

2. RTK Fundamentals [Електронний ресурс]. – Режим доступу: https://gssc.esa.int/navipedia/index.php/RTK_Fundamentals.

3. Precise Point Positioning [Електронний ресурс]. – Режим доступу: https://gssc.esa.int/navipedia/index.php/Precise_Point_Positioning.

4. AR в строительстве [Електронний ресурс]. – Режим доступу: <http://tofar.ru/ar-v-stroitelstve.php>.

Фесенко І.А.

студент,

Науковий керівник: Шевчук Є.В.

викладач,

Науковий керівник: Гутнік К.О.

викладач другої категорії,

Коледж інформаційних технологій та землевпорядкування

Національного авіаційного університету

ОСОБЛИВОСТІ ХМАРНОЇ ВЕБ-ПЛАТФОРМИ ДЛЯ КОРИСТУВАЧІВ

Суть концепції хмарних обчислень полягає в наданні кінцевим користувачам віддаленого динамічного доступу до послуг, таких як програмне забезпечення, платформа чи інфраструктура. Та якщо провайдери хмарних сервісів забезпечують захист ресурсів, які надають у користування, то про захист ресурсів, які користувач надає у загальний доступ, він повинен подбати сам. У наш час все більше набувають популярності хмарні технології. Хмарні технології – це парадигма, що передбачає віддалену обробку та зберігання даних [1]. Ця технологія дозволяє вести значно ефективніше управління підприємством (CRM, ERP) [2] за рахунок централізації управлінської та облікової інформації, обробки, пропускової здатності та надійності зберігання даних.

Є безліч переваг використання саме хмарних технологій, серед них: непотрібні потужні комп'ютери, менше витрат на закупівлю програмного забезпечення і його систематичне оновлення, необмежений обсяг збереження даних, доступність з різних пристроїв і відсутня прив'язка до робочого місця, забезпечення захисту даних від втрат та виконання багатьох видів навчальної діяльності, контролю і оцінювання, тестування он-лайн, відкритості освітнього середовища і т. д.

Дана платформа спрямована у двох напрямках: Приватна хмара та Публічна хмара.

Приватна хмара (private cloud) – це хмарна інфраструктура, яка призначена для використання виключно однією організацією, що включає декілька користувачів (наприклад, підрозділів). Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника. Даний тип розгортання є дуже зручним для

використання всередині організації, оскільки забезпечує більшу безпеку шляхом розміщення на власних серверах.

Публічна хмара (public cloud) – це хмарна інфраструктура, яка призначена для вільного використання широким загалом. Публічна хмара може перебувати у власності, керуванні та експлуатації комерційних, академічних (освітніх та наукових) або державних організацій (чи будь-якої їх комбінації). Публічна хмара перебуває в юрисдикції постачальника хмарних послуг.

Платформа орієнтована саме веб додаток, фізичний сервер (або сервери) схову та публічний програмний інтерфейс для взаємодії зі сховищем (API).

GigaCloud – відомий український хмарний оператор. Він пропонує IaaS (інфраструктуру як сервіс) на базі різних технологічних платформ для корпоративних клієнтів, малого і середнього бізнесу. Виконує будь-які проекти: від підбору недорогих хмарних серверів до розгортання власної інфраструктури, рішень із резервного копіювання даних. У GigaCloud ви отримуєте допомогу на кожному етапі: вибір потрібної послуги, міграція даних у хмару, тестування та оптимізація. Додатково надається розширена підтримка, галузеві хмарні рішення.

Міжсайтова підробка запиту (CSRF) досить типова вразливість, яку можна подолати за допомогою передачі спеціального підпису (токена) у додаток, та його перевірки. Дану перевірку слід виконувати на початку обробки запиту.

SQL ін'єкція – один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні запит довільного SQL-коду. Оскільки у даній платформі використовується база даних, слід обов'язково унеможливити здійснення ін'єкцій. Даний етап перевірки на ін'єкцію слід здійснювати при запиті до бази даних, використовуючи спеціальні технології як Entity Framework та LINQ, а також уникати передачі всіх параметрів у відкритому вигляді та без обробки [4].

Динамічний антивірусний захист є обов'язковим для машин на базі операційних систем сімейства Windows. Такий захист повинен передбачати агрегацію журналів подій. Основним засобом, який забезпечує живучість цієї інфраструктури, є реплікація основних елементів, за доступ до яких відповідають розподільники навантаження: зовнішній і внутрішній. Будь-які події, які відбуваються у цій мережі, реєструє централізований сервер реєстрації подій. Головний пріоритет у реєстрації подій: · пов'язаних з IDS; подій антивірусів; пов'язаних із системою-приманкою.

Проблема безпеки у публічних хмарних обчислювальних мережах є однією із найгостріших у сучасному світі інформаційних технологій, оскільки цей ресурс став доступний кожному за своїм кошторисом. Та провайдери хмарних сервісів забезпечують захист інформації лише на рівні надання своїх послуг.

Список використаних джерел:

1. AmazonWebService [Електронний ресурс]: портал Amazon. – Режим доступу: <http://aws.amazon.com/>. – Назва з титул. екрана.
2. Neha Patwari, Parvati Bhurani – Framework of SQL Injection Attack. [Електронний ресурс]. – Режим доступу: <http://arxiv.org/ftp/arxiv/papers/1207/1207.1542.pdf>.

3. Класифікація загроз безпеки WEB-додатків [Електронний ресурс] – Режим доступу: <http://www.infosecurity.ru/iproduct/websec/classification/>.
4. Хмарні технології. [Електронний ресурс]. – Режим доступу: <http://j.parus.ua/ua/358>.

Цейко Б.О.

аспірант,

Державний університет інфраструктури та технологій

РОЗРОБКА ФОРМИ ЗВОРОТНЬОГО ЗВ'ЯЗКУ ДЛЯ ПЕРЕВЕЗЕННЯ ВАНТАЖІВ ПРИ ОБСЛУГОВУВАННІ КЛІЄНТІВ НА ЗАЛІЗНИЦІ

На теперішній час для управління перевезеннями вантажів застосовуються підходи, в яких головним елементом перевізної ланки є вантаж. В практичній реалізації це зумовлює те що залізниця здійснивши перевезення вантажу, не отримує інформацію від своїх клієнтів – вантажовласників, вантажовідправників та вантажоодержувачів, стосовно якості умов оформлення вантажу та інших організаційних аспектів взаємодії їх із залізницею. Тому потреби створення форм зв'язку, які будуть клієнтоорієнтованими, а також не тільки вантажоцентричними, а і клієнтоцентричними є актуальними.

Проблематика застосування інформаційних технологій в управлінні процесами доставки вантажу, концепція інтелектуальної транспортної системи управління процесами доставки вантажу, а також аспекти функціонування та роботи Інтелектуальної системи управління процесом доставки вантажу приведені у працях, Г. І. Кириченко [1; 2; 3].

Методологічний аспект формування критеріїв ефективного управління залізничною транспортною системою розкриває колектив авторів у [4].

Питання інтелектуальних технологій управління висвітлюються у [5].

Становлення України як самостійної держави спричинило потребу приділяти увагу більш якісному транспортному обслуговуванню клієнтів, що повинно підняти рівень конкурентоспроможності транспортних послуг.

З цією метою пропонується створення форми зворотнього зв'язку для перевезення вантажів(ФЗЗПВ).

Така форма зв'язку буде як більш клієнтоорієнтована, так і поєднає в собі сучасні технології, які вже використовуються у інших сферах людської діяльності, що дозволить скоротити затрати часу до мінімальних та підвищити комфорт і якість транспортного обслуговування.

Передбачається, що сайт системи буде легким та зрозумілим для середньостатистичного інтернет-користувача.

Візуалізація розробки форми зворотнього зв'язку для перевезення вантажів (ФЗЗПВ) при обслуговуванні клієнтів на залізниці передбачається у вигляді сайту.