бланків суворої звітності;
- взаємодія кас і сховищ банку;
- облік готівкових коштів по робочих місцях касирів.

*Модуль обліку клієнтських конверсійних операцій:*

- реєстрація заявок клієнтів по купівлю-продаж валюти;
- операції «обов'язковий продаж», «покупка-продаж за рахунок коштів банку», «покупка-продаж на біржі».

З іншого боку, можна провести виділення модулів по основним об'єктам і процесам обліку та автоматизації. В цьому випадку резонно виділити наступні аспекти функціонування БАІС:

- автоматизація основної діяльності - це в основному характерні автоматизовані банківські системи (АБС);
- автоматизація бухгалтерського обліку в банку;
- автоматизація касових операцій;
- автоматизація депозитарних операцій;
- автоматизація податкової звітності;
- автоматизація внутрішньої бухгалтерії банку як рядового підприємства;
- автоматизація роботи з кредитами;
- автоматизація роботи філій банку;
- автоматизація роботи з клієнтами системи «банк-клієнт»;

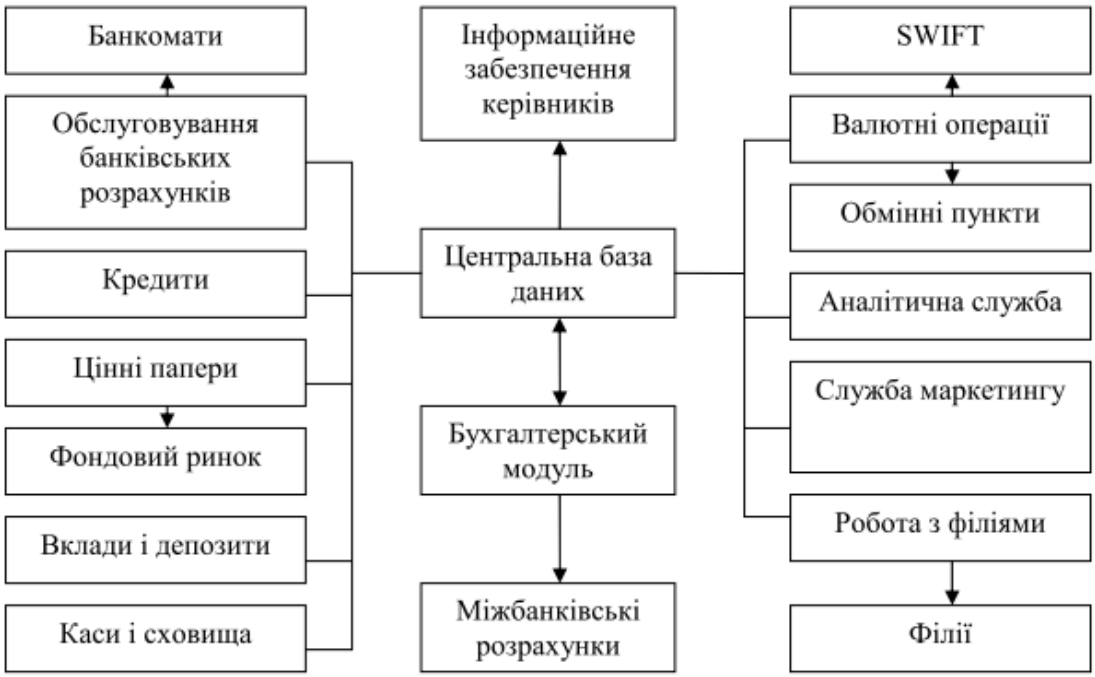


Рисунок 2.4 – Структура інтегрованої банківської системи

автоматизація міжбанківських розрахунків - системи електронних платежів;

перехід на систему безготівкових розрахунків з випуском пластикових карт;

аналітичні системи як системи підтримки прийняття рішень при перспективному стратегічному плануванні [23].

## 2.3 Інтернет-банкінг

Інтернет-банкінг (онлайн / веб-банкінг) – вид надання віддалених фінансово-кредитних послуг через Інтернет [58].

Мобільний банкінг – це різновид Інтернет-банкінгу надання фінансово-кредитних послуг за допомогою встановленого на смартфон мобільного додатку [59].


Рисунок 2.5 – Конкурентні переваги банку при використанні Інтернет-технологій в сучасних умовах [61]

За допомогою Інтернет-банкінгу можна: безкоштовно сплачувати комунальні послуги; купувати та продавати USD та EUR в режимі онлайн 24/7; створити індивідуальний логін для більш зручного доступу до системи; отримувати інформацію про залишки коштів; самостійно формувати / експортувати виписки по рахунках; здійснювати платежі в національній валюті за довільними реквізитами; поповнювати депозити та погашати кредити; поповнювати депозити та погашати кредити; встановлювати індивідуальні ліміти на різні типи розрахунків платіжними картками; самостійно налаштовувати шаблони та регулярні платежі; мати дистанційний доступ до корпоративних карток; самостійно управляти послугою смс-інформування та перевіркою CVV2-коду; онлайн замовляти додаткові картки [60].

Автором був проведений SWOT аналіз використання Інтернет-банкінгу.

| **ПЕРЕВАГИ** | **НЕДОЛІКИ** |
|---|---|
| - мінімізація витрат на обслуговування клієнтів (зменшення собівартості послуг)<br>- Дистанційне управління картою 24/7<br>- Швидке виконання фінансових операцій<br>- Самостійна оплата послуг<br>- Оперативна взаємодія з банком<br>- Мінімальна або нульова комісія | - Відсутність можливості «живого» спілкування з клієнтом<br>- Необхідність підключення до Інтернету<br>- Додаткові витрати на підтримку платформи<br>- Наявність помилок в роботі системи<br>- Можливість шахрайських дій |
| **МОЖЛИВОСТІ** | **ЗАГРОЗИ** |
| - Розширення переліку послуг<br>- Впровадження новітніх IT технологій<br>- Залучення нових інвесторів<br>- Нові напрямки банківських послуг<br>- Підвищення комп'ютерної грамотності населення | - Порушення банківської таємниці через НСД<br>- Можливість втрати даних через кібератаки<br>- Звільнення працівників банку<br>- Втрата частини клієнтів, які віддають перевагу традиційному обслуговуванню |

Рисунок 2.6 - SWOT аналіз використання Інтернет-банкінгу

Втім існують суттєві проблеми, які обмежують застосування Інтернет-банкінгу. По-перше, це не досконаліть системи безпеки. Система безпеки дуже швидко застаріває і її періодично потрібно оновлювати, проводити профілактичні роботи. Адже хакери і зломщики не коли не дрімають і завжди готові вкрасти ваші гроші. По-друге, відсутність зрозуміло будь-якому користувачеві інтерфейсу. По-третє, не всі ресурси працюють постійно, що трапляються перебої і збої в роботі систем. Дуже часто люди скаржаться на те, що система працює несправне, приносять тим самим дискомфорт всім користувачам, яким потрібно зробити термінові операції.

## 2.4 Передумови використання банками хмарних технологій

Банки давно використовують хмарні технології: в тій чи іншій мірі їх впровадили 95% банків розвинутих світових країн. Однак за винятком стартапів і деяких банків, велика частина не збирається повністю мігрувати в хмари. В результаті хмарні технології використовуються не на 100%, а банки

розділилися на 2 табори - одні відстоюють переваги хмарних технологій, а інші ставляться до них скептично (посилаючись на питання безпеки і можливі складнощі з вимогами регуляторів). За даними Accenture, перехід на хмарні сервіси скорочує операційні витрати компанії на 10-20%, а час виведення продукту на ринок зменшується на 30-50%.

Поява COVID-19 призвело до того, що протягом декількох тижнів масштабованість, стійкість, гнучкість і доступність публічних хмар стали набагато важливіше для банків, ніж раніше. Під час пандемії банкіри могли порівняти продуктивність хмарних технологій (як публічних, так і приватних) із застарілими технологіями. Багато банкірів прийшли до висновку, що публічна хмара показало надзвичайно хороші результати: наприклад, з'явилася можливість створення величезних віртуальних колл-центрів за лічені години. Можливості, які з'являться в результаті переходу на хмарні технології, будуть революційними як для окремих банків, так і для галузі в цілому.

Прихильників впровадження хмарних технологій поступово стає все більше. Це пояснює, чому в останні роки інвестиції в «хмару» зросли приблизно на 30%. Дослідницька компанія Forrester очікує, що до 2022 року темп зростання знизиться до 15% в рік, але це все одно буде приблизно в 3 рази швидше, ніж зростання витрат на технології в цілому.

15% банків користуються послугами тільки одного постачальника, 60% вважають за краще мульті хмарну стратегію, тобто користуються послугами декількох провайдерів (найбільш популярні Amazon Web Services і Microsoft Azure). Незважаючи на те, що тренд очевидний, банки говорять, що розчаровані в публічних хмарах. За даними дослідження, проведеного 2019 року, Cloud Outcomes 2.0 Survey, тільки 35% банків повністю отримали ті переваги, які вони очікували від переходу на хмарні технології. Аналітики вважають, що це відбувається через невірну стратегію переходу [62].

Хмарні технології будуть затребувані у тих банків, чий бізнес може бути гнучким, інноваційним, а сам перехід на нові технології знизить витрати.

Банківський бізнес в цілому стає більш інноваційним. Конкуренція з боку таких стартапів, як Stripe, Monzo, Chime і Transferwise, які працюють на загальнодоступних хмарних платформах, змушує банки пробувати щось нове, а не просто модернізувати існуючий бізнес. Нові напрямки бізнесу можна розвивати і на основі власних технологій банку, але кредитним

організаціям все одно необхідно користуватися новими інструментами, аналітикою та технологіями штучного інтелекту. Найпростіше це робити, створюючи їх у публічній хмарі [62].

Вартість хмарних обчислень нижче, ніж використання власної інфраструктури. Особливо важливим це стає, якщо продукт необхідно розгорнути на велику кількість клієнтів. Оплата послуг хмарних провайдерів може здатися високою в порівнянні з вартістю створення і запуску власних програм банків, але досвід показує, що загальні витрати будуть нижчими у тих банків, хто користується загальнодоступними платформами, а потім впроваджує інновації в бізнес-процеси поверх них.

У банків, які планують переходити на хмарні технології, є три варіанти:

Таблиця 2.2 – Особливості застосування хмар для банків

| | Вид хмари | Особливість застосування |
|---|---|---|
| 1 | Публічна | Використання такого сервісу дозволяє банку помітно заощадити: оплачувати потрібно тільки ті послуги, які необхідні банку. До того ж, публічні хмари дають майже необмежені можливості для масштабування |
| 2 | Гібридна | Гібридні хмари (в яких локальна інфраструктура банку поєднується з загальнодоступною хмарою) дають більше можливостей контролювати перехід на хмарні технології. Крім того, в цьому випадку перехід стає більш плавним. |
| 3 | Приватна | Надає максимальну гнучкість - банк може налаштувати свою хмару відповідно до конкретних бізнес-потреб. Також вони можуть надати максимальний рівень контролю і продуктивності, оскільки ресурси хмари використовуються тільки одним клієнтом. |

# 3 ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У ПЛАТІЖНИХ СИСТЕМАХ

## 3.1 Поняття хмарних технологій та опис підходів до їхнього застосування

Хмарні технології - це модель забезпечення зручного мережевого доступу на вимогу до фонду ресурсів, що конфігуруються, які можуть бути оперативно надані, масштабовані та звільнені з мінімальними експлуатаційними витратами і зверненнями до постачальника. Хмарна інфраструктура формує необхідні умови для реалізації спільних ініціатив між фінансовими організаціями, платіжними системами та організаціями інших секторів економіки, дозволяє оперативно створювати нові бізнес-моделі і прискорює виведення нових продуктів на ринок. Хмарні сервіси поділяються на кілька моделей надання послуг - від базових інфраструктурних сервісів до комплексу готових бізнес-функцій, наприклад сервісів обліково-операційної діяльності банків.

### 3.1.1 Інфраструктура як послуга (IaaS)

*Інфраструктура як послуга* (англ. *Infrastructure as a service, IaaS*) — це модель обслуговування, в межах якої споживачу надається можливість керувати засобами обробки та збереження, комунікаційними мережами, та іншими фундаментальними обчислювальними ресурсами, на базі яких споживач може розгортати та виконувати довільне програмне забезпечення, до складу якого можуть входити операційні системи та прикладні програми. Споживач не керує фізичною та віртуальною інфраструктурою, що лежить в основі хмари, проте він контролює операційні системи, системи збереження, встановлені програми та має обмежений контроль над деякими мережевими компонентами (наприклад, мережевими екранами вузлів) [25]

У даній моделі споживач послуг не працює з апаратним забезпеченням безпосередньо, а отримує по підписці попередньо налаштовані віртуальні сервери, які мають задану потужністю, простором для зберігання та доступом до мереж. Споживач послуг самостійно управляє орендованими обчислювальними ресурсами, а також налаштовує програмне забезпечення

для експлуатації розвитку своїх додатків - наприклад, в рамках управління базами даних, зберігання електронних документів (ЕД) або систем для координації бізнес-процесів.

#### 3.1.1.1 Поширені бізнес-сценарії IaaS

До найпоширеніших бізнес-завдань, які вирішуються завдяки IaaS, відносяться [25]:

*Тестування і розробка.* Команда може швидко розгортати і демонтувати середовища тестування і розробки, швидше виводячи нові додатки на ринок. IaaS дозволяє збільшувати масштаб середовищ тестування і розробки швидко і економічно.

*Розміщення веб-сайтів.* Робота веб-сайтів при використанні IaaS може бути менш витратною, ніж традиційне розгортання в Інтернеті.

*Зберігання, архівація і відновлення даних.* Організації позбавляються від необхідності робити капітальні вкладення і долати труднощі, пов'язані зі зберіганням даних і управлінням сховищем, для чого звичайно потрібні висококваліфіковані фахівці з управління даними і забезпечення відповідності нормативним вимогам. IaaS дозволяє справлятися з непередбачуваним попитом і стабільно зростаючими потребами в зберіганні даних. IaaS також може легко спланувати свою систем резервного копіювання та відновлення і управління ними.

*Веб-додатки.* IaaS забезпечує всю інфраструктуру для підтримки веб-додатків, включаючи сховище, веб-сервери і сервери додатків, а також мережеві ресурси. Організації можуть швидко розгортати веб-додатки на базі IaaS і легко масштабувати інфраструктуру, коли число звернень до додатків стає непередбачуваним.

*Високопродуктивні обчислення*. Високопродуктивні обчислення на суперкомп'ютерах, в комп'ютерних мережах або кластерах допомагають вирішувати складні завдання, які включають мільйони змінних і великі обсяги обчислень. Як приклади можна привести моделювання землетрусів і згортання білка, прогнози змін клімату і погоди, фінансове моделювання та оцінку проекту продукту.

*Аналіз великих даних.* Великі дані - це популярний термін для великих наборів даних, які потенційно містять цінні шаблони, тенденції та зв'язки. Інтелектуальний аналіз наборів даних для виявлення прихованих шаблонів

вимагає великих обчислювальних потужностей, які може забезпечити IaaS без значного вкладення коштів.

#### 3.1.1.2 Переваги IaaS

*Усуває капітальні витрати і знижує поточні витрати.* IaaS дозволяє позбутися попередніх витрат на розгортання локального центру обробки даних і управління ними, відкриваючи можливості для організації стартапів і компаній, що тестують нові ідеї.

*Покращує безперервність бізнес-процесів і ефективність аварійного відновлення.* Реалізація високого рівня доступності, безперервності бізнес-процесів і аварійного відновлення вимагає значних витрат, оскільки для цього потрібно багато одиниць обладнання та співробітників. Однак завдяки правильній угоді про рівень обслуговування IaaS дозволяє знизити витрати і використовувати додатки і дані в звичайному порядку при виникненні надзвичайної ситуації або відключенні живлення.

*Швидке впровадження інновації.* Як тільки ви вирішите запустити новий продукт або ініціативу, необхідна обчислювальна інфраструктура буде підготовлена за хвилини або години, а не за дні або тижні, а то й місяці, як в разі внутрішньої інфраструктури.

*Швидке реагування на мінливі умови бізнесу.* IaaS дозволяє швидко масштабувати ресурси, щоб обробляти піковий обсяг звернень, наприклад у вихідні дні, а потім знову зменшувати обсяг виділених ресурсів при зменшенні активності, щоб заощадити кошти.

*Концентрація на власному бізнесі.* IaaS звільняє вашу команду і дозволяє їй концентруватися не на IT-інфраструктуру, а на бізнес-завдання компанії.

*Підвищення стабільності і надійності системи, а також якості підтримки.* Завдяки IaaS немає необхідності обслуговувати і оновлювати програмне забезпечення та обладнання або усувати проблеми в роботі обладнання. Завдяки необхідній угоді про рівень обслуговування постачальник служб працює над тим, щоб ваша інфраструктура була надійною і відповідала вимогам угоди.

*Покращена безпека.* Завдяки угоді про обслуговування постачальник хмарних служб забезпечує безпеку додатків і даних, яка може бути вищою за ту, яку ви могли б забезпечити самостійно.

*Швидке надання користувачам нових додатків*. Оскільки користувачам не потрібно спочатку налаштовувати інфраструктуру, щоб розробляти і надавати додатки, при використанні IaaS власники можуть швидше надавати користувачам нові додатки [26].

### 3.1.2 Платформа як послуга (PaaS)

*Платформа як послуга* (англ. *Platform as a service, PaaS*) — модель надання хмарних обчислень, при якій споживач отримує доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, зв'язного програмного забезпечення, засобів розробки і тестування розміщених у хмарних провайдерах. У цій моделі вся інформаційно-технологічна інфраструктура, включаючи обчислювальні мережі, сервери, системи зберігання, цілком керується провайдером, ним же визначається набір доступних для споживачів видів платформ та набір керованих параметрів платформ, а споживачеві надається можливість використовувати платформи, створювати їх віртуальні екземпляри, встановлювати, розробляти, тестувати, експлуатувати на них прикладне програмне забезпечення, при цьому динамічно змінюючи кількість споживаних обчислювальних ресурсів [27].

Провайдер хмарної платформи може стягувати плату зі споживачів залежно від рівня споживання, тарифікація можлива за часом роботи додатків споживача, за обсягом оброблювальних даних і кількості транзакцій над ними, по мережному трафіку. Провайдери хмарних платформ досягають економічного ефекту за рахунок використання віртуалізації та економії на масштабах, коли з безлічі споживачів в один і той же час лише частина з них активно використовує обчислювальні ресурси, споживачі - за рахунок відмови від капітальних вкладень в інфраструктуру і платформи, розрахованих під пікову потужність і непрофільних витрат на безпосереднє обслуговування всього комплексу [27].

У даній моделі споживач послуг отримує платформу з готовим набором компонентів для розвитку та експлуатації власних додатків, а також середовище управління платформою, що дозволяє швидко зробити прототипи, розгортати нові версії програми, наприклад, мобільний банк-

клієнт, систему управління взаємовідносинами з клієнтами (CRM) і автоматизовану банківську систему (АБС).

#### 3.1.2.1 Поширені сценарії PaaS

Зазвичай організації використовують PaaS в наступних випадках [28].

*Середовище для розробки*. PaaS надає середовище, яку розробники використовують для розробки або налаштування хмарних додатків. Аналогічно тому, як створюється макрос для Excel, PaaS дозволяє розробникам створювати додатки з використанням вбудованих компонентів програмного забезпечення. Хмарні функції, такі як масштабування, висока доступність і підтримка декількох користувачів, вже включені і знижують обсяг коду, який необхідно розробляти.

*Бізнес-аналітика.* Кошти, надані в рамках PaaS, дозволяють організаціям аналізувати дані, знаходити тенденції і робити прогнози з метою поліпшення планування, рішень по продуктах, підвищення повернення від інвестицій і прийняття інших бізнес-рішень.

*Додаткові служби.* Постачальники PaaS можуть пропонувати інші служби, які підвищують можливості додатків, такі як робочі процеси, каталоги, безпека і планування.

#### 3.1.2.2 Переваги PaaS

Надаючи інфраструктуру як послугу, PaaS пропонує ті ж переваги, що і IaaS. Однак додаткові компоненти (ПЗ проміжного шару, засоби розробки та інші бізнес-засоби) створюють такі додаткові переваги.

*Скорочення часу програмування.* Засоби розробки PaaS можуть скоротити час, необхідний для програмування нових додатків завдяки заздалегідь підготовленим компонентам, вбудованим в платформу, включаючи робочі процеси, служби каталогів, компоненти безпеки, засоби пошуку та т. п.

*Додавання можливостей розробки без збільшення числа співробітників.* Компоненти платформи як послуги надають команді розробників нові можливості без необхідності наймати співробітників з відповідними навичками.

*Спрощена розробка для декількох платформ, включаючи мобільні платформи*. Деякі постачальники служб надають користувачам варіанти розробки для декількох платформ, наприклад комп'ютерів, мобільних пристроїв і браузерів, спрощуючи і прискорюючи таким чином крос-платформену розробку додатків.

*Економічне використання просунутих засобів.* Оплата по мірі використання дозволяє фізичним і юридичним особам використовувати просунуті засоби розробки і бізнес-аналітики, які можуть бути занадто дорогими для придбання у власність.

*Підтримка географічно розподілених команд розробників.* Оскільки доступ до середовища розробки здійснюється через Інтернет, команда розробників може працювати над одними проектами, навіть коли члени команди перебувають в різних місцях.

*Ефективне управління життєвим циклом додатків.* PaaS забезпечує всі можливості, які будуть потрібні для підтримки повноцінного життєвого циклу веб-додатків: створення, тестування, розгортання, управління і поновлення всередині одного інтегрованого середовища.

### 3.1.3 Програмне забезпечення як послуга: SaaS (Software as a Service)

У даній моделі клієнт отримує вже готову функціональність в додатку, при цьому розвиток і супровід програми залишається в зоні відповідальності постачальника послуги SaaS, наприклад, клієнт може купити підписку на хмарний CRM, систему автоматизації бухгалтерського обліку або кадрового діловодства.

### 3.1.4 Бізнес як сервіс *BaaS* (Bank / Business as a Service)

*Business as a service* є принципово новим рівнем застосування хмарних технологій, де клієнту надаються не технологічні можливості, а готовий автоматизований бізнес-процес по моделі підписки, яка дозволяє гнучко управляти об'ємом робіт, переданих на аутсорсинг.

Наприклад, якщо в моделі SaaS споживач замовляє хмарну автоматизовану банківську систему, в якій буде працювати і вибудовувати бізнес-процеси самостійно, то в BaaS він замовляє готові обліково-операційні сервіси, які не потребують витрат на їх організацію.

Таблиця 3.1 – Можливості SaaS [30]

| Позитивні фактори | | Обмежувальні фактори |
|---|---|---|
| Для замовників | Для розробників | |
| • Відсутність необхідності установки ПЗ на робочих місцях користувачів — доступ до ПЗ здійснюється через звичайний браузер;<br>• Суттєве скорочення витрат на розгортання системи в організації. Це витрати на оренду приміщення, організацію дата-центру, оплату праці співробітників і т. п.;<br>• Скорочення витрат на технічну підтримку і оновлення розгорнутих систем (аж до їх повної відсутності)<br>• Швидкість впровадження, обумовлена відсутністю витрат часу на розгортання системи<br>• Зрозумілий інтерфейс — більшість співробітників уже звикли до використання веб-сервісів<br>• Прозорість і передбачуваність платежів,<br>• Захист інвестицій;<br>• Багатоплатформеність<br>• Можливість отримати більш високий рівень обслуговування ПЗ | • Зростання популярності веб-сервісів для кінцевих користувачів;<br>• Розвиток веб-технологій, великі функціональні можливості веб-додатків і простота їх реалізації;<br>• Швидкі процеси впровадження і порівняно низькі витрати ресурсів на обслуговування конкретного клієнта;<br>• Легке проникнення на глобальні ринки;<br>• Відсутність проблем з неліцензійним поширенням ПЗ;<br>• На відміну від класичної моделі, замовник SaaS прив'язується до розробника — він не може відмовитися від послуг розробника і продовжувати використовувати систему. Таким чином, забезпечується захист інвестицій розробника в процес продажів;<br>• У довгостроковому періоді доходи від SaaS можуть виявитися вищими від прибутків, які можна отримати від продажу ліцензій та надання технічної підтримки (навіть з урахуванням витрат на хостинг і керування додатками | *По-перше,* SaaS можливо застосувати не для всіх функціональних класів систем. SaaS виявляється неефективною для систем, що вимагають глибокої індивідуальної адаптації під кожного замовника, а також інноваційних рішень.<br>*По-друге*, багато замовників побоюються застосовувати SaaS через міркування безпеки і через можливий витік інформації з боку постачальника цих послуг. Це обмежує використання концепції SaaS для критично важливих систем, в яких обробляється таємна конфіденційна інформація.<br>*По-третє*, обмежувальним фактором SaaS є необхідність наявності постійного підключення до Інтернету.<br>Багато продуктів SaaS компенсують це наявністю модулів для автономної роботи. З розвитком мережі значення цього чинника зменшується (у розвинених країнах він неактуальний зараз), проте в деяких регіонах подібні проблеми як і раніше виникають, і з ними доводиться рахуватися. |

Таблиця 3.2 – Приклад хмарної платформи для створення інтернет-банкінгу [31]

| Можливість | Переваги |
|---|---|
| Платформа онлайн-банкінгу для юридичних та фізичних осіб | Платформа складається з ряду модулів, що забезпечують усі потреби сучасного клієнта онлайн та мобільного банкінгу. До складу платформи входять модулі, що забезпечують:<br>o Керування рахунками та управління кредитами<br>o Операції з валютою<br>o Створення депозитів та отримання кредитів<br>o Управління доступом в особистий кабінет<br>o Робота з картками та корпоративними картками<br>o Зарплатний проект |
| Гнучкий дизайн побудований на базі інтуїтивних уподобань користувача | Платформа може бути адаптована під замовника, не втрачаючи при цьому зручності та цілісності зовнішнього вигляду. Дизайн мобільних додатків розробляється згідно стандартів Material Design Android та IOS Human Interface Guidelines |
| Можливості інтеграції (Платформа може бути інтегрована з) | o Різними банківськими CORE системами<br>o Різними процесинговими центрами та системами карткового офісу<br>o Агрегаторами сплати послуг<br>o Провайдерами P2P переказів<br>o Провайдерами SMS-послуг |
| Забезпечення повного захисту даних | o Автентифікація: логін та пароль, за відбитком пальцю чи FaceID, OTP by SMS, ЕЦП<br>o Залежність доступного функціоналу системи від способу аутентифікації<br>o Контроль і перевірка статусу сертифікатів користувача<br>o Розподіл доступу адміністраторів, технологів, користувачів банку згідно наданих ролей<br>o Підтримка різних систем криптографії та токенів (RSA, ДСТУ, ECDSA) |

На рисунку 3.1 схематично наведено формати надавання хмарних технологій.

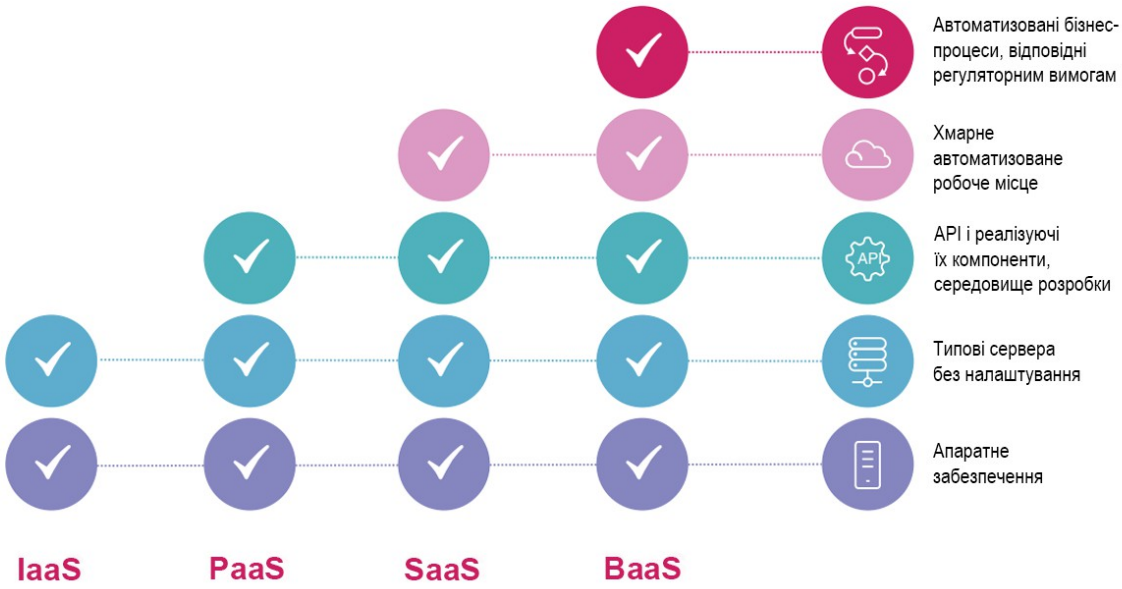


Рисунок 3.1 – Формати надавання послуг хмарних технологій

В таблиці 3.3 зроблено спробу порівняння можливостей IaaS, PaaS, SaaS за різними формалізованими параметрами

Таблиця 3.3 – Порівняння можливостей IaaS, PaaS, SaaS [29]

| *Можливість* | IaaS | PaaS | SaaS |
|---|---|---|---|
| Закупівля та підтримка обладнання | + | + | + |
| Віртуалізація | + | + | + |
| Адміністрування на фізичному та мережному рівні | + | + | + |
| Налаштування на рівні операційної системи | | + | + |
| Бази даних | | + | + |
| Програмне забезпечення | | + | + |
| Наповнення сайту | | | + |

## 3.2 Сервіси хмарної інфраструктури платіжних систем

Розглянемо можливі сценарії надання послуг платіжних систем з використанням хмарних технологій для фінансового ринку.

### 3.2.1 Інфраструктурні послуги

На сьогоднішній день в міжнародній практиці існує успішний досвід перенесення в хмарну інфраструктуру критичних бізнес-функцій, таких як обліково-операційна діяльність, управління ризиками та інформаційна безпека (ІБ). При цьому, як правило, використовується публічна хмарна інфраструктура від одного з технологічних гігантів, таких як Amazon, Microsoft або Google.

Так найбільший цифровий банк *Capital One* (США) ще 6 років тому, в 2015 р, повністю мігрував свої середовища розробки та тестування IT-систем на Amazon Web Services (AWS, США), а в 2017 р вибудував процеси міграції основних сервісів на AWS і сформував команду в кілька тисяч сертифікованих хмарних інженерів. Наприкінці 2018 р Capital One відмовився від 5 з 8 власних дата-центрів на користь хмарної інфраструктури в форматі PaaS. [32]

Цифровий банк *Bunq* (Нідерланди) повністю мігрував свої IT системи на IaaS від Amazon Web Services за два роки. Bunq віддалено надає свої послуги клієнтам в Нідерландах, Німеччині, Австрії, Італії і Іспанії з дата-центру Amazon у Франкфурті [33].

Крім сценаріїв міграції інфраструктури на публічну хмарну інфраструктуру, відомо кілька випадків створення відразу хмарних банківських IT-систем.

DBS Bank (Сінгапур) відкрив в Індії банк DigiBank - мобільний банк-клієнт в публічній хмарі, який використовує обліково-операційну систему материнського банку, розміщену на приватній інфраструктурі[34].

Atom Bank (Великобританія) - мобільний банк без відділень і веб-сайту, розвивається на хмарної інтеграційні платформі від постачальника MuleSoft (США), з використанням хмарної інтеграційної платформи (Integration Platform as a Service, iPaaS), що дозволило Atom Bank реалізувати

повністю наскрізну цифрову обробку (straight-through processing) заявок на іпотеку [35].

Oak North Bank (Великобританія) надає кредитні та депозитні продукти малому і середньому бізнесу в режимі онлайн, використовуючи хмарну автоматизовану банківську систему компанії Mambu (Німеччина). Запуск АБС в хмарі формату PaaS дозволив прискорити виведення продуктів на ринок з декількох раз в квартал до декількох разів на тиждень, що дає можливість швидко адаптуватися до зміни вимог клієнтів [36].

### 3.2.2 Інформаційна безпека як послуга

Традиційно кожна організація впроваджувала рішення з інформаційної безпеки на власній інфраструктурі. Перехід від приватних рішень до хмарних дозволяє впроваджувати високоякісні і сучасні системи інформаційної безпеки при сукупному зниженні вартості володіння для організації за рахунок відмови від установки і супроводу програмного і апаратного забезпечення, а також скорочення витрат на персонал, що обслуговує вказане обладнання.

Найбільш широко поширені хмарні рішення з безпеки:

- антивірусні сервіси;
- сервіси захисту від спаму;
- сервіси захисту зберігання інформації;
- сервіси захисту від шахрайства і DDoS-атак.

Також поширення набувають принципово нові сервіси з безпеки: хмарні рішення, що надають послуги зі зберігання і використання закритих ключів електронного підпису.

*Хмарні антивіруси* – це комплекси з клієнтського додатку і веб-сервісу. Така структура дозволяє знизити навантаження на комп'ютери користувачів. Також під хмарними антивірусами часто мають на увазі, антивіруси, що забезпечують безпеку на хмарних платформах. Перед тим як відкрити підозрілий файл - його бажано перевірити на віруси. Для цього існують онлайн сервіси, найбільш відомим з яких є VirusTotal. [37]

*VirusTotal* - один з найпотужніших онлайн-сканерів, який дозволяє виконувати пошук за URL-адресою, IP, домену або хеш-суми файлу. Крім цього у VirusTotal присутній стандартний метод перевірки шляхом

завантаження файлу на сервер. Цей сервіс виконує перевірку із залученням понад 70 різних сканерів і служб, він не просто повідомить про наявність загрози або шкідливого ПЗ, а повідоме конкретну назву і класифікацію шкідливого вірусу [38].

Антивірусне ПЗ - найнадійніше комплексне рішення для боротьби з онлайн погрозами. Щоб оцінити їх серйозність, розглянемо найпоширеніші види шкідливих атак.

*Віруси.* Цей термін застосовується по відношенню до всього шкідливого ПЗ, але вірусами є тільки ті програми, які здатні самостійно проникнути в комп'ютер і додавати зловмисний код, або, іншими словами, "заразити" файл, програму або всю систему. Результатом зараження вірусом може бути збій роботи системи за рахунок порушення структури розміщення даних або навіть повне видалення операційної системи [38].

*Трояни*, на відміну від вірусів не заражають інші програми. Троянські програми також не проникають в комп'ютер самостійно - зловмисники маскують їх під виглядом корисного ПЗ, яке встановлює сам користувач. Трояни наносять ще більшої шкоди, оскільки крім видалення системних і особистих файлів здатні красти конфіденційну інформацію [38].

*Хробаки* (Черви) - шкідливі програми, які небезпечніше вірусів і троянів через високу швидкість поширення з використанням мережевих ресурсів. Миттєво обчислюючи мережеві адреси, черви проникають в інші комп'ютери, створюють на системних дисках робочі папки і тим самим призводять до підвисання системи [38].

*Шпигунські програми* - це ПЗ використовується для збору конфіденційної інформації про певного користувача шляхом тотального сканування системних і робочих папок його комп'ютера. Програми-шпигуни функціонують на чужому ПК зовсім непомітно, не надаючи видимого навантаження на операційну систему. Крім отримання особистих даних шпигунські програми застосовуються для віддаленого контролю чужого комп'ютера [38].

*Шифрувальники*, мета яких - проникнути в комп'ютер, отримати доступ до особистих медіа файлів і зашифрувати їх з метою вимагання коштів за їх розшифровку [38].

*Спам* - окремий вид шкідливих атак, що представляє собою масову розсилку поштових листів фінансового, політичного та агітаційного характеру. Зловмисники використовують спам для самих різних цілей - від виманювання з адресата великої суми грошей до банальної навантаження на поштові сервери, яка призводить до втрати важливих даних [38].

*Поштовий спам* - розсилка поштою форм для заповнення особистих даних.

*Онлайн фішинг* - створення сторінок, які скопійовані з оригінальних сайтів соціальних мереж, онлайн-банкінгу, платіжних систем [38].

*Мобільні загрози* - SMS розсилка, аналогічна поштовому спаму з метою дізнатися особисті дані.

Для того, щоб розуміти, як працює антивірус, *розглянемо основні функції антивірусного ПЗ* у хмарах:

*Захист від загроз в реальному часі*. Це базова функція всіх антивірусних програм, що представляє собою щосекундний моніторинг активності комп'ютера і своєчасний захист від усіх отриманих загроз.

*Виявлення загроз*. Вибіркове або загальне сканування застосовується в разі установки антивірусу на пристрій, що спочатку функціонував без захисту. Корисно також періодично проводити вибіркове сканування найбільш уразливих секторів системи.

*Менеджер паролів*. По суті, це зашифроване файлове сховище для збереження логінів і паролів. Прикладом такого сховища є Webpass. Менеджер паролей Webpass дає максимальні можливості контролю за створенням, зберіганням, наданням доступу і їх обліком, а також сховище паролів дозволяє звільнити IT-фахівців для інших завдань. Webpass блокує доступи для всіх звільнених співробітників, попереджаючи загрози безпеки інформації і захищаючи інформаційні системи. Для організації безпечного обміну паролями розподіл паролів та їх передача співробітникам відбувається в межах Webpass або шляхом передачі тимчасового доступу через посилання. Дані зберігаються в локальному сховищі браузера виключно в зашифрованому вигляді, тому навіть сам сервіс не має доступу до цих даних. Для шифрування даних використовуються алгоритми AES-256 і RSA, які використовують уряди різних країн [41].

Автором були докладно досліджені можливості сервісу Webpass з захисту паролів, які були зведені в таблицю:

Таблиця 3.4 – Дослідження можливостей хмарних сервісів із захисту паролів

| Можливість | Опис можливості |
|---|---|
| Повідомлення про ризики несанкціонованого доступу | Система безпеки стежить за конфіденційністю паролей; своєчасно повідомляє про випадки, коли користувачу потрібно змінити пароль від акаунту (співробітник загубив доступ до акаунту, був звільнений) |
| Webpass не має доступу до паролів | Сервіс розроблено таким чином, що будь які вразливі дані (паролі, нотатки) передаються на сервер та зберігаються в локальному сховищі винятково у зашифрованому вигляді, що виключає можливість взаємодії з даними, які зі сторони сервісу Webpass так і зі сторони сторонніх осіб. Ключ від шифру - майстер-пароль користувача ніколи не зберігається у відкритому вигляді. Захищеність такого методу також розрахована на те, що у випадку втрати основного і запасного майстер-пароля Webpass не зможе відновити дані користувача |
| Генератор паролів | Створення безпечних паролів з гнучким налаштуванням їх рівня складності |
| Налаштування допустимої складності паролей | Користувачі полюбляють використовувати однакові та занадто прості паролі. Можна обмежити мінімально доступну складність паролів, заборонити більш ніж одноразове використання одного і того ж пароля |
| Зберігання історії змін | Зберігаються детальні записи про те, хто і коли дивився, редагував і відкривав доступ до акаунтів |
| Двох факторна аутентифікація від Google | Можливість додаткового захисту облікового запису Webpass за допомогою двох факторної авторизації. На смартфон користувача в програмі Google Authenticator генерується ключ авторизації, який діє протягом 30 секунд. Таким чином, навіть знаючи майстер-пароль увійти до кабінету Webpass без доступу до смартфону неможливо. |

| | |
|---|---|
| Захист від підбору пароля до акаунту Webpass | Якщо зловмисник буде намагатися підібрати пароль, то система захисту відслідкує такі спроби та заблокує можливість авторизації миттєво повідомивши власника акаунта |
| Імпорт даних | Підтримує імпорт даних у форматі Exel або CSV |

| | |
|---|---|
| Шифрування даних AES-256 та RSA | *Вразливі дані* шифруються за допомогою AES-256 алгоритму, ключ до алгоритму отримується шляхом перетворення майстер-паролю в криптостійкий 256- бітний пароль. *Передача даних* між користувачами здійснюється за допомогою алгоритму RSA, математичні функції якого використовують два ключі – публічний та приватний. |
| Управління доступом співробітників до паролів | Обирається необхідний рівень доступу співробітників до будь-якого акаунту.<br>*Мінімальний рівень перегляду без паролю* – співробітник бачить в переліку акаунтів обліковий запис, але без підтвердженого запиту не має доступ до паролю.<br>*Стандартний рівень* – користувач може переглянути акаунт та копіювати пароль, але не може змінити його.<br>*Адміністративний рівень* – користувач може редагувати та видаляти акаунт, а також відкривати доступ іншим користувачам<br>*Повний доступ* – користувач може надавати адміністраторський рівень доступу іншим користувачам |
| Аналіз безпеки паролів | Складність паролю визначається часом, необхідним зловмиснику для підбору паролю. Система підкаже, наскільки безпечний пароль використовується в акаунті |
| Контроль актуальності пароля | Правила безпеки вимагають періодичної зміни паролю. Користувач може вказати прийнятний для нього період зміни паролів, а система буде його відслідковувати та сповіщувати адміністратора про необхідність зміни |

Автором було проведено аналіз 9 найкращих захищених менеджерів паролів 2021 року [51] та звів їх до таблиці 3.5. В таблиці кожен з паролів розглядається за трьома параметрами. По – перше, платформи, що підтримуються; по-друге, браузери, що підтримується; методи шифрування. Аналіз показав відсутність явного лідера.

Таблиця 3.5 – 9 топ захищених менеджерів паролів 2021 р.

| Менеджер паролів | Платформи, що підтримуються | Браузери, що підтримується | Шифрування |
|---|---|---|---|
| Dashlane [42] | Windows, macOS, Android, iOS та Linux. | Chrome, Safari, Firefox, Internet Explorer та Edge | 256-бітний ключ AES з ланцюгово-блоковим шифруванням та алгоритмом підрахунку коду аутентифікації та вибором між Argon2d й PBKDF2- SHA2 |
| Keeper [43] | Windows, macOS, Android, iOS та Linux. | Chrome, Firefox, Safari, Internet Explorer, Microsoft Edge та Opera. | 256-бітний ключ AES з PBKDF2-SHA2 |
| Roboforum [44] | Windows, macOS, iOS, Android, Linux та Chrome OS. | Chrome, Safari, Firefox, Microsoft Edge та Internet Explorer. | 256-бітне шифрування AES з PBKDF2 SHA256 |
| LastPass [45] | Windows, macOS, iOS, Android та Linux. | Chrome, Firefox, Safari, Internet Explorer, Opera та Microsoft Edge. | 56-бітне шифрування AES з PBKDF2 SHA-256 |
| ReamBeer [46] | Windows, macOS, iOS та Android. | Chrome, Firefox та Safari. | 256-бітне шифрування AES з PBKDF2 SHA256 |
| 1Password [47] | Windows, macOS, iOS, Android, Linux та Chrome OS. Крім цього, надається інструмент для роботи з командним рядком | Chrome, Firefox, Brave, Opera та Safari. | 256-бітне шифрування AES- GCM з PBKDF2-HMAC-SHA256 |
| Sticky Password [48] | Windows, macOS, iOS та Android | Chrome, Firefox, Internet Explorer, Opera, Chromium, Seamonkey, Yandex, Comodo Dragon та Pale Moon. | 256-бітне шифрування AES з PBKDF2 SHA256 |

| | | | |
|---|---|---|---|
| Intuitive<br><br>Password [49] | Windows, macOS, iOS та Android. | Microsoft Edge, Firefox, Safari, Chrome та Opera | 256-бітне шифрування AES з PBKDF2 |
| LogMeOnce [50] | Android та iOS. Підтримується й захищене сховище на USB. | Firefox, Internet Explorer, Safari та Chrome | 256-бітне шифрування AES з SHA-512 |

Після розгляду топ-9 захищених менеджерів паролів автором були сформульовані вимоги до їхнього вибору (таблиця 3.6).

Таблиця 3.6 – Вимоги до вибору менеджерів паролів

| Вимога | Обґрунтування |
|---|---|
| Безпека та прозорість | Всі проаналізовані менеджери паролів були створені компаніями, які мають бездоганну репутацію та відповідну історію в галузі кібербезпеки. Найбільш безпечні менеджери паролів завжди приділяють багато уваги прозорості своєї діяльності. Обраний менеджер паролів має надавати чітку та зрозумілу інформацію про принципи своєї роботи, та яку персональну інформацію збирає компанія. Більшість менеджерів паролів використовують *256-бітне шифрування AES*, яке має такий же ступінь захисту, як і системи, що використовуються банками та урядовими організаціями. Краще обирати менеджери паролів, які пропонують *двох факторну аутентифікацію*. Таким чином, ваші паролі не будуть наражатися на ризик крадіжки навіть в тому випадку, якщо хтось отримає доступ до вашого майстер-паролю. |
| Простота користування | Менеджер паролів повинен працювати з браузером та пристроями непомітно для користувача та автоматично вводити ім’я користувача та паролі там, де це необхідно. Більшість менеджерів паролів також допоможуть користувачу створити надійний пароль «на ходу», не відволікаючись від основної роботи. Це допоможе заощадити час та розумові зусилля, а також забезпечить таку надійність паролю, завдяки якій його буде неможливо зламати чи підібрати. |
| Сумісність | В ідеальному варіанті, потрібен менеджер паролів, який надає додаток, що є сумісним з усіма пристроями користувача – для забезпечення захисту під час придбання товарів онлайн, проведення фінансових операцій в онлайн-банкінгу та багатьох інших випадках. |

3.2.3 *Захист платежів*

Ця функція частіше присутня в розширених версіях платних антивірусів, і спрямована на запобігання крадіжки грошей під час онлайн оплати. Хмарні провайдери зазвичай самі по собі не здійснюють платіжні послуги. Провайдер може лише надати ресурси в оренду організації, що здійснює обробку платіжних карт. Отже, провайдери самостійно залишаються поза передачею, не обробляють і не зберігають дані про власників карт (CHD) або конфіденційні дані аутентифікації (SAD) при транзакціях. Втім багато клієнтів великого хмарного провайдера надають платіжні послуги населенню або бізнесу. Наприклад, це можуть бути банки, ритейлери, e-commerce - компанії, які розміщують свої системи в інфраструктурі провайдера. У цьому випадку обов'язки по захисту платежів поділяються між провайдером і клієнтом, але і провайдер, і клієнт в цьому випадку повинні відповідати вимогам PCI DSS в тому обсязі, в якому це визначено договором між цими сторонами. Таким чином, спільними зусиллями і провайдера і клієнта досягається відповідність усім вимогам PCI DSS, і цей тягар не лягає лише на одного клієнта [52].

PCI DSS (Payment Card Industry Data Security Standard) - ключовий стандарт безпеки даних для банківських платіжних карт. Розроблено він Радою за стандартами безпеки галузі (Payment Card Industry Security Standards Council, PCI SSC), а в його створенні брали участь всі головні міжнародні платіжні системи - Visa, MasterCard, American Express, JCB і Discover. На сьогодні PCI DSS існує у версії 3.2.1 і являє собою 12 докладних технічних і організаційних вимог, виконання яких забезпечує безпечну обробку даних про власників платіжних карт, а також їх передачу і зберігання в IT-системах різних організацій в рамках їх бізнес-процесів. Вимоги стандарту спрямовані на захист інформації, витік або несанкціонований доступ до якої може призвести до втрати конфіденційності та, як наслідок, грошових коштів фізичних осіб і / або установ. Отримання сертифікату підтверджує високий рівень безпеки та надійності IT-сервісів компанії і свідчить про комплексний підхід до забезпечення інформаційної безпеки карткових даних [52].

*Антиспам* - модуль, що фільтрує поштовий трафік, відправляючи підозрілі листи в окрему папку, де при відкритті листів блокуються

мультимедійні дані з метою запобігти проникненню черв'яків. Також здійснюється фільтрація рекламного і агітаційного спаму [38].

### 3.3 Хмарне середовище для обміну даними

Елементом хмарної інфраструктури для фінансового сектора є середовище для обміну даними на основі відкритих API, що забезпечує інтеграцію між хмарними компонентами постачальника інфраструктури та приватними компонентами одного з клієнтів-учасників. Уприклад, хмарна АБС і хмарний шлюз до платіжної системи можуть бути інтегровані з приватної реалізацією мобільного банку-клієнта. В іншому випадку кредитна організація може інтегрувати свій процес розгляду кредитних заявок з сервісами, які надає хмарний постачальник KYC-аналітики або альтернативного кредитного скорингу. При цьому у споживача послуги повинна бути можливість паралельно використовувати сервіси декількох постачальників з метою визначення найбільш підходящого для вирішення конкретних завдань. Отже, «хмара» є форматом надання послуги обміну даними, а відкриті API - способом публікації і використання цієї послуги.

В Україні широко використовується E-Cloud створений на базі платформи VMware. Зараз використовується стек продуктів актуальної версії: VMware vSphere 6.7, NSX Edge 6.5, vCloud Director 10. При розробці архітектури цієї хмари закладалася можливість швидкого переходу на нові версії продуктів VMware. Тому власники завжди надають клієнтам найсучасніший функціонал цієї платформи [53].

E-Cloud розміщується на базі трьох дата-центрів рівня TIER III, які працюють без простою протягом багатьох років: GigaCenter, BeMobile (Київ) і Atman (Варшава). Інфраструктура з трьох дата-центрів дозволяє побудувати будь-які складні і повністю зарезервовані IT-ландшафти [53].

Архітектура нового публічного кластеру хмари GigaCloud побудована на базі технологічного стеку VMware, з використанням професійного обладнання від постачальників «А-брендів». Архітектуру кластеру зручніше розглядати як поєднання трьох базових рівнів: сервісного шару, шару віртуалізації та апаратного шару [53].

Таблиця 3.7 – Можливості E-Cloud [53]

| Можливість | Опис |
|---|---|
| Контроль над виділеними ресурсами | Самостійне управління хмарною інфраструктурою, створення та видалення серверів, розподіл між ними ресурси, налаштування мережевих з'єднань, резервне копіювання і т.п. |
| Побудова будь-якої мережевої інфраструктури | Будь-яка топологія L2 / L3-мереж, а також потужний функціонал VMware NSX, доступний в кожному проекті E-Cloud, незалежно від його розміру та складності |
| Свобода вибору ОС і будь-яких шаблонів VM | Створюючи власний проект на базі E-Cloud, можна обрати те, що потрібно конкретно під завдання - будь-які шаблони віртуальних машин і операційні системи |
| Створення гібридних хмар | Об'єднавши E-Cloud, власне обладнання, послуги colocation від Giga Center і організацію каналів зв'язку від Giga Trans, можна створити будь-яку гібридну інфраструктуру |

Вищий *Сервісний шар* базується на порталі самообслуговування VMware vCloud Director v.10, що використовує та розподіляє ресурси віртуальних дата-центрів (VDC). Портал надає можливість автоматизації розгортання та надання пулу ресурсів у оренду користувачам через веб-портали (з використанням HTML5). Для порівняння: попередній кластер публічної хмари E-Cloud використовує vCloud Director v.9.1. За допомогою порталу, на ресурсах провайдерських VDC створюються одиниці адміністрування – Організації (Organization), тобто середовища ресурсів, користувачів та груп. Один Клієнт може володіти jрганізацією, де використовуються ресурси декількох віртуальних дата центрів одночасно [53].

*Шар віртуалізації* під керуванням VMware vCenter Server поєднує в пули ресурсів публічної хмари ресурси віртуалізованих через vSphere v.6.7 хостів (фізичних серверів), систем зберігання даних (СЗД) та мережевого стеку обладнання.

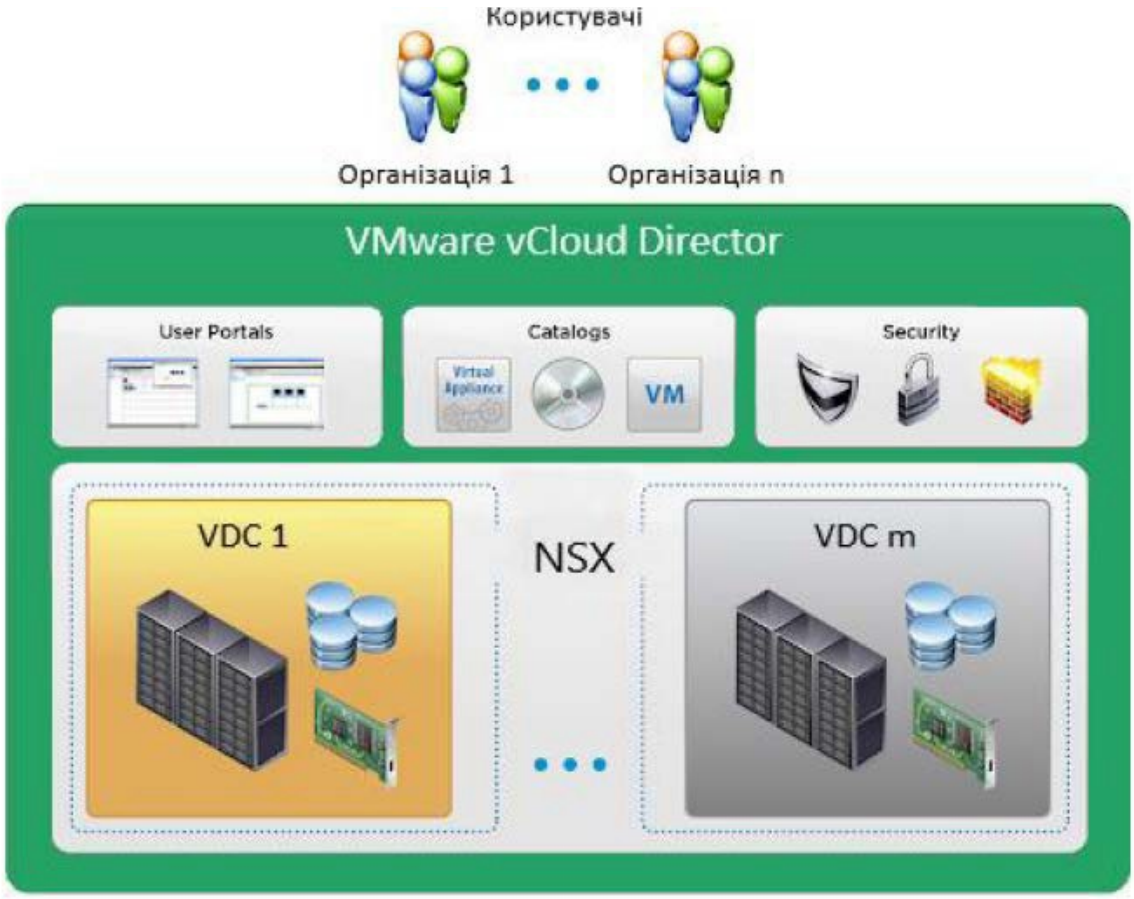


Рисунок 3.2 – Сервісний шар Giga Cloud [53].

Для порівняння: попередній кластер публічної хмари E-Cloud використовує стек віртуалізації VMware vSphere v.6.0/6.5 та vCenter v.6.5. Платформа віртуалізації VMware створює програмно-визначені провайдерські VDC, ресурси яких використовує вищий Сервісний шар [53].

Система віртуалізації нового кластеру базується також на рішенні VMware NSX - платформі керування віртуальними мережами та забезпечення безпеки мережевих сервісів. Наприклад, механізми NSX Edge забезпечують для VDC функції маршрутизації, Firewall, NAT, DHCP, Site to Site VPN, SSL VPN-Plus, Load Balancing та High Availability [53].


Рисунок 3.3 – Платформа віртуалізації [53].

*Апаратний шар нового кластеру.* Надійність роботи кластеру забезпечується архітектурою «без єдиної точки відмови», що зібрано виключно з комплектуючих А-брендів. Апаратна частина містить сервери Intel / Lenovo останніх поколінь з 18-ядерними процесорами Intel Xeon® Gold 6240 gen2, що працюють на базових тактових частотах 2,60 GHz. Для порівняння: попередній кластер публічної хмари E-Cloud використовує сервери з процесорами Intel Xeon E5-2690v4 та Gold 6132. Сервери кластеру комплектуються оперативною пам'яттю, модулі якої спеціально відібрано та встановлено згідно рекомендацій виробника для досягнення найвищої продуктивності. Для високонавантажених вузлів пропонується також конфігурація з високочастотними процесорами Intel Xeon Gold 6246 (24 фізичних ядер, по 2 потоки 3,3 GHz на ядро) [53].

У кластері використовуються СЗД (системи зберігання даних) Fujitsu DX200 S4 /S5 або Lenovo DE2000H. Всі моделі СЗД містять швидкісні диски All Flash, що поєднано у RAID. Технології All Flash забезпечують набагато вищу продуктивність та стабільність роботи СЗД, ніж гибрідні рішення з використанням шпіндельних магнітних дисків (HDD). Підвищену надійність системі додає наявність у корпусі одночасно двох контролерів (на випадок відмови компонентів). Рішення СЗД передбачає резервування N+2, тобто в кожному пулі дисків знаходяться 2 резервних. Внаслідок, навіть малоймовірна одночасна відмова будь-яких двох дисків – не призводить до втрати даних. Додатково, кожна полиця містить ще 1 диск у «холодному резерві» для швидкої дистанційної заміни вибувшого з ладу (з метою збереження резервування N+2) [53].

Для збереження даних, клієнт може обирати між сховищами потрібних об’ємів (розміром від 100 GB, далі кратно 10 GB) у вигляді 3 типів «storage policy», що відрізняються параметрами швидкодії [53]:

- HDD (до 200 IOPS) [53];
- SSD (до 2000 IOPS) [53];
- Fast SSD (до 20 000 IOPS) [53].

У разі необхідності, за запитом надається окрема виділена «полиця» з ізольованими дисковими масивами SSD/HDD у Системі зберігання даних. Для порівняння: на відміну від нового, у попередньому кластері публічної хмари E-Cloud використовується також конвергентна архітектура vSAN v.6.2. (поєднує функції обчислення та зберігання на окремих хостах, об’єднаних мережею зберігання даних) [53].

Стек VMware містить також технології vCloud Availability, що призначені для міграції інфраструктури Клієнта у хмару та побудови сервісу катастрофостійкості DRaaS (Disaster Recovery as a Service). Це необхідно для забезпечення безвідмовності роботи серверів, що мають працювати цілодобово (режим 24/7 критичних бізнес-сервісів). Стек маршрутизаторів також побудовано на обладнанні А-брендів. Для поєднання компонентів кластеру в програмно-визначену мережу «без єдиної точки відмови», організовано лінки стандарту 20G [53].

## 3.4 Обліково-операційні сервіси в хмарних технологіях

Подібні види сервісів є актуальними для швидкого виходу нових учасників платіжних систем на фінансовий ринок. Сервіс хмарного бек-офісу не зажадає значних капіталовкладень, так як IT-інфраструктури, що обслуговує персонал і операційні процеси включені в формат послуги, яку можна масштабувати пропорційно змінам кількості виконаних операцій [54].

Постачальником такої послуги може бути:

- фінансова організація, що надає сегмент свого бек-офісу в форматі Bank as a service;

- технологічна компанія, яка додатково до автоматизації бек-офісу пропонує інші функції, реалізовані самостійно або через партнерів.

### 3.5 Керування платежами у хмарах

Постачальник хмарної платформи може надавати шлюзи до платіжних систем за моделлю підписки аналогічно оренді обліково-операційних послуг. У такій схемі він створює безпечну і масштабовану інтеграцію з платіжними системами, наприклад з системами платіжних карт або системами швидких платежів. У свою чергу, організація-клієнт, розмістивши свій додаток всередині контуру хмари, зможе отримати спрощену схему інтеграції з платіжними системами, істотно скоротивши витрати на інфраструктуру, необхідну для підключення до них. Наприклад, компанія Ant Financial (Китай) створила торговельний майданчик хмарних послуг з хмарної автоматизованої банківською системою і шлюзом до процесингу AliPay.

Управління платежами - одна з опцій, актуальних для бізнесу, і тут потрібно рішення, яке дозволяє забезпечити гнучкі, безпечні і централізовані процеси для всіх вихідних платежів. Ефективне, безпечне і прозоре управління платежами B2B всієї компанії є одним з основних завдань сучасних організацій, особливо коли спроби шахрайства ростуть у всьому світі. Якщо такі типові проблеми з платежами здаються знайомими, саме час подумати про проблеми, які нині виникають:

- Відсутність стандартизації платіжних процесів призводить до неефективності і не прозорості процесу платежів;
- Необхідність роботи з великим набором різних форматів платежів;
- Наявність безлічі банків, які потребують різних механізмів інтеграції з обліковою системою, що ускладнює централізований моніторинг платежів;
- Ручні операції схильні до помилок і забирають багато часу;
- Децентралізована та розрізнена система IT ландшафту перешкоджає тотальному контролю і ефективному управлінню платежами.

Слід використовувати єдиний платіжний хаб в хмарі, який з'єднує всі дочірні компанії і забезпечує цілісну центральну платформу для підключення до локальних ERP-систем, забезпечує єдиний інтерфейс на всі платіжні транзакції, конвертує в необхідний формат платежів, підписує з допомогою надійної криптографії і підключається до всіх банків. Від власника хмари клієнт отримує такі послуги, як впровадження платформ в їх систему, а також постійна підтримка на протязі всього періоду співпраці.

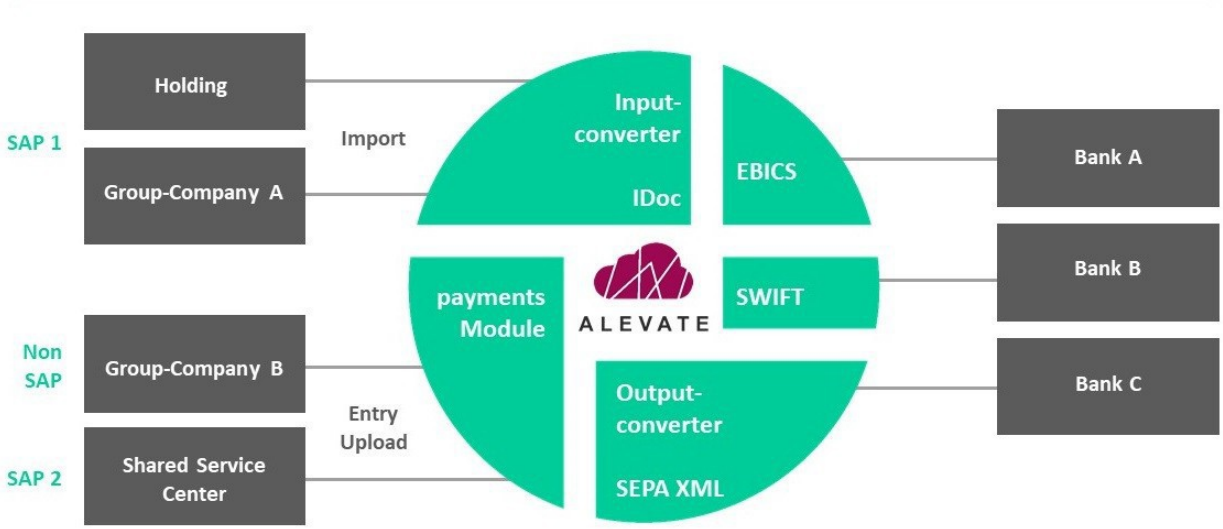


Рисунок 3.4 – Платіжна платформа Serrala Alevate Payments

Компанії використовують такі хаби як платіжну платформу, виконуючи всі свої фінансові операції: управління грошовими коштами, об'єднання грошових коштів і централізовані платежі в хмарі. Пропоновані хмарні рішення для платежів може бути об'єднано з інтегрованими в SAP рішеннями FS2 для формування дійсно гібридної платіжної хмари. Це дозволяє скористатися кращими локальними і хмарними рішеннями одночасно [55].

## 3.6Шаблонні додатки на основі технології розподілених реєстрів

В даний час обов'язковою умовою для підключення до систем, заснованим на технології розподілених реєстрів (distributed ledger technology, DLT), є необхідність розгортання інфраструктури для запуску відповідного рішення на стороні організації. Можливість створити бізнес-додаток на основі технології розподілених реєстрів з типових шаблонів і згодом

розгорнути його на хмарній інфраструктурі з мінімальними тимчасовими витратами дозволить прискорити час виведення продукту на ринок, знизити вартість його запуску і в результаті запропонувати більш вигідні і конкурентні умови для партнерів і потенційних клієнтів. Наприклад, Microsoft (США) надає шаблони в рамках хмарного рішення Azure Blockhain Workbench, Amazon (США) - в рамках Amazon Web Services Blockchain.

### 3.7RegTech-сервіси

Закономірним продовженням розміщення операційної діяльності на хмарній інфраструктурі є реалізація хмарних RegTech-сервісів, включаючи послуги формування обов'язкової фінансової звітності та її передачі фінансовому регулятору і державним органам. RegTech (Regulatory Technology, регулятивні технології) - це технології, які допомагають компаніям відповідати вимогам регуляторів. Для цього використовуються big data, хмарні обчислення, штучний інтелект і машинне навчання, блокчейн. RegTech націлений на галузі з високим рівнем зарегульованості і великою кількістю правил: в першу чергу мова йде про фінансовий ринок, платіжні системи і державні органи. На думку багатьох експертів це «логічне продовження концепції FinTech і LegalTech, яке знаходиться на вістрі атаки і за своєю значимістю заслужило власне окремий напрямок» [56].

RegTech використовується при підготовці звітності, управління ризиками, а також для запобігання шахрайства, перевірці відповідності регуляторним вимогам, проведення стрес-тестів і т.п. Технологічні рішення дозволяють автоматизувати процеси, знизити витрати і підвищити ефективність робочих процесів. Важлива відповідність вимогам KYC (Know Your Client, "знай свого клієнта" - ідентифікація користувачів) і AML (Anti Money Laundering, перешкоджання відмиванню доходів). Наприклад при роботі від іноземної юридичної особи необхідно мати на руках документи, що підтверджують чистоту походження отриманих грошей. Докази доведеться пред'явити фінансовим регуляторам для отримання тієї чи іншої ліцензії, або банку при відкритті рахунку. В Sum & Substance спеціально для цих цілей існують звіти по кожному користувачеві і AML-документація, що

описує методологію застосовуваного due diligence (процедура перевірки компанії перед операцією) [56].

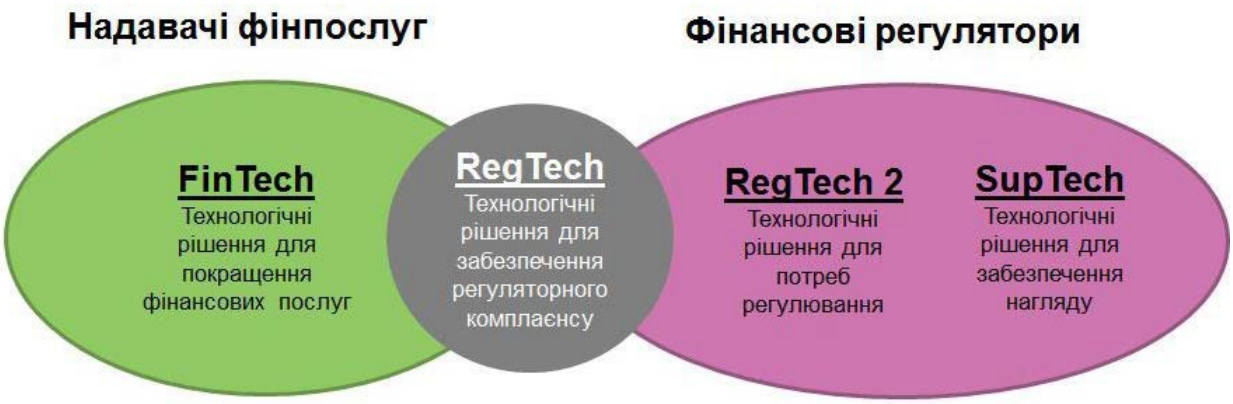


Рисунок 3.5 – Співвідношення FinTech, SupTech I RegTech [57]

RegTech виконує наступні функції:

*Ідентифікація клієнтів і перевірка даних у відповідності з політикою KYC.* Це спрощує верифікацію користувачів, допомагає відслідковувати підозрілі транзакції і управляти ризиками. RegTech-компанії пропонують проводити багатофакторну ідентифікацію користувачів по відбитках пальців (Sonavation, TransmitSecurity), сітківці ока (HYPR), особливостям поведінки (BioCatch, Socure), біографії (Onfido) і навіть по Селф (Smile identity) [56].

*Автоматизація обробки даних і відповідність стандартам.* Наприклад, технологія NEX Regulatory Reporting компанії Abide Financial дозволяє готувати звіти відповідно до вимог регуляторів Європи, США, Австралії і Сінгапуру. Компанія Vizor допомагає зі звітністю для органів страхового нагляду, а Global Fund Watch - з адмініструванням і юридичної звітністю [56].

*Захист даних.* Технології допомагають контролювати передачу даних, боротися з відмиванням грошей, запобігати шахрайству за допомогою аналізу транзакцій. У цій області RegTech-компанії пропонують страхування від кібератак (Cyence, RedSeal Networks, Prevalent Networks), аналіз дій і поведінки співробітників (Cylance), тестові кібератаки (TrapX, Illusive Networks), відстеження аномалій (DarkTrace) [56].

*Аналіз ризиків і пропозиція можливих рішень*. Аналіз кредитоспроможності клієнта, репутації і стану компаній, а також забезпечення відповідності вимогам законодавства. Такі рішення, наприклад, пропонують ComplyAdvantage (оцінка компаній), Kyckr Ireland (перевірка контрагентів в Азії), Credit Benchmark (оцінка кредитних ризиків), Convercent (відстеження нововведень в законодавстві) [56]..

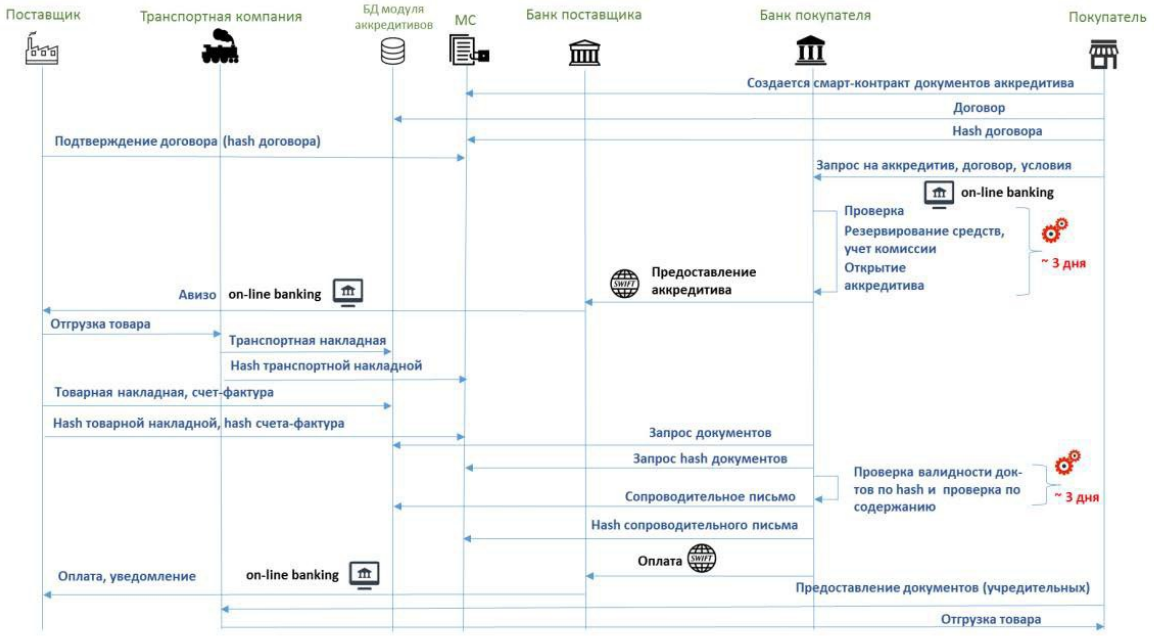


Рисунок 3.6 – Схема роботи цифрового акредитиву [56]

Однією з ключових переваг здійснення діяльності фінансового ринку на хмарній інфраструктурі може стати створення середовища, що забезпечує своїм клієнтам автоматичне виконання базових регуляторних вимог [57 ]. Наприклад, компанія nCino 4 (США) забезпечує надання обов'язкової звітності. Компанія Tradle 5 (США) забезпечує аналіз кредитних ризиків і проведення процедур, спрямованих на відповідність вимогам щодо протидії відмиванню грошей і фінансуванню тероризму.

## 3.8. Хмара як супермаркет фінансових послуг

Крім сервісів, що автоматизують виконання регуляторних вимог, хмарна інфраструктура може пропонувати торговельний майданчик для публікації інноваційних рішень від нішевих компаній, наприклад послуг із застосування машинного навчання в кредитного скорингу, андеррайтинг або

автоматизації маркетингових кампаній. У цьому форматі інноваційні компанії одночасно отримають середовище для розміщення своїх послуг і колективний доступ до дорогої інфраструктури і інформаційних платформ. Таким чином, у фінансово-технологічних компаній з'являється можливість скоротити витрати на підтримку інфраструктури та каналів просування своїх послуг. Наприклад, міжнародна фінансова група ING надає можливість здобувати через свою платформу як власні фінансові продукти, так і продукти своїх конкурентів.

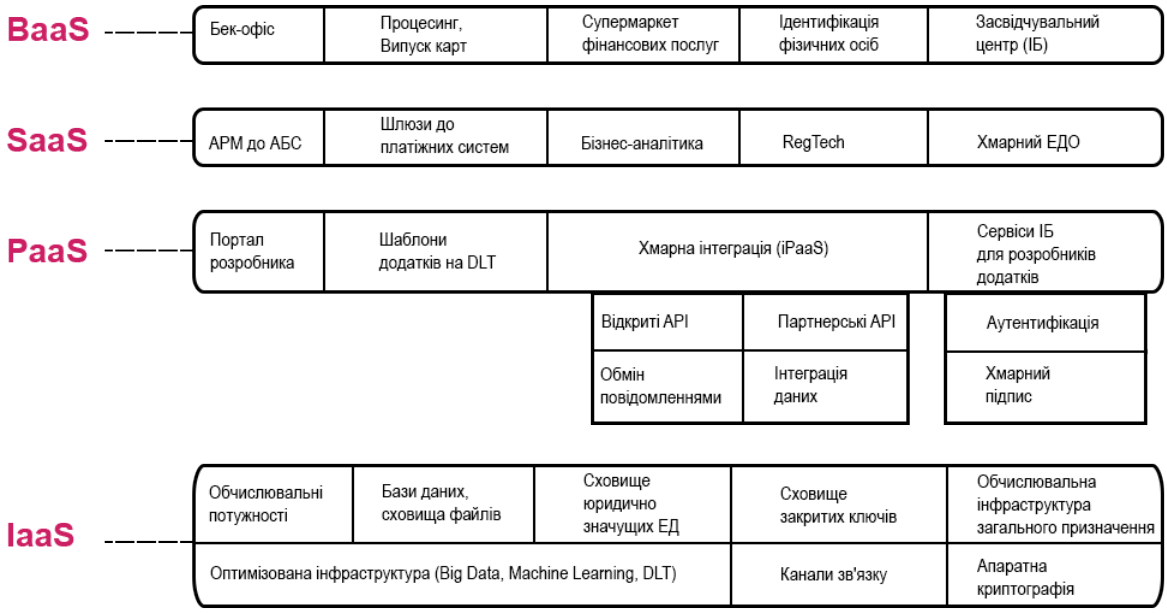


Рисунок 3.7 – Основні компоненти перспективної хмарної технології платіжних систем

## 3.9 Торгова площадка хмарних послуг

Торговельний майданчик являє собою комплексний набір хмарних послуг, при цьому спосіб реалізації деяких з них можна вибирати з декількох варіантів від компаній-конкурентів. таке середовище може включати в себе єдиний підхід до побудови програмних інтерфейсів (API), можливість розміщення своїх додатків на інфраструктурі майданчики, типові договори, а також уніфіковані підходи до вимірювання показників доступності сервісів, виставлення рахунків і оплати хмарних послуг.

Компанія Ant Financial 6 (Китай) створила торговий майданчик хмарних послуг, вибудувану за принципом Bank as a Service. У хмарну

інфраструктуру Ant Financial можуть вбудовуватися як традиційні банки, так і фінтехстартапи. У число сервісів, що надаються самою Ant Financial, входять шлюз до процесингу AliPay і хмарна АБС.

Банк Fidor Solutions (германію) створив в ЄС аналогічну платформу Bank as a Service, в яку входять хмарна АБС, шлюз до процесингу і супермаркет фінансових послуг. Fidor Solutions надає банкам можливість використовувати власну ліцензію на банківську діяльність і полегшену інтеграцію з сервісами з супермаркету послуг. У стартапів, що розвиваються без прив'язки до одного банку-партнеру, є можливість запускати свою діяльність з використанням банківської ліцензії Fidor.

Аналогічно (за рахунок реалізованих механізмів інтеграції з партнерами) N26 (Німеччина) є універсальним цифровим банком. Спочатку банк працював в форматі BaaS с аутсорсингом обліково-операційного функціоналу Wirecard7, потім отримав власну банківську ліцензію та перевів рахунки клієнтів на свою інфраструктуру. Після цього N26 став розвивати функціонал фінансового маркетплейса, надаючи продукти партнерів через свій інтерфейс. Зокрема, страхові продукти в N26 надає Allianz, який є одночасно їх інвестором, а транскордонні перекази організовані через TransferWise.

Компанія-розробник програмних продуктів для цифрового банкінгу Backbase (нідерланди) інтегрує дані і функціональність традиційних банківських систем з фінтехкомпаніямі в єдиний цифровий клієнтський інтерфейс.

Торгова площадка Open Banking Marketplace від Backbase надає послуги широкого спектру провайдерів. Серед послуг є такі категорії, як ідентифікація, аутентифікація, підпис транзакцій, фінансові повідомлення, платежі, боротьба з шахрайством і дотримання процедур KYC.

# 4 ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ ПЛАТІЖНИМ СИСТЕМАМ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ

Інформаційна безпека в хмарі забезпечується в цілому так само, як і в локальних центрах обробки даних, тільки без витрат на фізичні сервери і команду, яка підтримує їх постійну роботу. Використання хмар для розміщення даних, додатків та інших активів надає ряд переваг з точки зору управління, доступу і масштабованості. Хмарна середовище дозволяє бізнесу швидко нарощувати необхідні потужності, але коли мова заходить про масштабування IT-інфраструктури, інформаційна безпека нерідко відходить на другий план. Деякі організації і зовсім не замислюються про посилення системи захисту, оскільки повністю довіряють хмарному провайдеру. Втім використання хмарних рішень поряд з локальною інфраструктурою не виключає кібератак з боку зловмисників, які шукають способи доступу до корпоративних мереж і платіжних систем. Запобігання витоків і крадіжки даних критично важливо для збереження довіри клієнтів і репутації компанії, не кажучи вже про можливі фінансові втрати. Необхідність дотримання нормативних вимог, що пред'являються регуляторами, також змушує багато компаній, що працюють в хмарному середовищі, дбати про забезпечення належного рівня інформаційної безпеки. У разі невідповідності стандартам їм доведеться виплачувати чималі штрафи [63].

## 4.1 Інформаційні ризики хмарних технологій

### 4.1.1 Неправильна конфігурація параметрів безпеки

Це одна з основних причин витоку даних з хмарної середовища. Якщо хмарна інфраструктура спроектована невірно, то виникають ризики небезпечного доступу до ресурсів, компрометації облікових даних, видачі надмірних дозволів, відключення журналу подій або відсутності моніторингу, а також необмеженого доступу до портів і службам.

Багато компаній не знайомі з захистом хмарної інфраструктури і використовують хмарні рішення від різних постачальників: приватне, публічне або мультіхмару - кожне зі своїм набором засобів управління безпекою, що надаються постачальниками. Через неправильну конфігурації

або відсутності контролю безпеки хмарні ресурси організації можуть виявитися відкритими для зловмисників [64].

### 4.1.2 Відмова в обслуговуванні

Функціонування хмарної середовища безпосередньо залежить від підключення до Інтернету. Однак така інфраструктура особливо вразлива до атак типу відмова в обслуговуванні (DoS) і розподілена відмова в обслуговуванні (DDoS). Зловмисники можуть наповнити хмарну мережу компанії великим обсягом веб-трафіку, роблячи ресурси недоступними як для клієнтів, так і для співробітників. Чим більше сервісів і додатків компанії розміщено в хмарі, тим більшої шкоди можуть завдати дії зловмисників.

Як це працює? Хакер використовує уразливість програмного забезпечення, відправляє помилкові запити. Атака може йти через один (DoS) або кілька (DDoS) підключених до інтернету пристроїв. Як хакери відправляють так багато шкідливих запитів? Для цього використовується ботнет-мережу з пристроїв, до яких вони отримали доступ. Після того як пристрій стало частиною ботнету, воно буде виконувати інструкції від централізованих машин. Ботнет може складатися із сотень і тисяч заражених пристроїв, а жертвами можуть стати навіть добре захищені сервери: шлюзи для оплати кредитними картами, банки, урядові органи. DDoS-атаки існують давно, але з появою сервісів в хмарі з'явилася глобальна загроза безпеці. Хмарна модель дає атаці ще більшу обчислювальну потужність, дозволяє вкрасти дані мільярдів користувачів [64, 65, 66].

### 4.1.3 Витік даних

Недостатній рівень захисту може дозволити зловмиснику отримати прямий доступ до конфіденційної інформації компанії і привести до витоку даних, як з локальної мережі компанії, так і з хмарної інфраструктури. Витік даних, в свою чергу, може завдати шкоди репутації компанії, викликати недовіру з боку клієнтів і партнерів. Порушення конфіденційності даних пов'язане і з фінансовими витратами у вигляді санкцій як з боку регуляторів, так і з боку клієнтів, які постраждали від витоку. Ще один ризик - втрата інтелектуальної власності компанії (ноу-хау, власні розробки, технології, моделі товару і т.п.), що вплине на випуск на ринок нової послуги або продукту, що володіє конкурентними перевагами [67].

### 4.1.4 Злом акаунтів

Злом (компрометація) облікового запису - одна з найбільш серйозних проблем, оскільки співробітники компанії не завжди мають достатньо складні паролі, а іноді використовують один пароль для кількох облікових записів. В результаті зловмисник за допомогою одного вкраденого пароля може отримати доступ до декількох систем, і бізнес-логіка, дані і додатки, а часом і компоненти інфраструктури, що залежать від облікового запису, можуть опинитися під загрозою [64].

### 4.1.5 Небезпечні API-інтерфейси

Прикладні програмні інтерфейси додатків (API) призначені для оптимізації хмарних обчислень. Якщо їх залишити без контролю і не застосовувати адекватні заходи захисту, API-інтерфейси можуть відкрити зловмисникам лінії зв'язку для доступу до хмарним ресурсів. Часто розробники створюють API без належних елементів управління аутентифікацією, в результаті ці інтерфейси можна задіяти для доступу до корпоративних даних і систем. При відсутності відповідних елементів управління авторизацією компрометація внутрішніх даних стане для зловмисників тривіальним завданням [65].

Багато API-інтерфейсів мають власні уразливості безпеки, використання яких може поставити під загрозу хмарне середовище. Щоб зменшити цю загрозу, необхідно регулярно тестувати на уразливості додатки, з якими працюють співробітники, аналізувати ризики перед їх впровадженням і оперативно усувати уразливості, стежити за оновленнями безпеки і виправленнями додатків [66].

### 4.1.6 Шкідливі програми

За допомогою шкідливих програм можна отримати доступ до інформації в хмарі. Як це робиться? Для того щоб обійти налаштування безпеки хмарних сервісів, в рішення SaaS, PaaS або IaaS додають модуль зараженого сервісу. Якщо настройки слабкі, модуль перенаправляє запити користувача на екземпляр хакера, що, в свою чергу, запустить шкідливий код. Злочинець отримає повний доступ до даних і навіть зможе встановити прослуховувальну програму для прослуховування. Найбільш поширеними формами загроз безпеки з використанням шкідливих програм є атаки із

застосуванням міжсайтових сценаріїв (додавання на сайт шкідливих скриптів Flash, JavaScript) і SQL-атак [65].

### 4.1.7 Крос-хмарні атаки

Основною метою крос-хмарних атак є попередні центри обробки даних. Для цього хакери використовують діри в безпеці загальнодоступних хмарних сервісів. Як це працює? Зловмисники використовують уразливості, що виникають при переміщенні однієї з робочих навантажень орендарів в середу загальнодоступного хмари (Amazon Web Services, Microsoft Azure) за допомогою будь-якого VPN-каналу, наприклад, Direct Connect. Вторгаючись в одну із середовищ, хакер може атакувати хмара, залишаючись непомітним для моніторингу систем безпеки. Спочатку атаку розпізнати не вдається - потрібен час на сканування середовища, щоб виявити експлойти і традиційні уразливості [66].

### 4.1.8 Атака по боковому каналу

Атака по боковому каналу спрямована на компрометацію IaaS. Як хакери це роблять? Основна мета - розмістити свою віртуальну машину поруч з тією, яку треба зламати. Атака проводиться в два етапи: розміщення шкідливої віртуальної машини поруч з цільовою; витягування корисної інформації [66].

### 4.1.9 Незаконне використання обчислювальних ресурсів

Ця загроза безпеки зачіпає не хмарну інфраструктуру, а безпосередньо ресурси, які надає провайдер. Яскравий приклад - незаконний майнінг криптовалют. Зламавши аккаунт, хакери можуть використовувати обчислювальні ресурси орендаря для обробки транзакцій, встановлюючи скрипт крипто-майнінг на серверах без відома користувача. Це призводить до збільшення навантаження на процесор і, як наслідок, може значно сповільнити роботу системи [66].

## 4.2 Визначення найнебезпечніших атак на платіжні системи в хмарах

Для визначення найнебезпечніших атак на хмари спочатку проаналізуємо 10 найпопулярніших атак 2020 р. на хмари за даними та класифікацією OWASP (Open Web Application Security Project) [70], виявивши, на що спрямована атака (контекст атаки) та технічні наслідки успішної реалізації. Порівняємо їх з відповідними видами атак згідно класифікації CAPEC (Common Attack Pattern Enumeration and Classification) [71]. Результати досліджень зведемо у таблицю 4.1.

Таблиця 4.1 – Аналіз найпопулярніших кібератак 2020 року

| № OWASP топ 10 | № CAPEC | Назва атаки | Мета (контекст) атаки | Технічні наслідки успішної реалізації |
|---|---|---|---|---|
| A1:2020-ін’єкція | CAPEC- 66. | SQL ін’єкція | Конфіденційність, Контроль доступу, авторизація, цілісність | Зчитування даних, модифікація даних, виконання недозволеного коду, команд, отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку |
| A2:2020-порушена автентифікація | CAPEC- 90: | Атака відображення в протоколі автентифікації маніпуляція протоколом | Конфіденційність, контроль доступу, авторизація | Отримання привілеїв доступу / підробка облікових даних, обхід механізмів захисту |
| A3:2020-розкриття конфіденційної інформації | CAPEC- 54: | Запит ІС на інформацію | Конфіденційність | Зчитування даних програмного додатку, зчитування даних пам’яті |
| A4:2020-XML зовнішні сутності | CAPEC-197: | XML розширення сутностей | Доступність | Перевищення лімітів, споживання ресурсів (ЦПП), споживання ресурсів (пам’ять), споживання ресурсів |

| | | | | |
|---|---|---|---|---|
| A5:2020-порушення контролю доступу | CAPEC- 74 | Маніпуляція ідентифікатором привілеїв користувача | Конфіденційність, контроль доступу, авторизація, цілісність | Отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку |

| | | | | |
|---|---|---|---|---|
| A6:2020-Неправиль не налаштування ІБ | CAPEC- 25 | Циклічне блокування декількох паралельних процесів, завершення яких залежить від попередника | Доступність | Відмова роботи ІС через вичерпання доступ-них ресурсів |
| A7:2020-між.сайт.скриптниг | CAPEC- 63: | Міжсайтовий скриптниг (XSS) | Конфіденційність, цілісність, доступність | Виконання несанкціонованого коду, команд, модифікація даних програмного додатку, зчитування даних програмного додатку |
| A8:2020-небезпечна десеріалізація | CAPEC-250: | XML ін’єкція | Конфіденційність, контроль доступу, авторизація | Отримання привілеїв доступу / підробка облікових даних, зчитування даних програмного додатку |
| A9:2020-використання компонентів з відомими вразливостями | CAPEC-111: | JSON злам (Java Script злам) | Конфіденційність | Зчитування даних програмного додатку |
| A10:2020-недостатнє логування та моніторинг | CAPEC- 75: | Маніпуляція не захищеним від запису конфігурацій- ним файлом | Конфіденційність, контроль. доступу, авторизація | Отримання привілеїв доступу / підробка облікових даних |

Для платіжних систем насамперед важливе забезпечення цілісності та автентичності інформації. Порушення цілісності дозволяє злочинцю змінити реквізити реального платежу (суму, дату відправки), порушення автентичності дозволяє підмінити відправника або адресата, а також вставити фальшивий платіж. Наш аналіз виявив, що з 10-топ кібератак 2020 р., наведених у таблиці. 4.1, загрози цілісності та автентичності інформації становлять шість - CAPEC-66, CAPEC-90, CAPEC-74, CAPEC-63, CAPEC-

250, CAPEC-75. Тому далі будемо розглядати саме ці 6 атак. Для розрахунку імовірності настання ризику використовуються наступні фактори, згідно з даними ресурсу MITRE [71]. (таб.4.2)

Таблиця 4.2 – Фактори, які враховуються для оцінки кібератаки [71].

| Фактор | Сутність фактору |
|---|---|
| Імовірність | числова характеристика можливості того, що кібератака відбудеться в умовах, які можуть бути відтворені необмежену кількість разів. |
| Складність реалізації | необхідність наявності у порушника режиму ІБ певного рівня спеціальних знань та вмінь для здійснення кібератаки. |
| Можливість застосування | можливість застосовувати кібератаку на рівні різних архітектур, фреймворків, операційних систем, мов програмування. |
| Доступність ресурсів | можливість застосовувати кібератаку на рівні різних архітектур, фреймворків, операційних систем, мов програмування. |

Таблиця 4.3 - Числове значення параметру «*імовірність*» [71]

| *Параметр* | *Значення* |
|---|---|
| Малоймовірно | 0,1 |
| Ймовірно | 0,15 |
| Дуже ймовірно | 0,2 |

Таблиця 4.4 - Числове значення параметру «*складність реалізації*» [71].

| Необхідна кваліфікація та знання | Значення |
|---|---|
| Низькі | 0,1 |
| Середні | 0,15 |
| Високі | 0,2 |

Таблиця 4.5 - Числові значення параметру «*можливість застосування*» [71].

| *Можливість застосування атаки до різних компонентів* | *Оцінка* |
|---|---|
| атака застосовуватися до всіх типів архітектур, фреймворків, платформ, мов програмування | *0,2* |
| атака може застосовуватися до певних, широко розповсюджених типів архітектур, фреймворків, платформ (наприклад «клієнт-сервер», J2EE, Java) | 0,15 |
| атака може застосовуватися до окремих менш розповсюджених чи застарілих типів архітектур, фреймворків, платформ (наприклад<br>файловий обмін, Novel Netware, MS DOS, Cobol), | 0,1 |

Таблиця 4.6 Числове значення параметру «*доступність ресурсів та засобів реалізації*» [71].

| *Доступність ресурсів* | *Оцінка* |
|---|---|
| відсутність необхідності в спеціальних ресурсах, програмному забезпеченні, програмне забезпечення з відкритим програмним кодом, у вільному доступі | *0,2* |
| ліцензоване програмне забезпечення, необхідність у спеціалізованому апаратному забезпеченні | *0,15* |
| необхідність у значних програмних/апаратних ресурсів, суперкомп'ютерів значення параметру дорівнює | *0,1* |

Таблиця 4.7 – Фактори, які використовуються для розрахунку масштабів збитків [71].

| Мета атаки | Сенс атаки | Оцінка | | | |
|---|---|---|---|---|---|
| | | Низька | Середня | Висока | Дуже висока |
| Вплив на конфіденційність | ступінь впливу на конфіденційність, внаслідок успішної кібератаки, що призводить до порушення конфіденційності. | 1 | 2 | 3 | |
| Вплив на цілісність | ступінь впливу на цілісність, внаслідок успішної кібератаки, що призводить до порушення цілісності | 1 | 2 | 3 | |
| Вплив на доступність | ступінь впливу на доступність, внаслідок успішної кібератаки, що призводить до порушення доступності | 1 | 2 | 3 | |

| | | | | | |
|---|---|---|---|---|---|
| Потенційна шкода | розуміється тяжкість технічних<br><br>наслідків кібератаки і складність виконання заходів щодо відновлення ІС без втрат даних. | | 1 | 2 | 3 |

Таблиця 4.8 – Розрахунок числових значень факторів кібератак на платіжні системи у хмарах

| **Показники** | ***C-66*** | ***C-90*** | ***C-74*** | ***C-63*** | ***C-250*** | ***C-75*** |
|---|---|---|---|---|---|---|
| Імовірність | 0,2 | 0,2 | 0,15 | 0,2 | 0,2 | 0,2 |
| Складність реалізації | 0,2 | 0,15 | 0,15 | 0,1 | 0,2 | 0,15 |
| Можливість застосування | 0,2 | 0,2 | 0,2 | 0,15 | 0,15 | 0,2 |
| Доступність ресурсів | 0,2 | 0,15 | 0,15 | 0,2 | 0,2 | 0,1 |
| *Імовірність виникнення ризику* | *0,8* | *0,7* | *0,75* | *0,65* | *0,75* | *0,65* |
| Вплив на конфіденційність | 3 | 3 | 3 | 3 | 3 | 3 |
| Вплив на цілісність | 3 | 3 | 3 | 3 | 3 | 3 |
| Вплив на доступність | 3 | 1 | 2 | 3 | 2 | 2 |
| Потенційна шкода | 3 | 2 | 3 | 3 | 2 | 3 |
| *Масштаб збитків* | *12* | *9* | *11* | *12* | *10* | *11* |
| | *12,8* | *9,7* | *11,7* | *12,65* | *10,75* | *11,65* |

Наведена оцінка ризиків базується на якісній оцінці кібератак Для класифікації кібератак застосовуються стандарти корпорації MITRE. По осі Y розміщена шкала масштаб збитків, по осі X шкала вірогідність настання ризику. Значення для цих параметрів розраховуються для кожної із загроз. Кожна з загроз входить до однієї з категорій OWASP top 10. Для зручності візуалізації всі значення на діаграмі помножені на 10 [68].

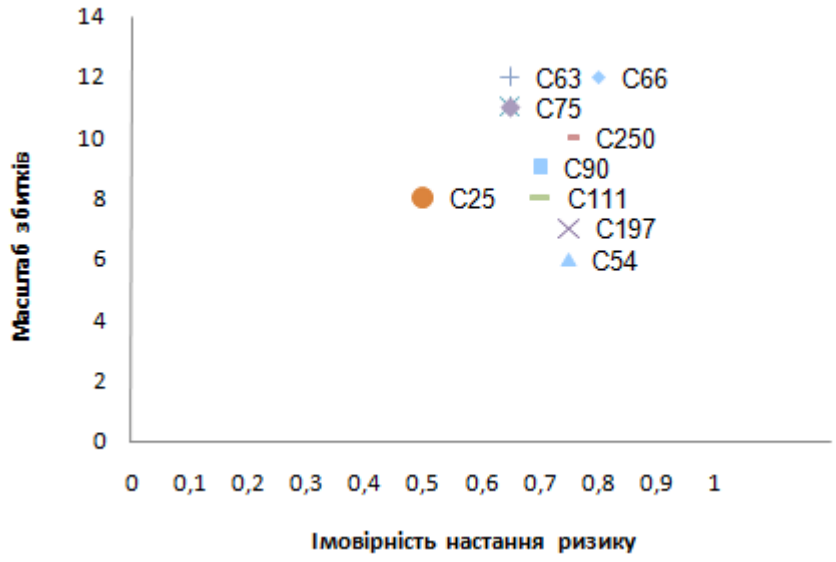


Рисунок 4.1 – Оцінка ризику кібератак на платіжні системи в хмарах

Загальне значення імовірності настання ризику розраховується як сума зазначених вище параметрів, та відображається по осі X.

Як видно з діаграми найбільш критичним щодо ймовірності настання і масштабу потенційного збитку є атаки з класифікації OWASP A1, яка відповідає атаці CAPEC-66, – SQL ін’єкція, що призводить до таких критичних технічних наслідків як виконання недозволеного коду, команд, отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку тощо.

# ВИСНОВКИ

В ході виконання кваліфікаційної атестаційної роботи були досліджені: основні засади функціонування платіжних систем в Україні; структури сучасних АІБС як учасників платіжних систем; хмарні технології з точки зору можливості їхнього застосування у платіжних системах; сервіси хмарної інфраструктури платіжних систем; хмарне середовище для обміну, яке може використовуватися в платіжних системах; обліково-операційні хмарні сервіси, які використовуються у платіжних системах; можливості управління платежами у хмарах; шаблонні додатки хмарних технологій на основі розподілених реєстрів, які використовуються в платіжних системах; RegTech-сервіси хмарних технологій, які використовуються в платіжних системах; можливості хмари з надання фінансово-кредитних послуг; торгові додатки хмарних послуг.

В атестаційній роботі автором був: проведений SWOT аналіз Інтернет банкінгу; запропонована структура моделі платформи хмарних технологій для Інтернет-банкінгу; з'ясовані можливості хмарних сервісів із захисту паролів, проаналізовані 9 найпопулярніших менеджерів паролів 2021 р. за платформами, браузерами, алгоритмами шифрування, складені вимоги для вибору менеджерів паролів; запропонована схема розміщення платіжної системи у хмарі; проаналізовані найпопулярніші кібератаки 2020 року за контекстом атаки та технічними наслідками у разі технічної реалізації та виявлені найнебезпечніші атаки для платіжних систем у хмарному середовищі; за допомогою методики MITRE розраховані числові значення найнебезпечніших атак на платіжні системи у хмарному середовищі.

Таким чином завдання на атестаційну роботу виконано в повному обсязі.

ПЕРЕЛІК ПОСИЛАНЬ


6.7.1. Закон України "Про національний банк України" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/679-14/page#Text.

6.7.2. Закон України "Про платіжні системи та переказ коштів в Україні [Електронний ресурс]. – 2001. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2346-14#Text.

6.7.3. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]. – 1994. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

6.7.4. Закон України "Про інформацію" [Електронний ресурс]. – 1992. – Режим доступу до ресурсу: https://www.tax.gov.ua/diyalnist-/dpa-i- gromadskist/normativno-pravova-baza-u-sferi/arhiv-normativno-pravova- baza/53366.html.

6.7.5. Закон України “Про електронні документи та електронний документообіг” [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/851-15#Text.

6.7.6. Закон України “Про основні засади забезпечення кібербезпеки України”"" [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6.7.7. Закон України "Про електронні довірчі послуги" [Електронний ресурс]
// 2017 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

6.7.8. Указ Президента України від 15 березня 2016 року № 96/2016 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

6.7.9. Проєкт постанови правління НБУ «Про затвердження Положення про захист інформації та кіберзахист в платіжних системах» [Електронний ресурс] // 2021 – Режим доступу до ресурсу: https://bank.gov.ua/admin_uploads/article/Project_of_resolution_11082020.pdf?v=4.

10. НБУ изменяет порядок идентификации клиентов и опровергает вероятность коллапса онлайн-платежей [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://msfz.ligazakon.ua/magazine_article/FZ002142.
11. Идентификация клиентов в банках: системы видеоаналитики [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://center2m.ru/videoanalitika/vca-identification.
12. Банки отримають нові провідні сучасні інструменти для дистанційної ідентифікації та верифікації клієнтів 15 квіт. 2020 16:10 [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://bank.gov.ua/ua/news/all/banki-otrimayut-novi-providni-suchasni-instrumenti-dlya-distantsiynoyi-identifikatsiyi-ta-verifikatsiyi-kliyentiv.
13. Дистанційна ідентифікація в банках: як це працює? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://miloan.ua/blog/distancijna-identifikacia-v-bankah-ak-ce-pracue.
14. Національний банк дозволив відкривати банківський рахунок з цифровим паспортом [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://bank.gov.ua/ua/news/all/natsionalniy-bank-dozvoliv-vidkrivati-bankivskiy-rahunok-z-tsifrovim-pasportom
15. НБУ запустив додаток для зчитування даних із біометричних паспортів [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://ua-news.liga.net/economics/news/nbu-zapustiv-dodatok- dlya-zchituvannya-danih-iz-biometrichnih-pasportiv.
16. Мирошниченко В. О. Біометрична ідентифікація клієнтів у банківській сфері [Електронний ресурс] / В. О. Мирошниченко // Міжнародна та національна безпека: теоретичні і прикладні аспекти Матеріали III Міжнародної науково-практичної конференції (ДДУВС, 15.03.2019). – 2019. – Режим доступу до ресурсу: http://er.dduvs.in.ua/bitstream/123456789/3401/1/91.pdf.
17. Назаренко В. ДО ПИТАННЯ ВИЗНАЧЕННЯ ПОНЯТТЯ «ПЛАТІЖНА СИСТЕМА» В УКРАЇНІ / Валентина Назаренко. // Підприємництво, господарство і право. – 2017. – №10. – С. 54.

18. Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0755500-14#Text.
19. Визначено перелік системно важливих, соціально важливих та важливих платіжних систем в Україні [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://bank.gov.ua/ua/news/all/viznacheno-perelik-sistemno-vajlivih-sotsialno-vajlivih-ta-vajlivih-platijnih-sistem-v-ukrayini.
20. Звіт за результатами оверсайта платіжних систем за 2018 рік [Електронний ресурс] // Національний банк України. – 2019. – Режим доступу до ресурсу: https://bank.gov.ua/admin_uploads/article/Report_oversight_2018.pdf?v=4.
21. Джусов О. А. Поточний стан, проблеми та перспективи розвитку платіжних систем в Україні / О. А. Джусов, О. І. Піляк. // Економічний простір. – 2020. – №154. – С. 190–195.
22. Система електронних платежів [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://bank.gov.ua/ua/payments/sep.
23. НБУ.Постанова «Про затвердження Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України" від 17 червня 2004 року N 265 [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: https://ips.ligazakon.net/document/TM022992.
24. Дубчак Л. В. Інформаційні системи і технології в банківській діяльності. Навчальний посібник. / Л. В. Дубчак, Л. А. Клюско, В. Ю. Свириденко. – Ірпінь: Національний університет ДПС України, 2016. – 248 с.
25. Інфраструктура як послуга [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D1%8F%D0%BA_%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B0.

26. Что такое IaaS? Инфраструктура как услуга [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://azure.microsoft.com/ru-ru/overview/what-is-iaas/.
27. Платформа як послуга [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D0%B0_%D1%8F%D0%BA_%D0% BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B0.
28. Что такое PaaS? Платформа как услуга [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://azure.microsoft.com/ru-ru/overview/what-is-paas/.
29. IaaS, что это такое? PaaS, SaaS, для чего они нужны? Примеры и сравнение [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://1cloud.ru/services/private-cloud/iaas-paas-saas.
30. Програмне забезпечення як послуга [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F_%D1%8F%D0%BA_%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B0.
31. Unity Bars - Платформа для онлайн банкинга [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://unity-bars.com/products/b-one?utm_source=google&utm_medium=cpc&utm_campaign=generic&utm_content=ch_google_adwords|trg_kwd- 21653289354|crt_469093810715|kwmt_b|ps_|srct_g|trgt_|src_|devt_c|devm_|cid_11236187440|lcl_1012866|fdi_|mrlid_18109|dop_&utm_term=%2Bbusiness%20%2Bbanking&gclid=Cj0KCQjwpdqDBhCSARIsAEUJ0hOlYpZuPq8iHVpUHhjIZctWSqVZQpZfNBkDE_fSvYmiH2aCd3yiLqYaAqsYEALw_wcB
32. Capital One Credit Cards, Bank, and Loans [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.capitalone.com/.
33. bunq | bank of The Free [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.bunq.com/home.

34. DBS Bank | Singapore [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.dbs.com.sg/index/default.page.
35. Atom - The app-based bank that makes money simple [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.atombank.co.uk/.
36. Oak North Bank [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.oaknorth.co.uk/
37. Облачные антивирусы - обзор на LiveBusiness [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.securno.ru/tags/oblachnye_antivirusy/.
38. VirusTotal [Електронний ресурс] – Режим доступу до ресурсу: https://www.virustotal.com/gui/.
39. Лямин Г. 5 бесплатных онлайн-сканеров: антивирус не нужен [Електронний ресурс] / Григорий Лямин. – 2019. – Режим доступу до ресурсу: https://www.iguides.ru/main/security/5_besplatnykh_onlayn_skanerov_antivirus_ne_nuzhen/.
40. 10 Лучших антивирусов - 2021 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.10bestantivirus.ru/?utm_source=google&kw=%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81&c=397606320870&t=search&p=&m=p&adpos=&dev=c&devmod=&mobval=0&network=g&campaignid=8147647133&adgroupid=84579932779&targetid=kwd-296752514378&interest=&physical=1012866&feedid=&a=8147647133&ts=&topic=&quality=&fbrem=&test=google_ru&gclid=Cj0KCQjwpdqDBhCSARIsAEUJ0hPRzdJGXrm7NgPPxPbgVRMCGtqp7jUk4hihkjArkvBl-0Vk7GN4-doaAvfDEALw_wcB.
41. Менеджер паролів для компаній [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://webpass.pro/ua/.
42. Dashlane: Password Manager App for Home, Mobile, Business [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.dashlane.com/.
43. Keeper Password Manager - IT Inventory Tracking Software [Електронний ресурс]. – 2021. – Режим доступу до

ресурсу: https://www.lansweeper.com/it-asset-management-software/?utm_source=google&utm_medium=cpc&utm_campaign=LSCORE&utm_term=Competition&creative=441590582359&keyword=keeper%20password%20manager&matchtype=b&network=g&device=c&utm_term=keeper%20password%20manager&utm_campaign=%5BEU%5DLSCORE_Search_competitors&utm_source=adwords&utm_medium=ppc&hsa_acc=4846545452&hsa_cam=10270317350&hsa_grp=102796142299&hsa_ad=441590582359&hsa_src=g&hsa_tgt=kwd-12962634133&hsa_kw=keeper%20password%20manager&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwyN-DBhCDARIsAFOELTlCKUv0oBI4kBNxHRa-uFGu0i_GhjpwI5fgWsOszh-v8mytqVChkWMaAqQaEALw_wcB.

44. Roboforum [Електронний ресурс] – Режим доступу до ресурсу: https://www.roboform.com/lp?affid=vment&frm=offer-vpnmentor.
45. LastPass [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.lastpass.com/?utm_source=impact-radius&utm_medium=affiliate&utm_campaign=affiliate-program&irgwc=1&clickid=VV7zp30esxyOTQLwUx0Mo3YXUknymPQH-Ql90k0.
46. ReamBeer [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.remembear.com/b/remembear-premium?utm_source=Affiliate&utm_medium=cj&ref_id=mkt_aff-cj-prem&cjevent=773e15521abb11ea81e6001e0a24060d&aff_id=4338021.
47. 1Password [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://1password.com/affiliate/teams/?cjevent=b0d5deee9dce11eb808e002e0a18050c&utm_medium=affiliate&utm_source=Webselenese+Ltd&utm_campaign=4338021&utm_content=8958915&utm_term=General+Campaign&cjdata=MXxOfDB8WXww.
48. Sticky Password [Електронний ресурс] – Режим доступу до ресурсу: https://www.stickypassword.com/lp/workfromhome?cid=CE571D-76E347&utm_source=vpnmentor2018&utm_medium=website&utm_term=mva&utm_content=lp-sp-scc50&utm_campaign=2018-12_vpnmentor&campaign_affid=d-websel-scc50.

49. Intuitive Password [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.intuitivepassword.com/.
50. LogMeOnce [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.logmeonce.com/.
51. Касуніч К. 9 Найкращих Захищених Менеджерів паролів у 2021 [Електронний ресурс] / Кейті Касуніч. – 2021. – Режим доступу до ресурсу: https://uk.vpnmentor.com/blog/%D0%BD%D0%B0%D0%B9%D0%BA%D1%80%D0%B0%D1%89%D0%B8%D1%85-%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%B5%D1%80%D1%96%D0%B2-%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%96%D0%B2/
52. Беляков Г. Как облако с PCI DSS-сертификацией обеспечивает безопасность платежей [Електронний ресурс] / Георгий Беляков. – 2020. – Режим доступу до ресурсу: https://www.comnews.ru/digital-economy/content/212151/2020-12-14/2020-w51/kak-oblako-pci-dss-sertifikaciey-obespechivaet-bezopasnost-platezhey.
53. ОБЛАЧНАЯ ИНФРАСТРУКТУРА E-CLOUD [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://gigacloud.ua/ru/services/e-cloud?utm_source=googleads&utm_medium=cpc&utm_campaign=gybridpublcl&utm_content=102517782602&utm_term=%2B%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%20%2B%D0%BE%D0%B1%D0%BB%D0%B0%D0%BA%D0%BE&gclid=CjwKCAjwmv-DBhAMEiwA7xYrd_dYSDbR9VRdNHewA2X4HK2tq04VezSOE4qWVMj4AP6fQffhkcbRlRoCL6oQAvD_BwE.
54. Раюшкин, Э. С. Облачные сервисы в цифровой экономике / Э. С. Раюшкин, В. О. Колесникова // Молодой ученый. — 2019. — № 20 (258). — С. 38-40.
55. Alevate Payments — Управление платежами в облаке [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://miotechcompany.ru/cash-visibility/alevate-payments- upravlenie-platezhami-v-oblake/
56. Сикирин В. Большие надежды банков, или что такое RegTech [Електронний ресурс] / Сикирин В. – 2018. – Режим доступу до

ресурсу: https://bloomchain.ru/detailed/bolshie-nadezhdy-bankov-ili-chto-takoe-regtech.

57. Курцев В. SupTech, RegTech та FinTech — що це таке і у чому різниця: пояснює експерт НБУ [Електронний ресурс] / В. Курцев. – 2019. – Режим доступу до ресурсу: https://ain.ua/2019/05/17/suptech-regtech-ta-fintech/.
58. Захаркін В. О. Роль інтернет-банкінгу в розвитку ринку фінансових послуг / В. О. Захаркін, Л. С. Захаркіна, М. О. Авраменко. // Причорноморські економічні студії. – 2017. – №23. – С. 173–177.
59. Що таке інтернет-банкінг? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://business.diia.gov.ua/handbook/finansovij-menedzment/so-take-internet-banking.
60. I-BANK (ІНТЕРНЕТ-БАНКІНГ) [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://credit-agricole.ua/privatnym-kliyentam/internet-banking-i-bank
61. Павленко Л. Д. Сучасний банкінг в україні: стан, проблеми та шляхи удосконалення в умовах конкуренції / Л. Д. Павленко, Д. О. Шматько. // Международный научный журнал «Интернаука». – 2017. – №18. – С. 61–66.
62. Киракасянц А. Accenture назвала преимущества облачных технологий для банков [Електронний ресурс] / Александра Киракасянц // Frank RG. Аналитика, новости и советы для банков. – 2021. – Режим доступу до ресурсу: https://frankrg.com/36483.
63. Безпека хмарних сховищ і технологій. Основні правила [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://datami.ua/bezpeka- hmarnih-shovishh-i-tehnologij-osnovni-pravila/.
64. Мустафаев М. Безопасность в облаке: угрозы и меры предотвращения [Електронний ресурс] / Мурад Мустафаев. – 2021. – Режим доступу до ресурсу: https://www.iksmedia.ru/articles/5727104-Bezopasnost-v-oblake-ugrozy-i-mery.html.
65. Защита информации в облачных сервисах [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://smoff.ru/howitworks/zashchita-informacii-v-oblachnyh-servisah.

66. Невструев С. Основные проблемы облачной безопасности в 2020 году [Електронний ресурс] / Сергей Невструев – Режим доступу до ресурсу: https://www.it-world.ru/cionews/security/157160.html.
67. Нефёдова М. 9 из 10 утечек данных из облаков происходят из-за человеческого фактора [Електронний ресурс] / Мария Нефёдова. – 2019. – Режим доступу до ресурсу: https://xakep.ru/2019/05/30/cloud-leaks/.
68. Баглай В.О. Загрози безпеки хмарних технологій для банків / В.О. Баглай // Системи обробки інформації. – 2018 - № 1 - с. 127-135
69. Бобиль В.В. "Хмарні" технології як фактор збільшення операційного ризику банку / В.В. Бобиль, М.А. Дронь // Банківська справа. – 2014. – № 11/12. – С. 47-62.
70. OWASP (2020), Open Web Application Security Project website [Електронний ресурс]. – Режим доступу до ресурсу: www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
71. Common Attack Pattern Enumeration and Classification (2018), MITRE corporation website [Електронний ресурс]. –Режим доступу до ресурсу: capec.mitre.org.
72. Бобиль В.В. Управління ризиками «хмарних» технологій в системі ризик-менеджменту банку/ В.В. Бобиль // Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна. Проблеми економіки транспорту. – 2014. – Вип. 7. – С. 29-36.
73. Зіссіс Д. Адресуючи проблеми безпеки хмарних обчислень / Д. Зіссіс, Д. Леккас // Комп'ютерні системи майбутнього покоління. – 2012. – № 28. – С. 583-592.
74. Джусов О. А. ПОТОЧНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПЛАТІЖНИХ СИСТЕМ В УКРАЇНІ / О. А. Джусов, О. І. Піляк. // Економічний простір. – 2020. – №154. – С. 191 - 196.