Додаток А Слайди презентації

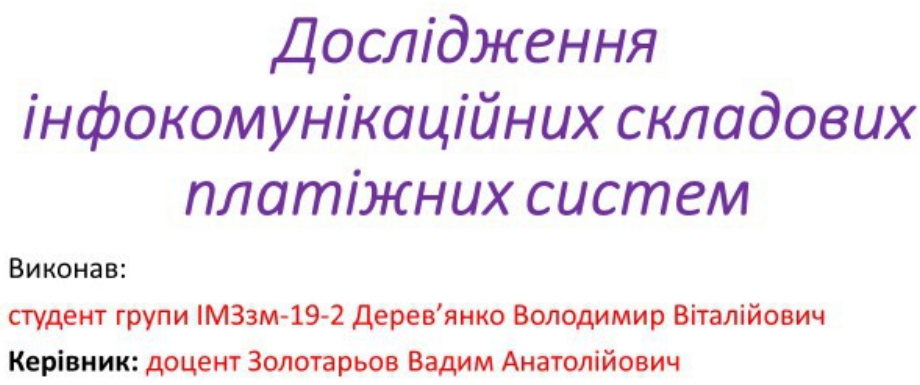


Рисунок А.1 – Тема атестаційної роботи

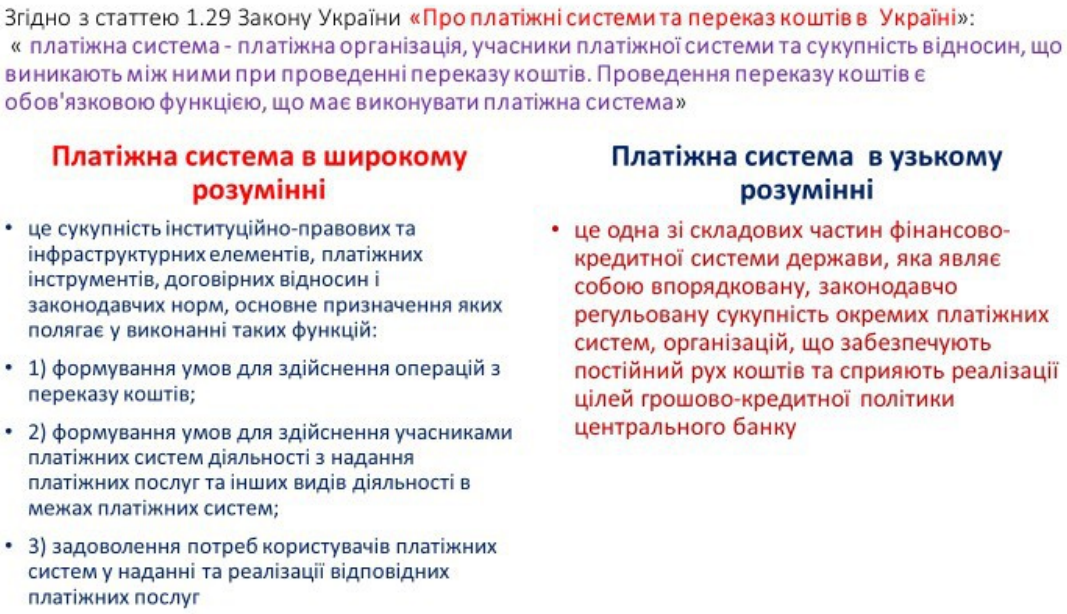


Рисунок А.2 – Визначення платіжних систем

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 перерахувань, 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

Рисунок А.5 – Структура АІС комерційного банку

Рисунок А.6 – Структура АІБС

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

Рисунок А.8 – Перспективи розвитку платіжних систем

Рисунок А.9 – Інфраструктура як послуга IaaS

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

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			+

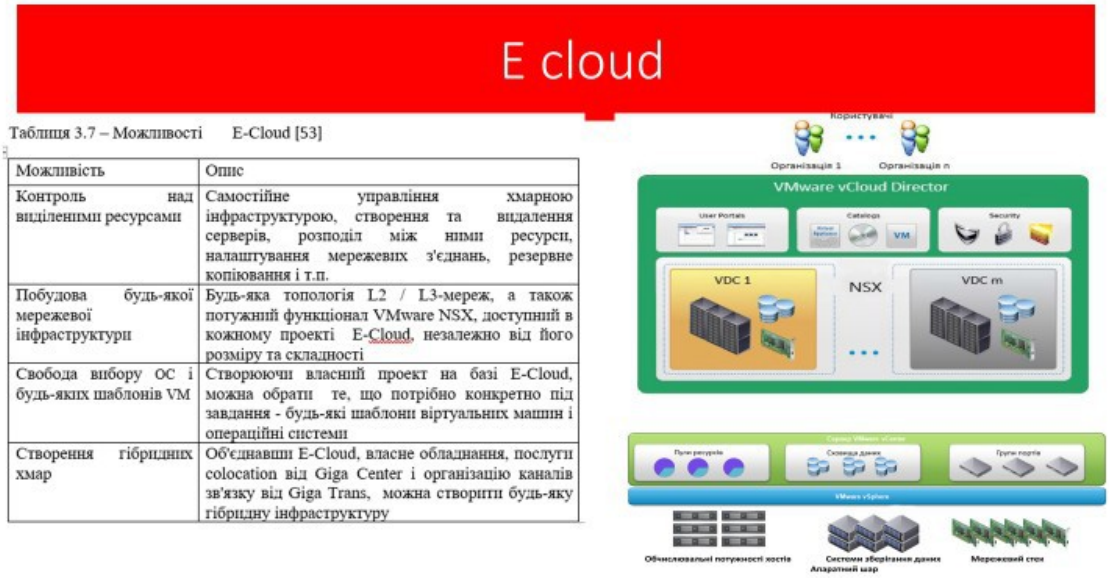
Рисунок А.13 – Порівняння можливостей хмарних технологій

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 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
RoamBeer [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 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

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



Таблиця 3.7 – Можливості E-Cloud [53]

Можливість	Опис
Контроль над виділеними ресурсами	Самостійне управління хмарною інфраструктурою, створення та видалення серверів, розподіл між ними ресурсів, 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

Рисунок А.15 – E cloud

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

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

№ OWASP топ 10	№ CAPEC	Назва атаки	Мета (контекст) атаки	Технічні наслідки успішної реалізації
A6:2020-Неправильне налаштування ІБ	CAPEC-25	Циклічне блокування декількох паралельних процесів, завершення яких залежить від попередника	Доступність	Відмова роботи ІС через вичерпання доступних ресурсів
A7:2020-між. сайт. скриптинг	CAPEC-63:	Міжсайтовий скриптинг (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 конфігураційним файлом	Конфіденційність, контроль доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних

Рисунок А.17 – Аналіз найпопулярніших кібертак 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

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

Змін.	Арк.	Номер докум.	Підпис	Дата
Розробив		Дерев’янко		
Перевір.		Золотарьов		
Н. контр.		Золотарьов		
Затв.		Безрук		

Дослідження інфокомунікаційних складових платіжних систем

Літ.	Аркуш	Аркушів
У	1	1

ХНУРЕ кафедра ІМІ