

Дослідження інфокомунікаційних складових платіжних систем

Виконав:

студент групи ІМЗзм-19-2 Дерев'яно Володимир Віталійович

Керівник: доцент Золотарьов Вадим Анатолійович

Рисунок А.1 – Тема атестаційної роботи

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»

Платіжна система в широкому розумінні

- це сукупність інституційно-правових та інфраструктурних елементів, платіжних інструментів, договірних відносин і законодавчих норм, основне призначення яких полягає у виконанні таких функцій:
- 1) формування умов для здійснення операцій з переказу коштів;
- 2) формування умов для здійснення учасниками платіжних систем діяльності з надання платіжних послуг та інших видів діяльності в межах платіжних систем;
- 3) задоволення потреб користувачів платіжних систем у наданні та реалізації відповідних платіжних послуг

Платіжна система в узькому розумінні

- це одна зі складових частин фінансово-кредитної системи держави, яка являє собою впорядковану, законодавчо регульовану сукупність окремих платіжних систем, організацій, що забезпечують постійний рух коштів та сприяють реалізації цілей грошово-кредитної політики центрального банку

Рисунок А.2 – Визначення платіжних систем

Ключові елементи платіжної інфраструктури України

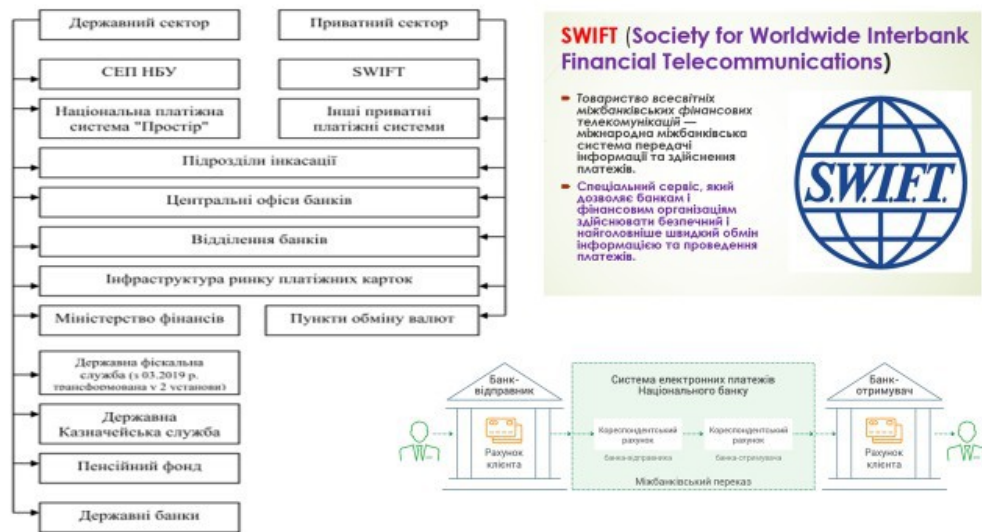


Рисунок А.3 – Ключові елементи платіжної інфраструктури України

Основні блоки платіжних систем

БЛОК	Складові
Інформаційний	складається з програмно-технічного захисту; нормативно-правового захисту інформації; адміністративно-правових засобів захисту; включаючи гарантії, що надаються законодавчою базою України
Технічний	автоматизовані програми, вузли зв'язку і телекомунікаційні системи, технічні прилади, допоміжні технічні та експлуатаційні пристрої.
Нормативно-правовий	законодавча база регіонального і державного масштабу, яка регулює і визначає відносини всіх взаємодіючих сторін в рамках організації платіжної системи та участі в ній
Фінансовий	порядок і правила здійснення бухгалтерського обліку, надання обов'язкової звітності, операційне супроводження перерахунків, що забезпечують економічно прозору модель функціонування платіжної системи та можливість контролю за виконанням операцій і процедур безготівкових розрахунків.

Рисунок А.4 – Основні блоки платіжних систем

Структура функціональної частини АІС комерційного банку



Загальна структура АІС стандартного комерційного банку

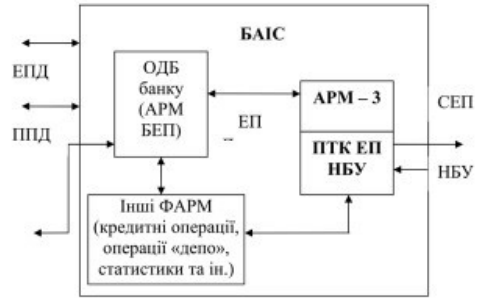
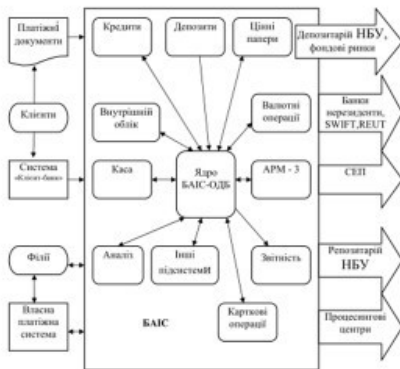


Рисунок А.5 – Структура АІС комерційного банку

Функціональний зв'язок модулів АІБС



Структура інтегрованої банківської системи



Рисунок А.6 – Структура АІБС

SWOT аналіз Інтернет-банкінгу



ПЕРЕВАГИ	НЕДОЛІКИ
<ul style="list-style-type: none"> - мінімізація витрат на обслуговування клієнтів (зменшення собівартості послуг) - Дистанційне управління картою 24/7 - Швидке виконання фінансових операцій - Самостійна оплата послуг - Оперативна взаємодія з банком - Мінімальна або нульова комісія 	<ul style="list-style-type: none"> - Відсутність можливості «живого» спілкування з клієнтом - Необхідність підключення до Інтернету - Додаткові витрати на підтримку платформи - Наявність помилок в роботі системи - Можливість шахрайських дій
МОЖЛИВОСТІ	ЗАГРОЗИ
<ul style="list-style-type: none"> - Розширення переліку послуг - Впровадження новітніх ІТ технологій - Залучення нових інвесторів - Нові напрямки банківських послуг - Підвищення комп'ютерної грамотності населення 	<ul style="list-style-type: none"> - Порушення банківської таємниці через НСД - Можливість втрати даних через кібератаки - Звільнення працівників банку - Втрата частини клієнтів, які віддають перевагу традиційному обслуговуванню

Рисунок А.7 – SWOT аналіз Інтернет-банкінгу



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 загальнодоступним 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 середу відповідно до конкретних бізнес-потребах. Також вони можуть надати максимальний рівень контролю і продуктивності, оскільки ресурси хмари використовуються тільки одним клієнтом.

Рисунок А.8 – Перспективи розвитку платіжних систем

Інфраструктура як послуга (англ. *Infrastructure as a service, IaaS*) — споживачу надається можливість керувати засобами обробки та збереження, комунікаційними мережами, на базі яких споживач може розгортати та виконувати довільне програмне забезпечення, до складу якого можуть входити операційні системи та прикладні програми.

Бізнес-сценарії	Переваги
<ul style="list-style-type: none">• <i>Тестування і розробка</i>• <i>Розміщення веб-сайтів</i>• <i>Зберігання, архівація і відновлення даних</i>• <i>Веб-додатки.</i>• <i>Високопродуктивні обчислення</i>• <i>Аналіз великих даних.</i>	<ul style="list-style-type: none">• <i>Усуває капітальні витрати і знижує поточні витрати.</i>• <i>Покращує безперервність бізнес-процесів і ефективність аварійного відновлення.</i>• <i>Швидко впроваджуйте інновації.</i>• <i>Швидко реагування на мінливі умови бізнесу.</i>• <i>Концентрація на власному бізнесі.</i>• <i>Підвищення стабільності і надійності системи, а також якості підтримки</i>• <i>Покращена безпека.</i>• <i>Швидке надання користувачам нових додатків.</i>

Рисунок А.9 – Інфраструктура як послуга IaaS

Платформа як послуга (англ. *Platform as a service, PaaS*) — 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.

Бізнес-сценарії	Переваги
<ul style="list-style-type: none">• <i>Середовище для розробки.</i>• <i>Бізнес-аналітика.</i>• <i>Додаткові служби</i>	<ul style="list-style-type: none">• <i>Скорочення часу програмування</i>• <i>Додавання можливостей розробки без збільшення числа співробітників.</i>• <i>Спрощена розробка для декількох платформ, включаючи мобільні платформи.</i>• <i>Економічне використання просунутих засобів.</i>• <i>Підтримка географічно розподілених команд розробників.</i>• <i>Ефективне управління життєвим циклом додатків.</i>

Рисунок А.10 – Платформа як послуга PaaS

Програмне забезпечення як послуга: SaaS (Software as a Service) - клієнт отримує вже готову функціональність в додатку, при цьому розвиток і супровід програми залишається в зоні відповідальності постачальника послуги SaaS

Позитивні фактори		Обмежувальні фактори
Для замовників	Для розробників	
<p>Відсутність необхідності установки ПЗ на робочих місцях користувачів</p> <p>Суттєве скорочення витрат на розгортання системи в організації.</p> <p>Скорочення витрат на технічну підтримку і оновлення розгорнутих систем</p> <p>Швидкість впровадження, Зрозумілий інтерфейс</p> <p>Ясність і передбачуваність платежів,</p> <p>Багатоплатформність</p> <p>Можливість отримати більш високий рівень обслуговування ПЗ</p>	<p>Зростання популярності веб-сервісів</p> <p>Великі функціональні можливості веб-додатків і простота їх реалізації;</p> <p>Швидкі процеси впровадження і порівняно низькі витрати</p> <p>Легке проникнення на глобальні ринки;</p> <p>Відсутність проблем з неліцензійним поширенням ПЗ;</p> <p>Замовник SaaS прив'язується до розробника</p>	<p>- SaaS можливо застосувати не для всіх функціональних класів систем.</p> <p>- багато замовників побоюються застосовувати SaaS через міркування безпеки</p> <p>- необхідність наявності постійного підключення до Інтернету.</p>

Рисунок А.11 – Програмне забезпечення як послуга SaaS

Бізнес як сервіс BaaS (Bank / 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.
- Платформа онлайн-банкінгу для юридичних та фізичних осіб
- Гнучкий дизайн побудований на базі інтуїтивних уподобань користувача
- Можливості інтеграції
- Забезпечення повного захисту даних

Рисунок А.12 – Бізнес як сервіс BaaS

Порівняння можливостей хмарних технологій

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			+

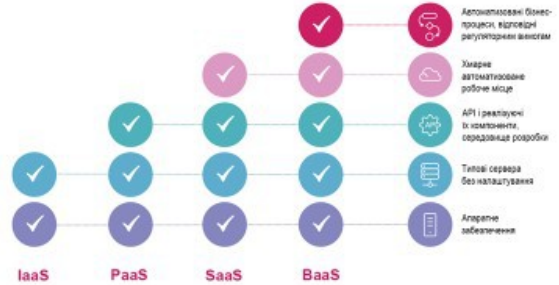


Рисунок А.13 – Порівняння можливостей хмарних технологій

Дослідження можливостей хмарних сервісів із захисту паролів:

- Повідомлення про ризики несанкціонованого доступу
- Webpass не має доступу до паролів
- Генератор паролів
- Налаштування допустимої складності паролей
- Зберігання історії змін
- Двох факторна аутентифікація від Google
- Захист від підбору пароля до акаунту Webpass
- Імпорт даних
- Шифрування даних AES-256 та RSA
- Управління доступом співробітників до паролів
- Контроль актуальності пароля

Менеджер паролів	Платформи, що підтримуються	Браузери, що підтримуються	Шифрування
Dashlane [42]	Windows, macOS, Android, iOS та Linux.	Chrome, Safari, Firefox, Internet Explorer та Edge	256-бітний ключ AES з динамічно-блокованим шифруванням та алгоритмом пірахауку коду аутентифікації та вибором між Argon2id й PBKDF2-SHA256
Keeper [43]	Windows, macOS, Android, iOS та Linux.	Chrome, Firefox, Safari, Internet Explorer, Microsoft Edge та Opera	256-бітний ключ AES з PBKDF2-SHA256
RoboForm [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
Bitwarden [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, Яндекс, Comodo Dragon та Pale Moon.	256-бітне шифрування AES з PBKDF2 SHA256
Intuitive 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 словник на USB.	Firefox, Internet Explorer, Safari та Chrome	256-бітне шифрування AES з SHA-512

Рисунок А.14 – Дослідження можливостей хмарних сервісів із захисту паролів

E cloud

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 мережних 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

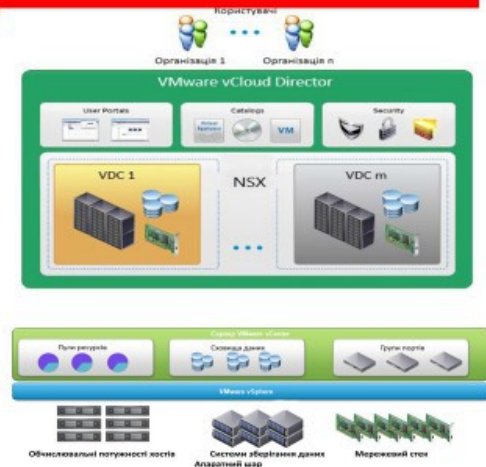


Рисунок А.15 – E cloud

Основні компоненти перспективної хмарної технології платіжних систем

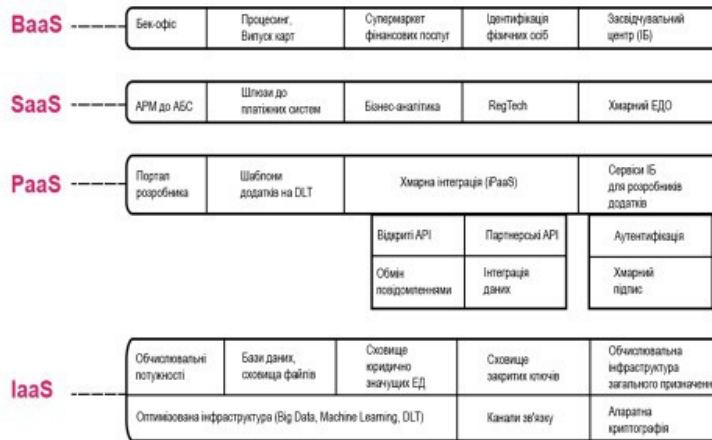


Рисунок А.16 – Основні компоненти перспективної хмарної технології платіжних систем

Аналіз найпопулярніших кібератак 2020 року

№ OWASP топ 10	№ CVE/CWE	Назва атаки	Мета (континент) атаки	Технічні наслідки успішної реалізації атаки
A1-2020-ін'єкція	SAPEC-66	SQL ін'єкція	Конфіденційність, Контроль доступу, авторизація, цілісність	Зчитування даних, модифікація даних, виконання недовзведеного коду, команда, отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку
A2-2020-порушення автентифікації	SAPEC-90	Атака відображення в протокол автентифікації маніпуляція протоколом	Конфіденційність, контроль доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних, обхід механізму захисту
A3-2020-розкриття конфіденційної інформації	SAPEC-54	Запит ІС на інформацію	Конфіденційність	Зчитування даних програмного додатку, зчитування даних плагінів
A4-2020-XML зовнішньої сутності	SAPEC-197	XML розширення сутностей	Доступність	Перезавантаження лінійки, споживання ресурсів (ДПП), споживання ресурсів (пам'ять), споживання ресурсів
A5-2020-порушення контролю доступу	SAPEC-74	Маніпуляція ідентифікатором користувача	Конфіденційність, контроль доступу, авторизація, цілісність	Отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку
A6-2020-Неправильно налаштування ІБ	SAPEC-25	Циклічне блокування декількох програмних процесів, завершення яких залежить від попередника	Доступність	Відмова роботи ІС через вичерпання доступних ресурсів
A7-2020-ін'єкція скриптів	SAPEC-63	Можливий скриптинг (XSS)	Конфіденційність, цілісність, доступність	Виконання неавтентифікованого коду, команда, модифікація даних програмного додатку, зчитування даних програмного додатку
A8-2020-небезпечна десеріалізація	SAPEC-250	XML ін'єкція	Конфіденційність, контроль доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних, зчитування даних програмного додатку
A9-2020-використання компонентів в відповідній вразливості	SAPEC-111	JSON або Java Script (або)	Конфіденційність	Зчитування даних програмного додатку
A10-2020-недостаток логування та моніторингу	SAPEC-75	Маніпуляція не захищеними від запису конфігураційними файлами	Конфіденційність, контроль доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних

Рисунок А.17 – Аналіз найпопулярніших кібератак 2020 року

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

Рисунок А.18 – Розрахунок числових значень факторів кібератак на платіжні системи у хмарах

Висновки

Дослідженні

- 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
- Найпопулярніші кібератаки 2020 року

Розроблено

- Проведено SWOT аналіз Інтернет банкінгу
- Побудовано модель платформи хмарних технологій для Інтернет-банкінгу
- З'ясовані можливості хмарних сервісів із захисту паролів, проаналізовані 9 топ менеджерів паролів 2021 р. за платформами, браузерами, алгоритмами шифрування, складені вимоги для вибору менеджерів паролів
- Запропонована структура 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 проаналізовані найнебезпечніші атаки для платіжних систем у хмарному середовищі

Рисунок А.19 – Висновки по атестаційній роботі



Рисунок А.20 – Завершення доповіді

Позначення	Найменування	Дод. відомості
	Текстові документи	
1.	Пояснювальна записка	с.94
	Графічні документи	
2.	Слайди презентації	20

