DOI: 10.15587/2312-8372.2018.134981

ДОСЛІДЖЕННЯ МОДЕЛЕЙ РОЗГОРТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Баглай Р. О.

1. Вступ

В силу особливостей діяльності, регуляторних вимог та побудови бізнес процесів системні універсальні банки оперують великими обсягами даних та мають комплексні інформаційні технології (надалі ІТ) ландшафту. Застосування хмарних технологій дозволяє значно підвищити ефективність ІТ в цілому. Крім цього, підвищується відомовостійкість, гнучкість та масштабованість банківських ІТ, а також показник швидкості виводу продуктів на ринок (від англ. time to market, надалі ТТМ). Разом із тим існують значні регуляторні обмеження щодо переміщення даних до хмари. В ході дослідження буде обґрунтовано можливість отримання цих переваг хмарних технологій без порушення регуляторних вимог.

Тому актуальним є дослідження моделі розгортання Public Cloud, адже така модель дозволяє отримати найкращі цінові пропозиції щодо вартості сервісу, оскільки датацентри постачальників розташовуються у регіонах з мінімальною вартістю ресурсів.

2. Об’єкт дослідження та його технологічний аудит

Об’єктом дослідження є банківські інформаційні технології.

В контексті Євроінтеграції українські системні банки мають бути готовими до радикальної модернізації клієнтських, операційних та звітних систем. Впровадження Європейських регуляторних вимог є складною проблемою для служб ІТ будь-якого українського банку. Вирішення проблеми лежить в площині застосування новітніх ІТ технологій, зокрема побудови архітектури ІТ банку, які базуються на хмарних сервісах.

Основна цінність банку – це дані. Володіння клієнтськими даними накладає цілу низку регуляторних обмежень, таких як Уніфіковане положення щодо захисту даних (англ. General Data Protection Regulation, надалі GDPR), та інших. Це породжує юридичні та операційні ризики, пов'язані з тим, що банк у будь-який момент часу повинен контролювати клієнтські дані та забезпечувати їх конфіденційність, цілісність та доступність. Автор вважає, що саме з цим пов’язано більшість регуляторних обмежень та заборон щодо переходу на хмарні технології в різних правових системах.

3. Мета та задачі дослідження

Метою даної роботи є дослідження перспективних напрямів застосування хмарних технологій на різних рівнях ІТ ландшафту для банківських ІС, для скорочення витрат та підвищення ефективності підтримки ІТ для бізнес-процесів банку.

Для досягнення поставленої мети необхідно виконати такі задачі:

1. Скласти високорівневу архітектурну схему інформаційних технологій ландшафту банку.

2. Згрупувати системи, визначити їх функціональне призначення, проаналізувати кількісні та якісні показники.

4. Дослідження існуючих рішень проблеми

Проблеми застосування хмарних технологій в різних соціально-економічних сферах досліджувались у роботі [1].

Серед основних напрямків вирішення проблеми застосування моделей розгортання Public Cloud та Hybrid Cloud, виявлених в ресурсах світової наукової періодики, можуть бути виділені публікації [2–4]. У цих публікаціях враховано специфіку забезпечення захисту інформації, що становить банківську таємницю, але не міститься пропозицій щодо деперсоналізації даних. Зокрема, робота [5] присвячена вирішенню проблеми конфіденційності даних шляхом шифрування, але це накладає істотні обмеження щодо обробки даних.

Праці інших науковців [5–7] не враховують в повній мірі специфіку забезпечення безпеки ІТ для банківських установ.

Роботи [8–10] містять пропозиції щодо використання хмарних технологій, але не містять комплексного аналізу щодо архітектури банківських інформаційних систем (надалі ІС) на основі хмарних технологій з урахуванням регуляторних обмежень.

Таким чином, результати аналізу дозволяють зробити висновок про те, що впровадження хмарних технологій в ІТ ландшафт банків України, має відповідати регуляторним вимогам. Зокрема, нормативно-правовим актам Національного банку України [11], Європейського центрального банку [12], Базельського комітету з банківського нагляду, Ради стандартів безпеки платіжних карт, та інших установ. Такі особливості зумовлюють специфіку побудови архітектури ІТ та організації системи безпеки, що визначає необхідність вивчення механізмів забезпечення операційної ефективності та захисту від загроз безпеки ІТ для банків.

5. Методи досліджень

При дослідженні були використані наступні наукові методи:

- графічний метод – при вивчені архітектурних схем ІС;
- метод класифікації систем – при визначенні пріоритетних напрямів застосування різних моделей розгортань хмарних технологій;
- метод кількісного аналізу – при вивченні нефункціональних вимог до банківських ІС;
- метод синтезу – при формуванні вибірки систем, які несуть найбільше навантаження і є критичними щодо безперервності бізнесу.

6. Результати дослідження

Згідно роз’яснень Національного Банку України (надалі НБУ), застосування хмарних технологій в діяльності банківських установ України можливе за умови розташування даних на серверах, що знаходяться на території України. Це

відповідає моделі розгортання Private Cloud. Розглянемо моделі розгортань On-Premise, Private Cloud, Public Cloud. Hybrid Cloud більш докладно.

Public Cloud. За такої моделі розгортань постачальник хмарних сервісів, наприклад, Amazon Web Services (AWS) або Microsoft Azure, володіє обчислювальними ресурсами та підтримує їх, надаючи доступ клієнтам через мережу інтернет. Ресурси спільно використовуються та розподіляються між всіма користувачами. Така модель також відома як орендне середовище багатьох користувачів (англ. multi-tenant environment). За рахунок економії масштабів розташування дата центрів в місцях з мінімальною вартістю ресурсів, постачальники хмарних сервісів мають змогу надавати ресурси за набагато нижчою ціною, ніж вартість підтримки власної інфраструктури.

Private Cloud. За такої моделі розгортань банк створює та підтримує хмарну інфраструктуру у власному дата центрі або на орендованих потужностях. Основна відмінність від Public Cloud полягає в тому, що банк – це єдиний користувач, який володіє і використовує ресурси приватної хмари. Така модель розгортань відома як орендне середовище одного користувача (від англ. single-tenant environment). Private Cloud не має таких переваг щодо економії витрат як Public Cloud, але все ж дозволяє використовувати функціональні переваги хмарних сервісів для підвищення ефективності бізнес-процесів банку.

Hybrid Cloud. За гібридної моделі розгортань поєднуються хмарні технології. Public та Private Cloud для отримання переваг обох моделей. Автор вважає, що саме така модель дозволить максимально убезпечити дані, водночас отримавши переваги економічної ефективності Public Cloud.

On-Premise – модель розгортання, при якій інформаційні активи (дані, програмне забезпечення, процеси), розміщуються на власних фізичних серверах банку. При цій моделі банк несе максимальні витрати – капітальні інвестиції, операційні витрати на підтримку та комунальні платежі, амортизація. Така модельне передбачає отримання функціональних переваг хмарних сервісів.

Розглянемо основні типи архітектурних ландшафтів банківських ІС:

Монолітна архітектура – комплексне рішення ІТ, що включає в себе фронт енд, автоматизовану банківську систему, головну бухгалтерську книгу, підсистеми налаштування банківських продуктів та сховище даних від одного постачальника. Зазвичай призводить до тотальної залежності від постачальника (від англ. Vendor lock in situation) зменшення гнучкості у задоволенні потреб банку та погіршення ТТМ.

Модульна архітектура – рішення ІТ, що базується на великій кількості програмних модулів від різних постачальників та внутрішніх розробників, які інтегровані між собою через корпоративні шини даних (від. англ. Enterprise serial bus) з дотриманням принципів сервісно-орієнтованої архітектури (від англ. Service Oriented Architecture). Недоліком такої архітектури зазвичай є високі витрати ресурсів для підтримки та розвитку складного інтегрованого ландшафту ІТ, що сповільнює ТТМ. Крім того це породжує необхідність створення та розвитку внутрішніх центрів компетенції, які здійснюють зміни на рівні корпоративної шини даних.

Мікросервісна архітектура базується на мікро сервісах, що використовують події, які породжуються програмними додатками, перетворюючи їх в процеси, що забезпечують виконання сценаріїв бізнес логіки, шляхом застосування стандартизованих механізмів та API функцій. Така архітектура є найбільш інноваційною, адже дозволяє в повній мірі використати потенціал хмарних технологій, значно зменшуючи показник TTM для банківських установ.

Запропоновано розглянути умовний банк, в архітектурному ландшафті якого поєднуються другий і третій тип архітектури. З метою визначення кількісних та якісних параметрів, які будуть взяті за основу для визначення функціональних та нефункціональних вимог до банківських ІС пропонується наступний сценарій:

- банк має ліцензію НБУ та здійснює діяльність у всіх клієнтських сегментах бізнесу – обслуговування фізичних та юридичних осіб, міжнародних корпорацій, державного сектору, надає казначейські послуги;
- клієнтська база налічує до 15 млн. клієнтів;
- кількість відділень 2 тис. (до 10 працівників одночасно працюючих на одне відділення в годину пік);
- кількість операцій до 50 млн. в день, половину в годину пік;
- кількість клієнтських рахунків 25 млн.

Високорівнева архітектурна схема IT ландшафту банку (рис. 1) складається з наступних функціональних блоків програмних додатків:

1. Клієнтські ІС/програмно-апаратні комплекси публічного доступу (англ. Public channels).
2. Системи управління відносинами з клієнтом (англ. Customer Relationship Management, надалі CRM).
3. Забезпечення міжсистемної взаємодії, інтеграційний шар (англ. Integration layer).
4. Операційні банківські системи (англ. Back end systems).
5. Системи управління даними (англ. Enterprise data management).

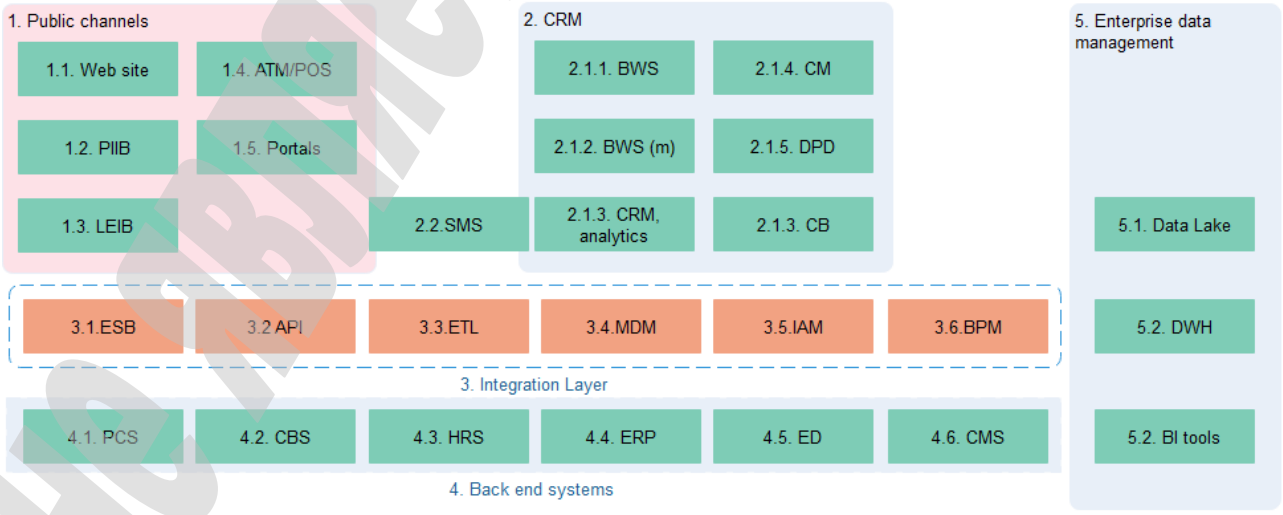

Рис. 1. Високорівнева архітектурна схема інформаційних технологій ландшафту банку

Розглянемо ці блоки більш докладно:

1. *Клієнтські ІС/програмно-апаратні комплекси публічного доступу* включають в себе програмні додатки та апаратні засоби для взаємодії з клієнтами банку, фізичними та юридичними особами. Ці системи несуть велике навантаження з точки зору кількості користувачів, що одночасно використовують функціонал (кількість активних сесій користувачів). Крім того доступ з публічних мереж збільшує ризик порушення цілісності внаслідок зовнішніх атак. Для підтвердження автентичності платіжних транзакцій має використовуватися електронний цифровий підпис (надалі ЕЦП). Доступність цих систем напряму впливає на безперервність бізнесу, тому час відновлення цих систем має бути мінімальним.

2. *Системи управління відносинами з клієнтом* включають в себе програмні додатки для введення, обробки та аналізу клієнтських даних, що здійснюється працівниками банку. Ці системи несуть значно менше навантаження, з точки зору кількості користувачів і зазвичай не мають інтерфейсів для доступу з публічних мереж. Для підтвердження автентичності платіжних транзакцій має використовуватися ЕЦП. Доступність цих систем має менший вплив на безперервність бізнесу тому рівень сервісу з відновлення (від англ. Service Level Agreement, надалі SLA) може передбачати більший час відновлення, ніж для систем з функціонального блоку № 1 і № 3.

3. *Забезпечення міжсистемної взаємодії, інтеграційний шар* включає в себе системи, які забезпечують можливість обміну та трансформації даних між програмними додатками. Ці системи несуть велике навантаження з точки зору кількості транзакцій, що обробляються в режимі он-лайн (від англ. Online Transaction Processing, надалі OLTP) від інтегрованих між собою систем, часто відіграючи роль транспорту або джерела даних для всіх інших систем. В окремих випадках може бути передбачено доступ з публічних мереж, що збільшує ризик порушення цілісності внаслідок зовнішніх атак. Доступність цих систем безпосередньо впливає на безперервність бізнесу, тому час відновлення цих систем має бути мінімальним.

4. *Операційні банківські системи включають* в себе системи обробки документів для обліку та формування звітності за операціями банку, обробки подій, які генеруються системами функціональних блоків № 1–3 та відображення результату цих подій в балансі банку. Окремі системи, зокрема автоматизований операційний день банку (від англ. Core Banking System, надалі CBS), несуть велике пікове навантаження під час оперативної аналітичної обробки даних (від англ. Online Analytical Processing, надалі OLAP) для виконання регламентних розрахункових процесів закриття операційного дня і формування щоденної звітності. В окремих випадках може бути передбачено доступ з публічних мереж, що збільшує ризик порушення цілісності внаслідок зовнішніх атак. Доступність цих систем значною мірою впливає на безперервність бізнесу, тому час відновлення цих систем має бути близьким до мінімального.

5. *Системи управління даними включають* в себе сховища структурованих (від англ. Data Warehouse, надалі DWH) і неструктурованих

даних (від англ. Data Lake) та інструменти перетворення та аналізу даних (від. англ. Business Intelligence Tools, надалі BI tools) для аналізу, візуалізації даних для формування регуляторної і управлінської звітності та прийняття рішень. Доступ з публічних мереж не надається. Доступність цих систем не вливає на безперервність бізнесу, тому SLA з відновлення може передбачати більший час відновлення ніж для систем з функціонального блоку № 1–4. Однак, варто зазначити, що ці системи часто є джерелом для формування регуляторної звітності, зокрема згідно Міжнародних стандартів фінансової звітності, тому їх недоступність більше доби вплине на своєчасність надання звітності до НБУ та Європейських регуляторів.

Функціональне призначення банківських ІС. Дамо коротке визначення функціонального призначення кожної із систем, які входять до зазначених вище функціональних блоків.

1. Клієнтські ІС/програмно-апаратні комплекси публічного доступу (від англ. Public channels):

1.1. Веб сторінка банку/Контакт центр (від англ. Web site). Призначена для розміщення структурованого контенту щодо продуктів банку з можливістю інтерактивного чату з працівниками контакт центру для клієнтів банку.

1.2. Інтернет банкінг для фізичних осіб (Private individuals Internet banking, PIIB). Призначена для управління власними рахунками та картками для клієнтів банку, фізичних осіб.

1.3. Інтернет банкінг для юридичних осіб (Legal Enteties Internet Banking, LEIB). Призначена для управління власними рахунками, кредитними лініями, зарплатними проектами для клієнтів банку, юридичних осіб.

1.4. Бакомати, POS термінали (від англ. Automated teller machine, Point of sale terminal, ATM, POS). Призначені для здійснення розрахункових операцій з платіжними картками для клієнтів банку.

1.5. Портали партнерів (від англ. Portals). Призначені для надання платіжних сервісів для клієнтів банку.

2. Система управління відносинами з клієнтом (CRM) призначена для комплексного обслуговування клієнтів, аналізу клієнтських даних і розробки рішень щодо пропозицій продуктів банку, що відповідають потребам клієнтів, на основі аналізу профілю клієнта, рейтингу ризику, політик банку.

2.1.1. Автоматизоване робоче місце (від англ. Branch work station, BWS) працівника відділення. Призначене для відкриття рахунків, видачі та обліку платіжних карток, касових платіжних операцій, валютобмінних операції, ведення анкети клієнта, фінансовий моніторинг.

2.1.2. Автоматизоване робоче місце – мобільний додаток (від англ. Branch work station, BWS). Призначена для оформлення зарплатних проектів, споживчих кредитів управління електронною чергою відділення для мобільних банкірів, заведення клієнтських кредитних заявок.

2.1.3. Система аналізу клієнтських даних та прийняття рішень (від англ. Customer relationship management, analytics). Призначена для аналізу профілю клієнта, на основі рейтингу ризику, розрахунків кредитних лімітів пропозиції щодо перехресного продажу продуктів для клієнтів банку.

2.1.4. Система управління заставним майном (від англ. Collateral management, CM). Призначена для реєстрації та збереження даних фото фіксації і оцінки заставного майна для підрозділів ризик менеджменту банку.

2.1.5. Система управління заборгованістю клієнтів (від англ. Days past due system, DPDS). Призначена для автоматичного розрахунку днів простроченої заборгованості для підрозділів ризик менеджменту банку.

2.1.6. Кредитне бюро (від англ. Credit burea, CB) – база даних проблемних позичальників для підрозділів ризик менеджменту банку.

2.2. Система автоматизованої доставки повідомлень клієнтам (від англ. Short message system, SMS). Призначена для доставки інформаційних повідомлень щодо кампаній акційних пропозиції, індивідуальних умов обслуговування для клієнтів банку.

3. Забезпечення міжсистемної взаємодії, інтеграційний шар:

3.1. Корпоративна шина даних (від англ. Enterprise service bus, ESB) призначена для забезпечення міжсистемної інтеграції і взаємодії банківських ІС.

3.2. Система управління API (від англ. Application programming interface) призначена для надання відкритих API для інтеграції з зовнішніми системами в тому числі порталами, що надають платіжні сервіси клієнтам.

3.3. Система перетворення та реплікації даних (від англ. Extract, Transform, Load, ETL) призначена для забезпечення синхронізації великих масивів даних довідників для ІС банку.

3.4. Система еталонних клієнтських даних (від англ. Master data management, MDM) призначення слугувати єдиним джерелом еталонних даних щодо клієнтів банку та он-лайн синхронізації з іншими системами банку, в яких містяться клієнтські дані.

3.5. Система управління обліковими даними та доступом користувачів (від англ. Identity and Access Management, IAM) призначена для забезпечення сильної автентифікації для зовнішніх і внутрішніх користувачів банківських ІС, динамічного управління їх правами доступу.

3.6. Система управління бізнес-процесами (від англ. Business process management, BPM) призначена для управління, автоматизації та роботизації внутрішніх процесів банку для підрозділів операційного сервісу.

4. Операційні банківські системи:

4.1. Продуктовий каталог (від англ. Product catalog system, PCS) призначений слугувати єдиним джерелом еталонних даних щодо продуктів банку та синхронізації з іншими системами банку, в яких містяться продукти банку.

4.2. Автоматизований операційний день банку (CBS) призначений для виконання функції головної бухгалтерської книги, виступаючи джерелом даних щодо активів та пасивів та щоденного балансу банку для НБУ.

4.3. Система управління людськими ресурсами (від англ. Human Resources System) призначена для управління режимом роботи та оплатою праці для працівників відділу кадрів банку.

4.4. Система обліку господарських операцій банку (від англ. Enterprise Resource Planning, ERP) призначена для управління обліком основних засобів,

малоцінних та швидкозношуваних предметів та інших активів банку для підрозділів фінансової вертикалі банку.

4.5. Електронний документообіг (від англ. Electronic Document flow, ED) призначений для зберігання, обробки та затвердження електронних документів клієнтів банку.

4.6. Процесинг операцій з платіжними картками (від англ. Card management system, CMS) призначений для управління мережею POS терміналів та кіосків, банкоматів, розрахунку комісій та покриття, управління життєвим циклом пластикових карток для працівників операційного сервісу банку.

4.7. Інші окремі продуктові системи (other) призначені для обліку операцій казначейства, документарних послуг, кастодіальних операцій, оренди депозитних скриньок, продажу монет та дорогоцінних металів, тощо.

5. Системи управління даними:

5.1. Сховище даних призначене для зберігання структурованих даних з систем джерел даних і збагачення даних для формування бухгалтерської, управлінської, статистичної і оперативної звітності. Користувачі – підрозділи аналізу даних банку.

5.2. Data Lake – сховище, яке призначене для зберігання як структурованих так і не структурованих даних (зображення, електронні листи, відео-, аудіо-дані та ін.) для управління даними банку в широкому розумінні, від фінансової звітності до маркетингових кампаній.

5.3. Інструменти перетворення та аналізу даних (BI tools) призначені для аналізу, перетворення, візуалізації даних для формування регуляторної і управлінської звітності та прийняття рішень.

Нефункціональні вимоги до банківських ІС. Автор пропонує розділити нефункціональні вимоги на блоки, які відповідають наступним якостям інформації:

- конфіденційність даних;
- цілісність даних;
- автентичність;
- доступність даних (в тому числі продуктивність ІС).

Конфіденційність означає, що дані, особливо ті, які становлять банківську таємницю мають бути захищеними від несанкціонованого розкриття. GDPR регламентує вимоги щодо захисту персональних даних та забезпечення можливості їх видалення з усіх систем банку, на вимогу клієнта [7]. В умовах розгортання за моделлю Public Cloud банк не володіє і не розпоряджається ресурсами, крім того ресурси, які використовуються для зберігання, обробки та передачі даних клієнта розподілені між іншими користувачами. Це вступає в конфлікт з зазначеними вимогами.

Для вирішення цієї проблеми дані, що розміщуються у хмарі, необхідно максимально де персоналізувати. Деперсоналізацію даних можливо забезпечити шляхом розміщення всіх даних, що становлять банківську таємницю, застосувавши модель розгортання Private Cloud, а при міжсистемній взаємодії з Public Cloud обмінюватись виключно унікальним секретним ідентифікатором клієнта. Такий ідентифікатор може бути прив’язаний до

міжнародного номеру банківського рахунку (від англ. International Bank Account Number, надалі IBAN) у поєднанні з унікальним ідентифікатором клієнта системи еталонних клієнтських даних (від англ. Master Data Management, надалі MDM).

Такий підхід також дозволить виключити ризик несанкціонованого використання даних постачальниками хмарних сервісів. Адже існує гіпотеза про те, що глобальні IT корпорації, заволодівши даними клієнтів банків та отримавши ліцензії на фінансову діяльність, можуть становити загрозу для існування фінансових інституцій. Останні не зможуть конкурувати з ними в технологічному аспекті. Цілісність означає, що активи IT можуть бути змінені тільки уповноваженими сторонами в дозволений спосіб, що стосується даних, програмного та апаратного забезпечення. Зокрема для захисту «сеансового рівня» взаємодії відкритих інформаційних систем НБУ регламентовано використання криптографічного протоколу захисту на транспортному рівні версії 1.2 (Trasport Layer Security, надалі TLS) для забезпечення контролю цілісності та конфіденційності інформації [6].

Автентичність – означає, що виключно уповноважені користувачі можуть отримати доступ до інформаційних ресурсів і функціональних можливостей систем. Управління обліковими даними та доступом користувачів на базі хмарних сервісів (від англ. Identity as a Service, IDaaS) забезпечує сильну автентифікацію користувачів і мінімізує ризики, пов’язані з атаками, направленими на втручання в сесію і крадіжку облікових даних. На ринку IT наявні комплексні рішення від провідних постачальників. Такі рішення включають в себе – двофакторну автентифікацію користувачів, динамічне управління доступом користувачів на базі шаблонно-рольової моделі, федеративні сценарії для різних доменів безпеки, аудит подій доступу та інші можливості. Функціональні можливості здатні повністю забезпечити потреби банківських установ.

Доступність означає властивість системи забезпечувати вхід авторизованого користувача та безперебійну роботу функціональності згідно його потреб.

Для досягнення максимального економічного ефекту хмарні сервіси доцільно застосовувати до систем з великим навантаженням. Серед критеріїв: кількість операцій одночасно працюючих користувачів або велике пікове навантаження під час оперативної аналітичної обробки даних, що вимагає великої обчислювальної потужності. Хмарні технології також дозволяють досягти максимального рівня доступності обчислювальних ресурсів (тобто відсутності збоїв, які спричиняють зупинку бізнес-процесу) для систем, зупинка в роботі яких є найбільш небезпечною з точки зору операційних ризиків банку.

Для визначення таких систем автор пропонує застосувати наступні параметри (табл. 1) в контексті доступності:

- Доступність 24/7 – значення параметру так/ні, означає можливість цілодобового доступу для клієнтів банку до ІС банку в режимі он-лайн.
- RPO (від англ. Recovery point objective) – означає точку у часі, на яку можливо відновити дані у випадку зупинки бізнес-процесу в наслідок збою в роботі ІС, в хвилинах.

− RTO (від англ. Recovery time objective) – це SLA з відновлення бізнес-процесу після зупинки внаслідок збою в роботі ІС, в хвилинах.

В контексті продуктивності:

− DB size – від англ. Data Base size – обсяг бази даних ІС в терабайтах.

− OLTP1 – кількість активних клієнтських сесій, тобто одночасно працюючих користувачів в режимі онлайн в тисячах.

− OLTP2 – кількість запитів в тисячах одиниць до системи і відповідей від інших ІС, що обробляються за годину.

− OLAP – інтервал оновлення даних системи даними інших систем в хвилинах.

Таблиця 1

Системи банку з максимальним піковим навантаженням

№ системи	24/7	RPO	RTO	DB size	OLTP 1	OLTP 2	OLAP
3.1	Так	0	60	<1	<1	5000	–
3.5	Так	240	60	<1	200	5000	240
1.2	Так	5	60	2-4	50	1500	240
1.5	Так	5	60	<1	50	1500	240
3.2	Так	0	60	<1	<1	1500	–
3.4	Так	5	60	>10	10	1000	240
4.6	Так	5	60	2-4	50	1000	240
1.3	Так	5	60	2-4	10	300	240

Виходячи з аналізу вибірки, приведеної в табл. 1, автор вважає, що наступні системи несуть найбільше навантаження і є критичними щодо безперервності бізнесу та SLA по відновленню роботи:

3.1. Корпоративна шина даних.

3.5. Системи управління обліковими даними та доступом користувачів.

1.2. Інтернет банкінг для фізичних осіб.

1.5. Портали партнерів.

3.2. Система управління API.

3.4. Система еталонних клієнтських даних.

4.6. Процесинг операцій з платіжними картками.

1.3. Інтернет банкінг для юридичних осіб.

7. SWOT-аналіз результатів досліджень

Strengths. Застосування моделі розгортання Public Cloud дозволило б досягти максимального ефекту щодо економічної ефективності, скорочення витрат та операційної стабільності. Адже забезпечення таких параметрів вимагає значних інвестицій в ресурси апаратного забезпечення, які банк несе при застосуванні моделей Public Cloud та On-Premise.

Weaknesses. Окремі системи, зокрема, автоматизований операційний день банку (на архітектурній схемі 4.2. CBS), несуть велике пікове OLAP навантаження під час виконання регламентних розрахункових процесів

закриття операційного дня і формування щоденної звітності. При цьому, в денний час ресурси апаратного забезпечення фактично недоутилізовані, та використовуються неефективно.

Opportunities. Одним з найперспективніших напрямів застосування Hybrid Cloud та Public Cloud є автоматизований операційний день банку. Розгортання двох примірників цієї системи – Private Cloud для клієнтських даних та Public cloud для деперсоналізованих клієнтських даних.

Деперсоналізацію даних можливо забезпечити шляхом розміщення всіх даних, що становлять банківську таємницю, застосувавши модель розгортання Private Cloud, а при міжсистемній взаємодії з Public Cloud обмінюватись виключно унікальним секретним ідентифікатором клієнта. Такий ідентифікатор може бути прив'язаний до міжнародного номеру банківського рахунку IBAN в поєднанні з унікальним ідентифікатором клієнта системи MDM.

Результати дослідження можуть бути використані в банківській системі будь-якої країни світу.

Threats. Застосування моделі Public Cloud без деперсоналізації даних неможливе з огляду на те, що це порушує вимоги GDPR та НБУ. Деперсоналізувати дані і застосувати модель Public Cloud для складних процесів онлайн взаємодії є дуже складним завданням для практичної реалізації.

8. Висновки

1. Складено високорівневу архітектурну схему IT ландшафту банку та визначено функціональні блоки програмних додатків, з яких вона складається. Для кожного з блоків узагальнено вимоги щодо конфіденційності, цілісності та автентичності даних. Це лягло в основу для визначення пріоритетних напрямів застосування різних моделей розгортань хмарних технологій.

2. Визначено функціональне призначення кожної з основних систем IT ландшафту банку, їх функціональне призначення, проаналізовано кількісні та якісні показники, зокрема, щодо нефункціональних вимог до банківських ІС.

Отриманий результат в кількісному вираженні показників навантаження на систему дозволяє знайти додаткові резерви для оптимізації часу обробки інформації і підвищення економічної ефективності за рахунок застосування Public Cloud. Найбільшого ефекту можливо досягти, застосувавши цю модель до автоматизованого операційного дня банку (від англ. Core Banking System). Для дотримання вимог та урахування обмежень щодо розміщення клієнтських даних в роботі запропонований механізм деперсоналізації.

Література

1. Zissis D., Lekkas D. Addressing cloud computing security issues // Future Generation Computer Systems. 2012. Vol. 28, No. 3. P. 583–592. doi: http://doi.org/10.1016/j.future.2010.12.006

2. Apostu A., Rednic E., Puican F. Modeling Cloud Architecture in Banking Systems // Procedia Economics and Finance. 2012. Vol. 3. P. 543–548. doi: http://doi.org/10.1016/s2212-5671(12)00193-1

3. Nagaty K. A Framework for Secure Online Bank System Based on Hybrid Cloud Architecture // Journal of Electronic Banking Systems. 2015. Vol. 1–13. doi: http://doi.org/10.5171/2015.614386

4. Rahman M., Qi X. Core Banking Software(CBS) Implementation Challenges of e-Banking: An Exploratory Study on Bangladeshi Banks // Journal of Administrative and Business Studies. 2016. Vol. 2, No. 4. P. 208–215. doi: http://doi.org/10.20474/jabs-2.4.6

5. Ambodo B. S., Suryanto R., Sofyani H. Testing of Technology Acceptance Model on Core Banking System: A Perspective on Mandatory Use // Jurnal Dinamika Akuntansi. 2018. Vol. 9, No. 1. P. 11–22. doi: http://doi.org/10.15294/jda.v9i1.12006

6. Reeshma K. Challenges of Core Banking Systems // Mediterranean Journal of Social Sciences. 2015. Vol. 6, No. 5. P. 24–27. doi: http://doi.org/10.5901/mjss.2015.v6n5p24

7. Personalized Security Approaches in E-banking Employing Flask Architecture over Cloud Environment / Hamidi N. A. et al. // Procedia Computer Science. 2013. Vol. 21. P. 18–24. doi: http://doi.org/10.1016/j.procs.2013.09.005

8. Karthigainathan M. Cloud Computing for Rural Banking // International Journal Of Engineering And Computer Science. 2016. Vol. 5, No. 9. P. 17880–17884. doi: http://doi.org/10.18535/ijecs/v5i9.15

9. Grivas S., Schurch R., Giovanoli C. How Cloud Will Transform the Retail Banking Industry // Proceedings of the 6th International Conference on Cloud Computing and Services Science. 2016. Vol. 1. P. 302–309. doi: http://doi.org/10.5220/0005910903020309

10. Bobyl V. V., Dron M. A. «Khmarni» tekhnolohii yak faktor zbilshennia operatsiinoho ryzyku banku // Bankivska sprava. 2014. No. 11–12. P. 47–62. URL: http://lib.sumdu.edu.ua/library/DocDescription?doc_id=441341 (Last accessed: 24.12.2017).

11. Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy: Resolution of the Board of the National Bank of Ukraine No. 95 from 28.09.2017 // Baza danykh «Zakonodavstvo Ukrainy» VR Ukrainy. URL: http://zakon2.rada.gov.ua/laws/show/v0095500-17 (Last accessed: 24.12.2017).

12. General Data Protection Regulation: Directive of European Parliament and of the Council of 27.04.2016 No. 95/46 // European Union Law data base. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (Last accessed: 24.12.2017).