

Д. І. Угрин¹, С. Ф. Шевчук¹, Б. М. Гаць², О. А. Баляснікова¹
¹Чернівецький факультет Національного технічного університету
“Харківський політехнічний інститут”,
²ПВНЗ “Буковинський університет”, м. Чернівці

ПЛАНУВАННЯ ТА МОДЕЛЮВАННЯ ПЛАТФОРМИ ТУРИСТИЧНОГО БІЗНЕСУ НА ОСНОВІ ХМАРНОЇ ТЕХНОЛОГІЇ ТА ЗАХИСТ ЇЇ ДАНИХ

© Угрин Д. І., Шевчук С. Ф., Гаць Б. М., Баляснікова О. А., 2015

Описано інфраструктуру хмарних технологій для розроблення платформи планування туристичного бізнесу та запропоновано її архітектуру, що ґрунтується на п'яти рівнях виконання обслуговування туристичного бізнесу. Також описано бібліотеку програмних модулів для вирішення оптимізаційних завдань і планування безпеки даних платформи туристичного бізнесу.

The paper describes the infrastructure of cloud technology platform for the development of tourism business planning and proposes its architecture, based on five performance levels of service tourist business. Also a library of software modules to address optimization tasks and planning data security platform tourism are described.

Keywords: information platform planning tourism business, cloud computing, data protection and security, information services infrastructure of tourism.

Ключові слова: інформаційна платформа планування туристичного бізнесу, хмарні обчислення, захист і безпека даних, сервіси інформаційної інфраструктури туризму.

Вступ

Технологія хмарних обчислень є однією з найперспективніших напрямків розвитку інформаційних технологій, які сьогодні розглядаються як альтернативи традиційної моделі обробки інформації. З використанням систем хмарних обчислень реалізують віддалену обробку інформації [1], що забезпечує досягнення високих показників відмовостійкості та доступності інформаційної інфраструктури різних сфер діяльності, зокрема туристичної.

Схожість сервісних процесів окремих напрямів організацій туристичної галузі у різних областях діяльності робить можливим розробку та впровадження типових програмних рішень для планування розвитку туристичного бізнесу. Проте впровадження великої кількості “локального” програмного забезпечення на територіально-розподілених туристичних організаціях призводить до істотних витрат тимчасових і матеріальних ресурсів для своєчасного передавання нових версій замовникам, настроювання, супроводу, оновлення, внесення змін, а також моніторингу роботи програмного забезпечення.

Загальна постановка проблеми

Практична реалізація концепції хмарних обчислень при вирішенні завдань планування туристичного бізнесу вимагає розроблення програмного комплексу (платформи), що матиме широкий діапазон функціональних можливостей та захисту даних. Це забезпечить впровадження та супровід програмного забезпечення та вирішення оптимізаційних завдань, що виникають у туристичних агентствах і інших організаціях цієї сфери (готелів, туристичних комплексів, баз лікування та відпочинку). Крім того, хмари як засоби індивідуального та публічного користування повинні забезпечувати належний рівень захисту даних та різного роду загроз.

Виклад основного матеріалу

Для застосування інтегрованих даних у платформі туристичного бізнесу необхідно сконцентрувати у єдиній системі збереження, опрацювання та доступ до даних. Сьогодні хмари поділяють за такою класифікацією:

1. Приватна хмара (private cloud) забезпечує виняткове обслуговування єдиною організацією, що об'єднує різноманітних користувачів (бізнес-одиниць). Інфраструктура може існувати як на боці споживача, так і у зовнішнього провайдера. Вона може перебувати у власності, контролюватися і управлятися самою організацією або третьою стороною чи їх комбінацією. Такий вид хмари буде корисним для туристичних комплексів невеликого масштабу, що діють незалежно від інших туристичних організацій місцевості чи регіону.

2. Громадська хмара (community cloud) забезпечує своє використання обмеженим числом споживачів з організацій, що мають спільні інтереси (наприклад, об'єднання лікувальних та оздоровчих закладів регіону, які мають єдині вимоги до політики безпеки, відповідності певним нормативним документам тощо). Така хмарна інфраструктура може перебувати у власності, контролюватися однією або низкою організацій у співтоваристві, третьою стороною або їх комбінацією і може існувати на боці як споживача, так і зовнішнього провайдера.

3. Публічна хмара (public cloud) надає можливість для відкритого використання громадськістю. Хмара може бути власністю, контролюватися, управлятися комерційною, науковою, урядовою організацією або їх комбінацією. Такого роду хмара об'єднує управління з питань туризму, туристичні організації різного роду та власне самого туриста – споживача цієї галузі.

4. Гібридна хмара (hybrid cloud) утворює композицію з двох і більше хмар (приватних, публічних або громадських), що залишаються унікальними за своєю сутністю, але об'єднані разом стандартизованими або пропріетарними технологіями, що забезпечують переносимість (мобільність) даних і додатків між хмарами (наприклад, такими технологіями, як пакетне передавання даних для балансування навантаження між хмарами).

Для кожного окремого випадку розвитку туристичної діяльності будуть підходити різні види хмар. Для діяльності окремого туристичного агентства якнайкраще підходить приватна хмара. Вона може бути розміщена централізовано (локально) або може бути розподіленою за кількома територіально розташованими туристичними організаціями. Рис.1 ілюструє локальну приватну хмару [2].

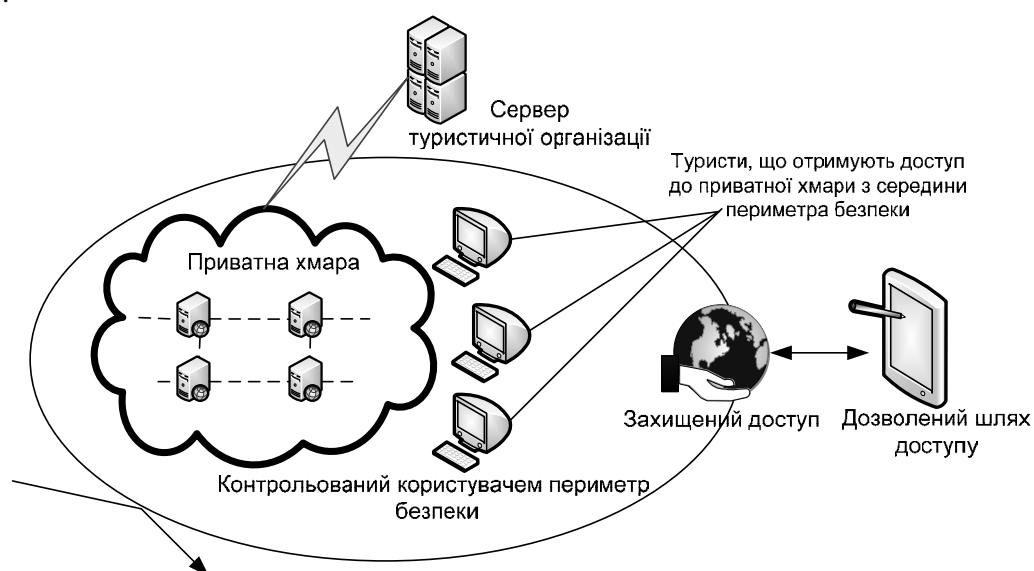


Рис. 1. Локальна приватна хмара

Як видно, інфраструктура хмари і ресурси споживачів (туристів) розташовуються в середині власного периметра безпеки. У приватній хмарі застосовні вже всі існуючі в організації заходи захисту даних і додатків. Перенесення додатків, баз даних і систем зберігання в приватній хмарі не

знижують захищеності даних. Власне це і є перевагою приватної хмари порівняно з іншими моделями розгортання.

Для туристичної організації, що використовуватиме хмару, важливим буде питання: чи є принципові відмінності між приватною та публічною хмарами? Насамперед це низька вартість послуг, якої досягають завдяки стандартизації та уніфікації рішень у публічній хмарі, що неприйнятно для приватної хмари, оскільки послуги чи сервіси, наприклад, для кожного туристичного агентства, є унікальними, і прийняті в ній технології та рішення забезпечують потрібний результат.

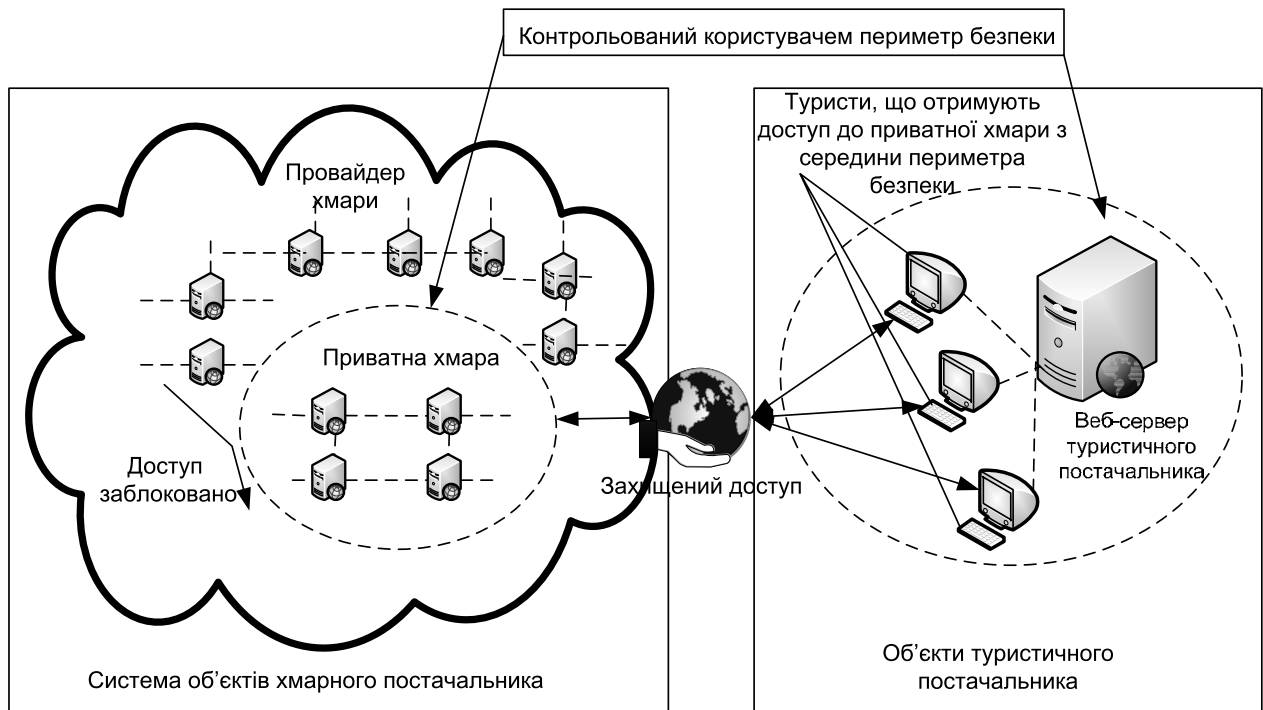


Рис. 2. Приватна хмара, передана на аутсорсинг хмарному провайдеру

Крім того, в публічних хмарах можуть реалізовуватися апаратно-програмні рішення. Такі рішення найбільш функціональні і гнучкі, але, як правило, доволі дорогі [3]. Втілювати або купувати такий інструментарій економічно доцільно тільки для великих туристичних комплексів, що об'єднують декілька видів діяльності. Мабуть, тільки публічна хмара економічно здатна на належному рівні забезпечити еластичність наявної інформаційної інфраструктури, наприклад, внаслідок вимоги додаткових ресурсів на відносно короткий термін, її проактивність і тісну інтеграцію з бізнес-процесами туристичної організації, а також вирішити питання забезпечення інформаційної безпеки, дотримання політик, необхідних для того чи іншого виду послуг [3].

Використання хмарних технологій для розроблення платформи планування туристичного бізнесу

Платформа планування туристичного бізнесу повинна містити такі основні компоненти:

- бібліотеки типових програмних модулів, що реалізують основні оптимізаційні алгоритми ведення обслуговувальних та супровідних сервісів;
- “хмарні” сервіси планування та управління складними обслуговувальними процесами туристичних центрів;
- бази та сховища даних пропозицій клієнтам і умови їх перебування під час надання туристичних послуг;
- допоміжні сервіси.

Бібліотеки типових програмних модулів проєктованих систем туризму створюються на основі розроблених раніше математичних моделей і методів для розв'язання оптимізаційних задач, які виникають під час планування та управління туристичними комплексами і лікувально-оздоровчими базами, зокрема задач туристичних фірм для пільгових та гарячих путівок, а також організації і реклами турів.

“Хмарні” сервіси планування та управління складними туристичними процесами від туристичних агентств та операторів до готелів, відпочинково-лікувальних та спортивних баз розробляється окремо, залежно від виду туристичних послуг. У межах прототипування необхідної консолідованої платформи пропонується розробити такі основні рішення:

- сервіс готельного та ресторанного бізнесу – для планування, організації та управління послугами щодо бронювання, розселення, проживання і харчування туристів, зокрема надання сервісів економ-класу з використанням для проживання і харчування хостелів та дешевих кафе із врахуванням у всіх послугах туристам транспортних перевезень;
- сервіс оздоровчого та лікувального бізнесу – для оптимізації процесів планування і управління відпочинком чи лікуванням туристів, зокрема надання лікувально-оздоровчих послуг у віддалених медичних закладах з урахуванням транспортних перевезень;
- сервіс історичного та спортивного бізнесу – для планування, організації та управління послугами туристам з підбором груп для маршрутів історичного, релігійного значення, а також спортивного та іншого активного виду туризму.
- сервіс туристичних турів – для планування та управління повним та частковим наданням туристичних послуг.

Незважаючи на зовнішню відмінність перерахованих вище сервісів, у багатьох випадках оптимізаційні завдання кожного сервісу можуть бути сформульовані і вирішені як окремі випадки багатоцільової туристичної задачі. Перелік запропонованих сервісів має бути відкритим і надалі доповненим необхідними для інших видів туризму.

Апаратна складова заданої платформи має бути представлена центром зберігання і обробки даних, що міститиме набір апаратно-програмних засобів для зберігання, обробки і передавання даних через зовнішні канали зв'язку, а також інфраструктуру для безперебійної роботи обладнання. Можна виділити такі базові компоненти центру зберігання і обробки даних:

- інформаційна інфраструктура – об'єднує сервери, дискові масиви та інше обладнання, що забезпечує інформаційне наповнення центру зберігання і обробки даних;
- телекомунікаційна інфраструктура – забезпечує з'єднання компонентів інформаційної платформи туризму та зв'язок з кінцевими користувачами системи;
- інженерна інфраструктура – містить систему безперебійного електропостачання для автономної роботи центру зберігання і обробки даних, систему кондиціонування та вентиляції приміщень для стабільної роботи центру, охоронну і пожежну сигналізацію.

Кінцевими споживачами послуг центру зберігання і обробки даних можуть бути комерційні структури туристичного бізнесу та державні організації, що пов'язані з туристичною сферою або фізичні особи, які зацікавлені у її розвитку [4].

Архітектура платформи планування туристичного бізнесу

Подамо програмну архітектуру платформи туристичного планування у вигляді схеми (рис.3) та зобразимо її у вигляді таких основних рівнів:

1. Система управління базами даних;
2. Сховище даних;
3. Сервер додатків;
4. Веб-сервер;
5. Клієнтське програмне забезпечення.

Система управління базами даних (перший рівень) відповідає за зберігання, наповнення та зміну даних, а також за надання інформації у відповідь на запити від сервера додатків. Платформа забезпечує роботу з різними СУБД, при цьому можуть бути використані бази даних створені в

середовищах Microsoft SQL Server або Oracle Database. Використання кластера серверів баз даних, що містить функції апаратного віддзеркалювання і резервного копіювання даних, забезпечує надійність, продуктивність і відмовостійкість платформи туристичного бізнесу.

Сховище даних (другий рівень) надає розвинені засоби інтеграції даних з різних джерел туристичних організацій та дає змогу працювати як з деталізованою, так і з агрегрованою інформацією, що надходить від засобів збереження туристичних даних. Для опрацювання даних використовуються технології уніфікованої консолідації, федералізації та розповсюдження шляхом застосування методів інтеграції даних з різних джерел, найпоширенішим з яких є підхід ETL (Extract, Transform, Load).

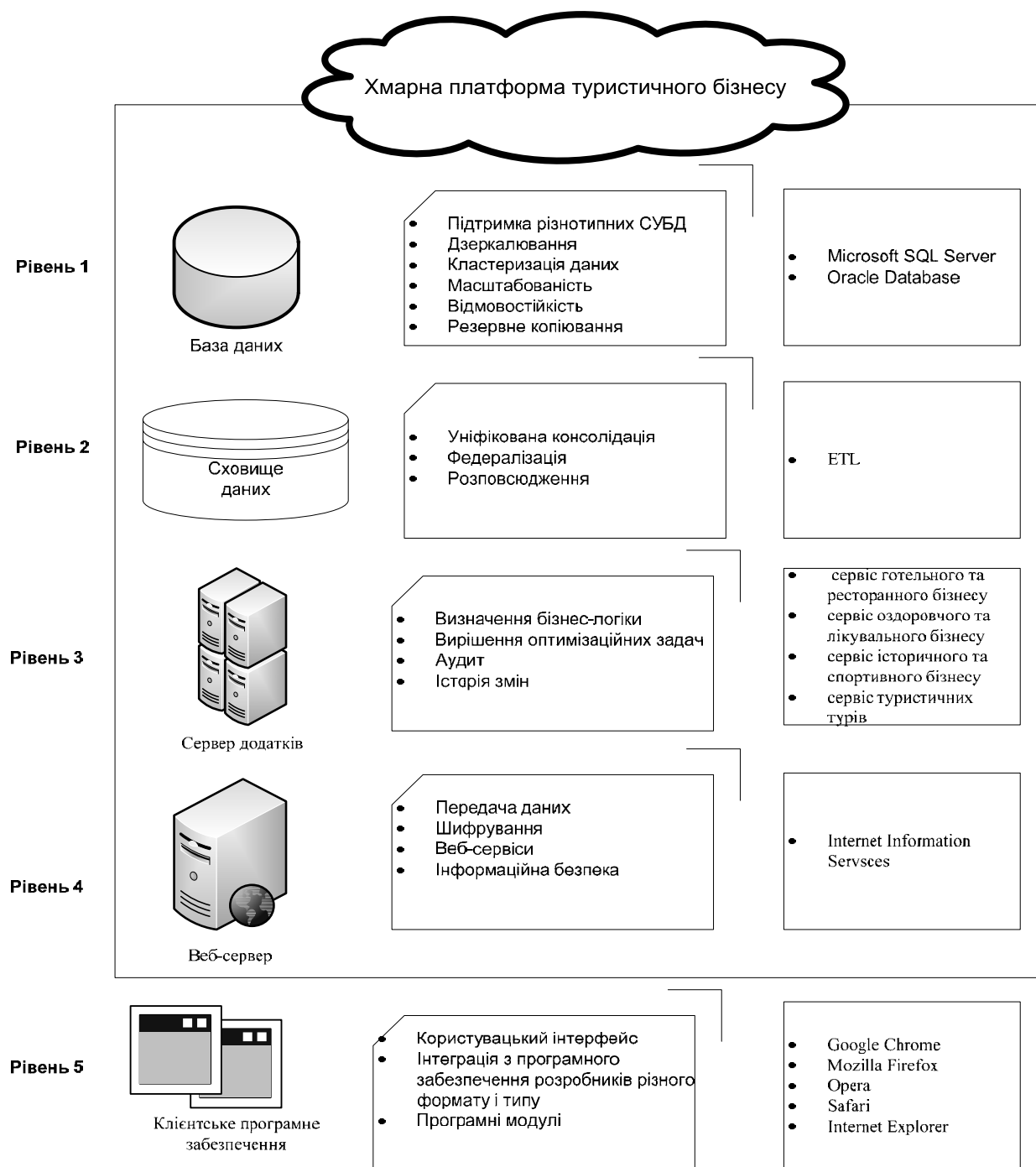


Рис. 3. Архітектура платформи планування туристичного бізнесу

Сервер додатків (третій рівень) оснований на бізнес-логіці програмних систем, що описують відповідні предметні області. Бізнес-логіка додатків об'єднує дані і сценарії та проектується у вигляді мережі взаємопов'язаних об'єктів. Всі алгоритми і математичні моделі реалізовані у вигляді програмних модулів з чітко регламентованим і документованим інтерфейсом доступу для забезпечення можливості використання різними програмними системами [6].

Сервер додатків фізично відділений від веб-сервера і експлуатується віддалено через зовнішні або внутрішні канали передавання даних, зокрема мережами Інтернет. Це дає змогу переносити частину обчислювальних витрат на віддалені сервери і тим самим скорочувати час для вирішення завдань, а також знижувати витрати на закупівлю обладнання. З використанням серверів у мережі Інтернет ця структура реалізує концепцію “хмарних обчислень”. Крім того, сервісний рівень надає допоміжні можливості для спрощення реалізації та аудиту програмних продуктів, отримання актуальної інформації про стан важливих частин програмних засобів, ведення журналу змін та інші.

Основним призначенням веб-сервера (четвертий рівень) є передавання даних клієнтського програмного забезпечення, яку подано у вигляді HTML розмітки і XML-коду, що генерується веб-сервісами, а також іншими форматами подання даних, що використовуються для обробки програмами-клієнтами. Крім того, веб-сервер шифрує канал передавання даних для безпеки клієнта і платформи туристичного бізнесу від несанкціонованого доступу. Як основну програмну реалізацію веб-сервера використовують Internet Information Services.

Клієнтське програмне забезпечення (п'ятий рівень) можна умовно подати як об'єднання трьох складових: користувацького інтерфейсу, інтеграції зі сторонніми програмними продуктами та обробки даних.

Основним компонентом користувацького інтерфейсу є веб-браузер, який формує візуальне уявлення продукту і передає дані шифрованим каналом зв'язку. Як основні використовують браузери Google Chrome, Mozilla, Firefox, Opera, Safari та Internet Explorer. Інтеграцію зі сторонніми програмними продуктами здійснюють за допомогою модулів, що гарантують взаємодію між програмною оболонкою і веб-сервером. Обробка даних являє собою сервіси, що використовують систему для вирішення складно структурованих задач вищого рівня.

Бібліотека програмних модулів для вирішення оптимізаційних завдань

Однією з основних складових платформи туристичного бізнесу є бібліотека програмних модулів сервера додатків для розв'язання оптимізаційних задач, що виникають під час планування та управління туристичними операторами і туристичними комплексами. Завдання суттєво ускладнюються через необхідність враховувати дискретність як організаційних процесів туристичних агентств, так і путівок; необхідністю зазначення послідовності виконання робіт, стохастичною природою туристичного процесу і т.д. Для вирішення таких завдань необхідні спеціальні засоби перетворення рішень. Нерідко обсяг обчислень, пов'язаних з такими перетвореннями, істотно вищий, ніж під час виконання основного завдання. Для виконання основного та допоміжних завдань у програмній бібліотеці потрібно реалізувати модуль “універсальний оператор рішень” для вирішення складних оптимізаційних задач планування туристичного бізнесу на основі матриці обмежень.

Матриця обмежень у прикладних задачах оптимізації, як правило, має доволі велику розмірність і яскраво виражену специфічну блочну структуру. З урахуванням великої кількості блоків матриці обмежень визначення та завдання їх взаємного розташування часто призводить до важких помилок. Тому в складі модуля “універсальний оператор рішень” необхідно реалізувати спеціальну структуру даних для підвищення ефективності зберігання і використання даних з урахуванням структури підматриць – “матричний конструктор”.

На основі модуля “універсальний оператор рішень” повинні бути реалізовані алгоритми вирішення завдань складного туристичного плану, враховуючи лінійні і нелінійні задачі оптимізації, багатоцільові завдання з комбінованими критеріями. Модуль забезпечує реалізацію методів лінійного, динамічного та дискретного програмування, ряду алгоритмів вирішення завдань опуклого програмування і схем декомпозиції, що дасть змогу з мінімальними витратами розв'язувати оптимізаційні задачі планування та управління туристичним комплексом.

Планування захисту і безпеки даних платформи туристичного бізнесу

Порівняно з традиційними інформаційними технологіями системи хмарних обчислень мають характерні особливості, які необхідно досліджувати щодо безпеки даних і враховувати під час аналізу захисту даних систем. До них належать:

1. Самообслуговування споживачів, що дає можливість самостійно отримувати доступ до інформаційних сервісів з необхідністю в односторонньому автоматичному режимі працювати без взаємодії з персоналом провайдера (в розумінні обслуговувальної системи, що використовує хмарні послуги);
2. Універсальність доступу з використанням інформаційно-телекомунікаційних мереж;
3. Можливість отримання доступу до інформаційних сервісів каналами інформаційно-телекомунікаційних мереж з використанням тонких або товстих клієнтів;
4. Висока консолідація обчислювальних ресурсів, що об'єднує обчислювальні ресурси в одній або декількох точках для обслуговування різних споживачів з можливістю динамічного призначення і перепризначення фізичних та віртуальних ресурсів відповідно до потреб споживачів;
5. Динамічна масштабованість, яка надає можливість оперативної автоматичної зміни продуктивності як у бік зменшення, так і у бік збільшення масштабів використання залежно від потреб споживача.

Ці особливості визначають основні переваги використання систем хмарних обчислень для споживачів, які полягають в оптимізації виробничих процесів завдяки зниженню капітальних і експлуатаційних витрат на власну інформаційну інфраструктуру.

Разом з тим ці особливості призводять до виникнення нових актуальних загроз інформаційній безпеці, пов'язаних, насамперед, зі зниженням рівня контрольованості процесів обробки інформації та з динамічністю моделі надання ресурсів. Так, з використанням систем хмарних обчислень у споживача немає можливості застосувати додаткові засоби обмеження доступу до інформації, такі як контроль фізичного доступу та інших організаційних і технічних заходів. Крім того, інформаційні впливи з боку недобросовісних споживачів можуть призвести до різкого скорочення кількості доступних обчислювальних ресурсів або невідповідності між вартістю споживання інформаційних сервісів і обсягом фактично використовуваних ресурсів.

Тобто, виникає істотне протиріччя між можливістю підвищення ефективності процесів туристичних послуг з використанням систем хмарних обчислень, з одного боку, і наявністю апріорно не розглянутих загроз інформаційній безпеці, а також відсутністю експлікації вимог інформаційної безпеки до систем хмарних обчислень – з іншого боку.

Зазначене протиріччя зумовлює необхідність детального аналізу загроз інформаційній безпеці, що виникають з використанням систем хмарних обчислень. Можна зазначити, що актуальність проблеми ідентифікації загроз інформаційній безпеці для систем хмарних обчислень зазначається в багатьох дослідженнях і аналітичних звітах [7, 8].

Для подальшого аналізу загроз інформаційній безпеці визначимо математичну модель інформаційної системи п'ятіркою множин (I, T, P, S, F) , де I – множина туристичної інформації, що обробляється в інформаційній системі; T – множина інформаційних технологій і технічних засобів; P – множина споживачів і персоналу провайдера; S – множина станів інформаційної системи; F – множина переходів з одного стану в інший, тобто $F: S \rightarrow S$.

Станом інформаційної системи $s \in S$ будемо називати набір властивостей (атрибутів) системи в окремий момент часу. З метою аналізу інформаційної безпеки для кожного стану системи введемо три атрибути безпеки інформації, що обробляється в системі: c_s – конфіденційність; i_s – цілісність; a_s – доступність, такі що $c, i, a \in \{0, 1\}$, причому $c = 1$ (аналогічно $i = 1$ і $a = 1$), якщо в цьому стані забезпечується конфіденційність (відповідно цілісність і доступність) інформації, що обробляється в системі. Стан $s \in S$ системи, в якому $(c_s, i_s, a_s) = (1, 1, 1)$, будемо називати безпечним станом, а множину всіх безпечних станів позначимо

$$S^+ = \{s \in S \mid (c_s, i_s, a_s) = (1, 1, 1)\}.$$

Стан, у якому хоча б один з атрибутів дорівнює нулю, будемо називати небезпечним. Множину небезпечних станів позначимо

$$S^- = \{s \in S \mid \exists k \in \{c_s, i_s, a_s\}, k = 0\}.$$

Тому

$$S^- \cup S^+ = S.$$

Інцидентом безпеки I_B в інформаційній системі назвемо перехід системи від безпечного стану в небезпечний стан, тобто

$$I_B = f \mid f \in F, F : S^+ \rightarrow S^-.$$

Модель загроз безпеки для інформаційних систем може бути представлена четвіркою множин (A, O, V, M) , де A – множина джерел загроз; O – множина об'єктів захисту; V – множина вразливостей; M – множина способів реалізації загроз, причому очевидно, що $M \subset F$.

Тому

$$O = \{o \mid o \in I \cup T \cup P\}.$$

Вразливістю $v \in V$ інформаційної системи будемо називати слабкість елемента системи $e \in T \cup P$, існування якої в певному стані системи $s \in S$ за наявності джерела загрози $Ag \in A$ може призвести до реалізації інциденту безпеки, тобто

$$V = \{v \mid v = e \bullet s \mid Ag \bullet s \Rightarrow In\}.$$

Загрозою безпеці τ назвемо комбінацію об'єкта захисту $o \in O$ і джерела загроз $Ag \in A$, що призводить до переходу системи в небезпечний стан $s^- \in S^-$, тобто

$$\tau = e \bullet Ag \Rightarrow s^-$$

Зауважимо, що певні вищевказані моделі є загальними для систем хмарних обчислень і традиційних інформаційних систем [9]. Однак слід зазначити, що характерні особливості систем хмарних обчислень зумовлюють розширення множин T і F порівняно з традиційними інформаційними системами. Такі зміни, своєю чергою, призводять до розширення множин A , O , V і M а, отже, розширення всієї моделі загроз інформаційній безпеці для систем хмарних обчислень.

Так, з погляду технічної реалізації для систем хмарних обчислень характерне використання засобів віртуалізації, що забезпечують можливість самообслуговування споживачів та динамічної масштабованості обчислювальних ресурсів. З використанням засобів віртуалізації з'являються додаткові особи і фактори, що впливають на системи хмарних обчислень і є джерелами загроз інформаційній безпеці, специфічними для технології хмарних обчислень. Так, збої в роботі засобів віртуалізації можуть призвести до порушення ізоляції і втрати оброблюваної інформації, а вразливість системи управління віртуальним середовищем створюють можливість для несанкціонованого доступу до обчислювальних ресурсів або даних з боку інших споживачів системи хмарних обчислень.

Універсальність доступу до інформаційних сервісів по каналах інформаційно-телекомунікаційних мереж розширює коло можливих сценаріїв реалізації загроз інформаційної безпеки з боку користувачів інформаційно-телекомунікаційних мереж. Водночас ця особливість систем хмарних обчислень дає змогу переносити процеси обробки інформації до захищених та відмовостійких центрів обробки даних хмарного засобу. Отже, ймовірність реалізації загроз інформаційної безпеки за допомогою фізичного доступу до компонентів системи хмарних обчислень скорочує втрати від реалізації загроз, пов'язаних зі стихійними лихами і природними явищами.

У зв'язку з використовуваною в системах хмарних обчислень моделлю надання інформаційних сервісів персонал хмарного провайдера володіє потенційно необмеженим доступом до інформації споживачів. На відміну від традиційних інформаційних систем, персонал хмарного провайдера не є представником споживача, а отже, знаходиться поза зоною його контролю. З урахуванням високої консолідації обчислювальних ресурсів у системах хмарних обчислень це значно розширює можливості реалізації загроз інформаційній безпеці з боку персоналу провайдера. Залежно від функціональних завдань персоналу загрози можуть бути реалізовані шляхом фізичного доступу до компонентів системи хмарних обчислень, а також з використанням системного та прикладного програмного забезпечення. Крім того, до можливих джерел загроз інформаційній безпеці в системах хмарних обчислень може входити оператор зв'язку [10], що надає послуги підключення між провайдером і споживачами та безпосередньо впливає на доступність інформаційних сервісів і захист переданих даних.

Висновки та перспективи подальших наукових розвідок

Використання хмарних сервісів для планування і управління туристичним бізнесом дає змогу зменшити фінансові витрати, пов'язані з розгортанням, супроводом і оновленням як програмного, так і апаратного забезпечення. Описано інфраструктуру хмарних технологій для розроблення платформи планування туристичного бізнесу та запропоновано її архітектуру, що основана на п'яти рівнях обслуговування туристичного бізнесу: системах управління базами даних, сховищі даних, сервері додатків, веб-сервері, клієнтському програмному забезпеченні. Крім того, визначено та описано бібліотеку програмних модулів для вирішення оптимізаційних завдань і показано планування й моделювання захисту даних платформи туристичного бізнесу.

1. Струбицький Р. П. Аналіз інфраструктури та моделей організації хмаркових сховищ даних / Р. П. Струбицький, Н. Б. Шаховська // Вісник Нац. ун-ту "Львівська політехніка". – 2014. – № 783. – С. 225–233. 2. Badger L., Grance T., Patt-Corner R., Voas J. *Cloud Computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-146.* – Режим доступу: <http://csrc.nist.gov/publications/nist-pubs/800-146/sp800-146.pdf>. 3. Частные облака // Открытые системы. – 2012. – № 4. – С. 1–64. *Private Clouds. Open Systems, 2012, no. 4, pp. 1–64.* 4. Артеменко О. І. Особливості побудови інформаційних технологій моделювання процесів розвитку туристичних та інфокомунікаційних комплексів / О. І. Артеменко, Б. М. Гаць, Н. М. Івануцак, Д. І. Угрин // Вісник Національного університету "Львівська політехніка". – 2014. – № 783: Інформаційні системи та мережі. – С. 406–411. 5. Воронин А. В., Шабаев А. И., Печников А. А. Конвейерная технология разработки программного обеспечения для управления производственными ресурсами и процессами. // Перспективы науки. – 2010. – Т. 4. – С. 95–99. 6. Таха Х. А. Введение в исследование операций / М.: Вильямс, 2005. – 912 с. 7. *Top Threats to Cloud Computing V1.0 / Cloud Security Alliance, March 2010.* [Електронний ресурс] – Режим доступу: <https://cloudsecurityalliance.org/topthreats/csath-reats.v1.0.pdf>. 8. *Cloud Computing. Benefits, risks and recommendations for information security / ENISA, November 2009.* [Електронний ресурс] – Режим доступу: <http://www.enisa.europa.eu/acti-ities/risk-management/files/deliverables/cloud-computing-risk-assessment>. 9. Peter R. Stephenson. *A Formal Model for Information Risk Analysis Using Colored Petri Nets. Colored Petri Nets (CPN), 2004* [Електронний ресурс] – Режим доступу: <http://daimi.au.dk/CPnets/proxy.php?url=/CPnets/workshop04/cpn/papers/index>. 10. Badger L. *DRAFT Cloud Computing Synopsis and Recommendations / L. Badger, T. Grance //NIST Special Publication* [Електронний ресурс] – Режим доступу: <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>.