МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УМАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ САДІВНИЦТВА
Факультет економіки і підприємництва
Кафедра інформаційних технологій

Допущено до захисту
"_____" _____ 2024 р.
Зав. кафедри, к.т.н., доцент
_____ **Ліщук Р.І.**

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ПОСЛУГАМИ ІНТЕРНЕТ-ПРОВАЙДЕРА

Виконав – студент 2 курсу, групи 21м-кн
освітньої програми "Комп’ютерні науки"
спеціальності 122 Комп’ютерні науки
Євстаф`єв Сергій Миколайович

Науковий керівник – к.т.н., доцент
Ліщук Роман Ігорович

Умань – 2024

Зміст

ВСТУП 3

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПІДХОДІВ ДО СТВОРЕННЯ ІНФОРМАЦІЙНИХ УПРАВЛЯЮЧИХ СИСТЕМ З УПРАВЛІННЯ ПОСЛУГАМИ ІТ-ПРОВАЙДЕРА 5

1.1. Аналіз існуючих інформаційно управляючих систем з управління послугами ІТ-провайдера 5

1.2. Дослідження ринку інформаційних систем з управління послугами ІТ-провайдера 12

1.3. Обґрунтування вибору підходів, технологій для створення інформаційних управляючих систем. Постановка задачі 19

РОЗДІЛ 2 ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ПОСЛУГАМИ ІНТЕРНЕТ-ПРОВАЙДЕРА 24

2.1. Структура і характеристика системи 24

2.2. Методи та моделі інформаційної системи з управління послугами ІТ-провайдера 28

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ПОСЛУГАМИ ІНТЕРНЕТ-ПРОВАЙДЕРА 35

3.1. Проектування бази даних для інформаційної системи з управління послугами ІТ-провайдера 35

3.2. Визначення показників для оцінки продуктивності системи 41

3.3. Реалізація інформаційної системи управління послугами інтернет-провайдера. 49

ВИСНОВКИ 53

СПИСОК ЛІТЕРАТУРИ 54

ДОДАТКИ 58

ВСТУП

Актуальність проблеми. З ростом комп'ютеризації та залежності від технологій, провайдери IT-інфраструктури стають важливими постачальниками послуг для організацій різних масштабів.

Дана інформаційна система дозволяє провайдерам ефективно управляти своїми послугами, забезпечуючи швидку та надійну реакцію на запити клієнтів, моніторинг стану системи, аналіз використання ресурсів, планування та вдосконалення послуг. Вона допомагає автоматизувати процеси, спрощує комунікацію з клієнтами і покращує загальну якість обслуговування.

Оскільки IT-інфраструктура стає все більш складною і розширеною, а клієнти вимагають більш широкого спектру послуг, належне управління інформаційними системами стає критичним завданням для провайдерів. Тому, актуальність цієї теми полягає в необхідності розуміння та впровадження ефективних систем управління послугами, які допоможуть забезпечити якісне обслуговування клієнтів та оптимізувати внутрішні процеси провайдера IT-інфраструктури.

Об’єкт дослідження: інформаційна система з управління послугами провайдера IT-інфраструктур.

Предметом дослідження: Методології проектування інформаційної системи з управління послугами провайдера IT-інфраструктур.

Мета і завдання. Дослідити теоретичні і практичні підходи до проектування інформаційної системи з управління послугами провайдера IT-інфраструктур.

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПІДХОДІВ ДО СТВОРЕННЯ ІНФОРМАЦІЙНИХ УПРАВЛЯЮЧИХ СИСТЕМ З УПРАВЛІННЯ ПОСЛУГАМИ IT-ПРОВАЙДЕРА

1.1. Аналіз існуючих інформаційно управляючих систем з управління послугами IT-провайдера

IT-інфраструктура - це сукупність апаратних, програмних та мережевих ресурсів, які використовуються для підтримки інформаційних технологій у певній організації або середовищі.

IT-інфраструктура включає такі компоненти:

Апаратне забезпечення - фізичні пристрої, такі як комп'ютери, сервери, мережеві комутатори, маршрутизатори, сховища даних (наприклад, сервери зберігання), принтери та інші пристрої, необхідні для функціонування системи.

Програмне забезпечення - програми та операційні системи, які працюють на апаратному забезпеченні. Вони можуть включати операційні системи (наприклад, Windows, Linux), бази даних, програми для роботи з документами, електронну пошту, програмне забезпечення безпеки та інші додатки.

Мережева інфраструктура - система комунікаційних засобів, що забезпечують зв'язок між різними пристроями в інфраструктурі. Вона може включати мережеві комутатори, маршрутизатори, мережеві кабелі, бездротові точки доступу та інші пристрої.

Засоби зберігання даних - сховища, які використовуються для збереження і обробки даних. Вони можуть включати сервери зберігання (storage servers), рейд-масиви, хмарні сховища, системи резервного копіювання та інші рішення зберігання даних.

Засоби безпеки - файрволи, антивірусне програмне забезпечення, системи виявлення та запобігання вторгненням, системи шифрування, політики безпеки та контроль доступу, а також резервне копіювання та відновлення даних.

Всі ці компоненти IT-інфраструктури співпрацюють, щоб забезпечити ефективну роботу інформаційних технологій в організації. Наприклад, сервери зберігання даних можуть бути підключені до мережевої інфраструктури, щоб

забезпечити швидкий доступ до даних для користувачів. Апаратне забезпечення та програмне забезпечення працюють разом, щоб запускати та виконувати різноманітні програми та послуги.

Важливо мати добре організовану та підтримувану IT-інфраструктуру для забезпечення безперебійної роботи систем, ефективного використання ресурсів, захисту від загроз та забезпечення задоволення потреб користувачів.

Побудова власної IT-інфраструктури за рахунок внутрішніх ресурсів компанії може бути складним та дорогим процесом. Для досягнення цієї мети, бізнесу потрібно наймати кваліфікованих фахівців з відповідним досвідом, виділяти значні бюджетні кошти і бути готовим до тривалого часового затягнення процесу.

Однак існує альтернатива - використання послуг провайдера IT-інфраструктури для побудови надійної системи з мінімальними витратами.

Провайдери IT-інфраструктури займаються наданням різноманітних послуг, пов'язаних з управлінням та підтримкою IT-інфраструктури для організацій. Основні функції та послуги, які надають провайдери IT-інфраструктури, включають:

Хмарні обчислення: надання доступу до віртуальних серверів, обчислювальних ресурсів та зберігання даних в хмарному середовищі. Це дозволяє організаціям зосередитися на своїх основних діяльностях, не звертаючи велику увагу на власну фізичну IT-інфраструктуру.

Колокація: надання фізичного простору, енергетичних ресурсів та мережевого з'єднання для розміщення серверів та інфраструктури організацій. Це дозволяє компаніям зберігати своє обладнання в надійному середовищі з професійними умовами забезпечення безперебійної роботи.

Мережеві послуги: надання мережевих рішень, таких як мережевий доступ, маршрутизація, комутація, встановлення вогневих стін та захист мережі. Це дозволяє підприємствам мати надійне та безпечне з'єднання з Інтернетом та іншими мережами.

Управління системами: надання послуги з управління та моніторингу систем, включаючи сервери, мережі, бази даних, програмне забезпечення. Це включає моніторинг ресурсів, виявлення проблем, резервне копіювання та відновлення даних, планування місткості та інші аспекти управління системами.

Консультаційні послуги: надання експертних порад та консультацій з проектування, розгортання та оптимізації IT-інфраструктури. Провайдери IT-інфраструктури можуть допомогти підприємствам визначити потреби в інфраструктурних ресурсах, розробити план розгортання, вибрати відповідне обладнання та програмне забезпечення, а також забезпечити належну інтеграцію і налаштування систем.

Безпека та захист: надання послуг забезпечення безпеки IT-інфраструктури, включаючи виявлення та запобігання вторгненням, моніторинг захисту, шифрування даних, управління ідентифікацією та доступом, а також резервне копіювання та відновлення даних. Це дозволяє забезпечити високий рівень безпеки та захищеності інформації організації.

Підтримка та обслуговування: надання послуг технічної підтримки, усунення несправностей, моніторингу та оптимізації роботи IT-інфраструктури. Провайдери IT-інфраструктури можуть відповідати за регулярні оновлення, управління патчами та вирішення проблем, що виникають, забезпечуючи безперебійну роботу систем.

Провайдери IT-інфраструктури виконують ці послуги з метою спрощення та оптимізації процесу управління IT-інфраструктурою для компаній. Вони забезпечують фахівців, ресурси та експертні знання, що дозволяють підприємствам ефективно використовувати свою IT-інфраструктуру та зосередитися на своїх основних бізнес-цілях.

Надання послуг клієнтам – це складний процес, який вимагає від фахівців знань щодо технічного та програмного забезпечення.

Розглянемо на прикладі надання послуг з VPS.

Віртуальний приватний сервер (VPS) – це машина, на якій знаходиться все програмне забезпечення та всі дані, необхідні для роботи веб-сайту програми. Його називають віртуальним, оскільки він використовує тільки частину фізичних ресурсів сервера, яким керує сторонній абонент, однак користувач отримує доступ до виділених ресурсів на цьому обладнанні.

Технологія, за якою реалізується досліджувана послуга VPS, виглядає так: фізичний сервер розділений на кілька віртуальних, і серверне програмне забезпечення (ПЗ) налаштовується на них окремо, змушуючи кожен віртуальний сервер працювати незалежно. Це означає, що потужність кожного сервера визначається набором технічних характеристик, зокрема оперативною пам’яттю, дискового простору, процесора тощо і ніяк не впливають на продуктивність один одного.

Проаналізуємо основну різницю VPS та VDS серверів при їх виборі державними установами. VPS – це віртуальний приватний сервер, а VDS – це віртуальний виділений сервер. Обидва терміни мають на увазі віртуальну машину, яка працює на базі фізичного сервера, встановленого в обслуговуючому дата-центрі. Фактично на одному фізичному сервері працює відразу кілька віртуальних серверів, кожен з яких має власний набір технічних параметрів відповідно до вимог замовника. За запитом можна орендувати сервер з необхідною кількістю і частотою ядер процесора, об’ємом оперативної пам’яті і дискового простору. Так само як і з фізичним обладнанням, пам’ять і продуктивність можна докупити, оновивши тарифний план у провайдера.

Слова "приватний" і "виділений" мають на увазі неподільне володіння і повне розпоряджання потужностями і програмним забезпеченням віртуального сервера. Купуючи VPS або VDS, користувач отримує гарантований набір технічних характеристик, який буде доступний виключно тільки йому.

Безпека та захист інформації є однією з головних причин оренди VPS для конфіденційних корпоративних проєктів. На відміну від фізичних, віртуальні сервери складніше зламати: розміщення хост-машин в дата-центрах забезпечує захист від збоїв в мережі і рейдерських захоплень, а багатий інструментарій

системного ПЗ дозволяє захистити VPS від DDoS-атак. Оренда VPS актуальна для маленьких компаній, які не планують купувати фізичні сервери для зберігання даних, і не мають можливості їх регулярно обслуговувати.

Серед складнощів з вибору VPS можна назвати те, що їх управління вимагає певних технічних навичок (VPS представлені групою OVS (Optimized Virtual Servers) на основі віртуалізації KVM). Крім того, вартість VPS вище, ніж у віртуального хостингу. Неправильні налаштування можуть призвести до вразливостей безпеки для зберігання конфіденційної інформації державної організації.

При виборі VPS потрібно відразу визначитись з обсягом даних, які будуть зберігатися на жорсткому диску та її пропускною здатністю, оскільки доступ до даних повинен здійснюватися на високій і стабільній швидкості. Вибирати VPN-сервіс потрібно з виділеними IP-адресами, так як не у всіх провайдерів вони є. Оскільки замовник буде власником віртуального сервера, то доступ до нього буде тільки у даної організації. Але організація може передати права на зміни даних, і тоді VPS-сервер передається з доступом до root-прав і тоді можливою стає регулювання відвідувачів.

Важливим є також аналіз характеристик "фізичного" сервера, і якщо провайдер є надійним, то він не буде приховувати ці дані. Бажано, щоб обладнання було відомого бренду, яке зарекомендувало себе з позитивного боку. Найпопулярнішими ОС є Windows і Linux. Linux, представлений у безлічі варіантів, коштує дешевше, але деякі програми він не підтримує (включаючи ASP. NET), тому для розробників, наприклад, не підходить. При виборі Windows необхідно уточнювати, чи включена вартість ліцензії в тариф. Якщо не включена – за неї доведеться державній установі доплачувати окремо.

Для будь-якого підприєства використання VPS для роботи є вигідним навіть з тієї сторони, що не потрібно оплачувати послуги власного комп’ютерного адміністратора, адже підтримку працездатності сервера, його налаштування, захист даних і додаткові роботи виконують представники, у яких отримується послуга VPS. Крім того, програмне забезпечення в режимі

реального часу контролює фактичне навантаження VPS і при необхідності автоматично збільшує потужність віртуального сервера.

В той же час, час замовник отримує в розпорядження ізольований від інших користувачів сервер, який можна індивідуально налаштовувати, встановлювати додаткове ПЗ. Можливою також є побудова гібридних систем з приватної хмари і локальної інфраструктури, розподіленої між дата-центрами або дата-центром і головним офісом державної установи. Такі системи підвищують відмовостійкість і допомагають впроваджувати disaster recovery plan.

Крім того, важливо забезпечити максимальний рівень безпеки та захисту даних. Для цього потрібно використовувати надійні алгоритми шифрування та механізми автентифікації, щоб забезпечити доступ тільки авторизованим користувачам. Також слід забезпечити резервне копіювання та відновлення даних, щоб забезпечити безперебійну роботу системи в разі виникнення проблем.

Отже, налаштування IT інфраструктури для підприємства може бути складним процесом, залежно від багатьох факторів, включаючи обсяг даних, що будуть зберігатися, рівень безпеки, надійність та швидкість. Також необхідно враховувати фактори, пов’язані з відповідністю правовим та регуляторним вимогам щодо збереження конфіденційної інформації та дотримання стандартів безпеки даних.

При наданні послуг важливим є укладання угоди про рівень надання послуг (SLA – Service level agreement).

Угода про рівень надання послуг (SLA) зазвичай є однією з двох основних угод, які постачальник послуг укладає з клієнтами. Багато постачальників включають основну угоду про рівень надання послуг для встановлення загальних умов співробітництва з клієнтами. SLA, в свою чергу, часто включається в договори через посилання на нього в основному договорі з постачальником послуг. У порівнянні з іншою угодою про надання послуг, SLA

надає більш детальну і специфічну інформацію про надані послуги та показники, що будуть використовуватись для оцінки їх ефективності.

У широкому розумінні, SLA зазвичай включає формулювання цілей, перелік послуг, які підпадають під угоду, а також визначає обов'язки постачальника послуг та замовника відповідно до угоди. Наприклад, замовник має забезпечити представника для вирішення питань з постачальником послуг, пов'язаних з угодою про рівень надання послуг. З свого боку, постачальник послуг несе відповідальність за дотримання рівня обслуговування, визначеного угодою.

Угода про рівень надання послуг також включає розділ, в якому детально описуються виключення - ситуації, коли гарантії угоди та санкції за їх невиконання не застосовуються. Цей розділ враховує такі непередбачувані події, як стихійні лиха або терористичні акти. Іноді його називають розділом про форс-мажорні обставини, який має на меті звільнити постачальника послуг від відповідальності за збитки, що виникають внаслідок подій, що перебувають поза його контролем.

Угоди про рівень надання послуг охоплюють широкий спектр понять та задовольняють потреби клієнтів постачальника послуг. SLA можуть змінюватися з часом, оскільки постачальники послуг періодично переглядають та оновлюють їх, щоб відповідати новим послугам, змінам у наявних послугах або змінам у нормативному середовищі. Угоди про рівень надання послуг важливі для постачальників, оскільки вони дозволяють керувати очікуваннями клієнтів та визначати відповідальність у випадку перебоїв або проблем.

Клієнти також виграють від угод про рівень надання послуг, оскільки вони описують експлуатаційні характеристики послуги, які можна порівняти з угодами інших постачальників та забезпечують механізми вирішення питань щодо обслуговування.

1.2. Дослідження ринку інформаційних систем з управління послугами IT-провайдера

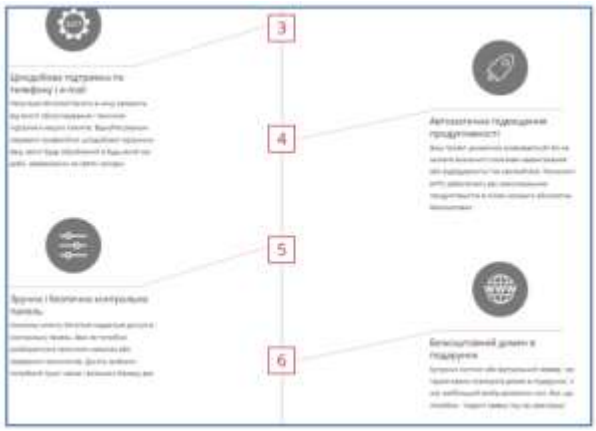
Дослідження показали, що на IT-ринку небагато підприємств, які надають послуги IT-провайдера. Втім, даний ринок динамічно розвивається.

Розглянемо найбільш популярні компанії з надання послуг щодо IT-інфраструктури.

Проаналізуємо три найбільш відомих провайдери, що надають послуги VPS в Україні.

Компанія Mirohost (URL: https://mirohost.net/ua) – спеціалізується переважно на надінні хостінг-послуг, вважається лідером в Україні в цьому напрямку.





Mirohost [1]. Провайдер здійснює базове адміністрування VPS, надає широкий вибір ОС (Windows Server, Linux CentOS, Debian, Ubuntu, BitrixVM) і панелей управління (VestaCP, ISPmanager Lite, ISPmanager Business, Bitrix 7).

Існує можливість змінювати конфігурацію сервера-підвищувати швидкість доступу, збільшувати кількість процесорів, обсяг жорстких дисків і оперативної пам’яті.

Перевагами компанії є: безлімітний трафік; великий вибір ОС; зручні панелі управління; безкоштовний SSL; гнучка конфігурація.

Недоліками компанії є: відсутність тестового періоду; захист від DDoS-атак – за додаткову плату; часте потрапляння IP адрес в спам-листи; наявність обмежень на типи проектів.

Підтримка користувача здійснюється, переважно, через телефон та email.

Наступний IT-провайдер - Gigacloud [2]. Надає послуги IT- хмарних інфраструктур.





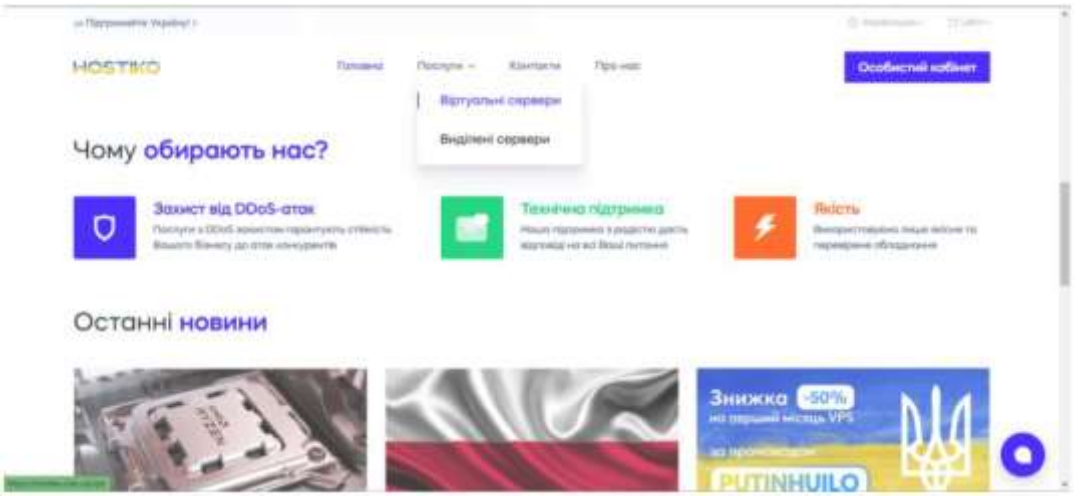
Gigacloud [2]. В даної компанії використовуються потужні фізичні сервери і канали зв’язку з пропускною здатністю 100 Мбіт/сек. На вибір представлений ряд операційних систем сімейства Linux (Fedora, Debian, OpenSuse, CentOS, Ubuntu і BitrixVM). Управління здійснюється через панель власної розробки, яка вбудована в особистому кабінеті. Конфігуратора тарифів немає: клієнт отримує, згідно з обраним тарифом, певну кількість процесорних ядер, деякий обсяг ОП і місце на диску, потім вибирає ОС і додаткове ПЗ.

Перевагами компанії є: безлімітний трафік; оперативна цілодобова технічна підтримка; базовий захист від DDoS-атак; безкоштовний SSL; одна IP-адреса-безкоштовно.

Недоліками компанії є: немає безкоштовного тестового періоду; висока вартість; відсутність конфігуратора сервера.

Hostiko [3] – компанія переважно молода на ринку IT-провайдерів.

Використовуються преміальне обладнання бренду Dell і високошвидкісні канали зв’язку. На всіх тарифах, крім базового, можна вибирати обсяг дискового простору з двох запропонованих значень. Провайдер здійснює базове адміністрування VPS сервера і підтримку в екстрених ситуаціях. При необхідності клієнт може скористатися розширеним адмініструванням за окрему плату. Працює цілодобова техпідтримка для вирішення будь-яких питань. Доступні кілька версій ОС на базі Linux-CentOS, Debian і Ubuntu, зі стандартною установкою або з додаванням панелі управління.



Перевагами компанії є: безлімітний трафік; оперативна цілодобова технічна підтримка; один IP – адреса-безкоштовно, доступне замовлення додаткових IP-

адрес; антивірусний захист; базовий захист від DDoS-атак; можливим є великий вибір конфігурацій.

Недоліками компанії є: відсутність безкоштовного тестового періоду; немає безкоштовного сертифіката SSL; обмежена конфігурація тарифів.

Для підтримки користувачівє форма зворотнього зв’язку та персональний кібінет.

Здійснимо також аналіз програмних продуктів для управління якістю надання послуг IT-інфраструктурами – Splunk , SignalFx та DataDog.

Програмне забезпечення Splunk вважається лідером в галузі спостереження за реальним рівнем надання послуг підприємствами. Воно було піонером у використанні метрик і логів для моніторингу стану системи в реальному часі, сповіщення про несправності та їх усунення. Метрики і логи є двома з трьох основних компонентів будь-якої системи спостереження за станом системи.

Останнім часом розробники Splunk розширили можливості спостереження шляхом інтеграції з FireLens, новою службою агрегації логів від AWS. Це дозволяє користувачам Splunk отримувати доступ до більш широкого спектру логів і розширює їх здатність аналізувати дані.

Splunk також надає користувачам інтерфейс для обробки даних, збереження даних в базі даних та механізм агрегації логів. Користувачі можуть виконувати пошук за допомогою простих пошукових термінів, але в програмному забезпеченні Splunk є потужна пошукова технологія обробки (SPL), яка дозволяє виконувати складніші фільтрації і статистичні операції над великими обсягами даних. SPL дозволяє знаходити конкретну інформацію в контексті і аналізувати її, наприклад, виявляти найповільніші програми, які спричиняють затримки для користувачів.

Таким чином, програмне забезпечення Splunk є потужним інструментом для спостереження за станом системи, аналізу даних та виявлення проблем у реальному часі.



Рисунок Візуалізація результатів моніторингу в програмі Splunk

SignalFx є програмним забезпеченням, яке розширює можливості Splunk у контексті моніторингу та управління рівнем надання послуг IT-інфраструктурою. В основі SignalFx є сервіс навігатора SignalFx для Kubernetes, який надає моніторинг та аналіз інфраструктури, особливо для середовищ, що містять контейнери, такі як Kubernetes.

SignalFx доповнює Splunk, яке в основному спеціалізується на збиранні, зберіганні та аналізі логів, але не надає спеціальних можливостей для управління рівнем надання послуг IT-інфраструктурою. Сервіс SignalFx надає засоби для збору метрик та логів, їх подальшого аналізу та моніторингу інфраструктури.

SignalFx Kubernetes Navigator є частиною SignalFx і є ідеальною платформою для моніторингу, аналізу та фільтрації середовищ, що використовують контейнери, зокрема Kubernetes. Він розроблений спільно з експертами з Kubernetes і надає готове рішення для спостереження за середовищем Kubernetes без необхідності складних налаштувань. Засоби візуалізації та аналітики, доступні в Kubernetes Navigator, дозволяють оперативно реагувати на складні ситуації та приймати відповідні рішення.

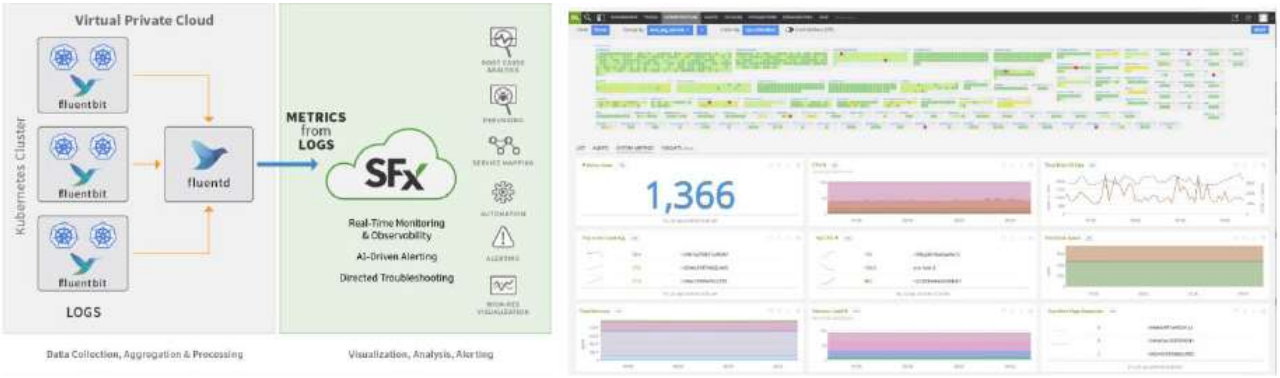


Рисунок Структура та інтерфейс системи системи SignalFx

Панелі навігації Kubernetes Navigator в SignalFx надають операторам інформацію про об'єкти та характеристики Kubernetes, що дозволяє їм переходити між різними рівнями абстракції і підтримувати ієрархічний контекст зразу після встановлення додатку. Це дозволяє ефективно вивчати та досліджувати можливі проблеми.

Щоб зробити тестування та вирішення проблем ще швидшими та активнішими, SignalFx Kubernetes Navigator використовує алгоритми штучного інтелекту, які автоматично аналізують проблему та надають рекомендації для подальшого вирішення.

Навігатор SignalFx Kubernetes надає операційним та інженерним командам розуміння, яке необхідне для моніторингу та управління здоров'ям контейнерних середовищ у режимі реального часу. Інженери зазвичай використовують SignalFx для спостереження за сервісами, які компанії переносять на Kubernetes. Це дає операційній команді змогу швидко діагностувати будь-які проблеми з IT-інфраструктурою або самою платформою оркестрації.

Таким чином, SignalFx Kubernetes Navigator забезпечує зручні інструменти для моніторингу, аналізу та управління контейнерними середовищами на основі Kubernetes, що дозволяє оперативно виявляти та вирішувати проблеми з інфраструктурою та сервісами.

Datadog – це інструмент моніторингу та аналітики для команд інформаційних технологій (IT) і DevOps, який можна використовувати для визначення показників продуктивності, а також моніторингу подій для інфраструктури та хмарних служб. Програмне забезпечення може контролювати такі служби, як сервери, бази даних і інструменти.

Програмне забезпечення для моніторингу Datadog доступне для розгортання на місці або як програмне забезпечення як послуга (SaaS).Datadog підтримує операційні системи Windows, Linux і Mac. Підтримка постачальників хмарних послуг включає AWS, Microsoft Azure, Red Hat OpenShift і Google Cloud Platform .

Datadog використовує агент на основі Go, а його серверна частина складається з Apache Cassandra, PostgreSQL і Kafka. Інтерфейс прикладної програми (API) Rest використовується для інтеграції Datadog з численними службами, інструментами та мовами програмування. Такі інтеграції, як Kubernetes, Chef, Puppet, Ansible, Ubuntu і Bitbucket.

Інтерфейс користувача містить настроювані інформаційні панелі, які можуть відображати графіки, що складаються з кількох джерел даних у режимі реального часу. Datadog також може надсилати користувачам сповіщення про проблеми з продуктивністю за будь-яким встановленим показником, наприклад швидкістю обчислення.Користувачі отримують сповіщення за допомогою таких засобів, як електронна пошта, Slack або PagerDuty.

Функції, які пропонує Datadog, включають:

- Надає групі IT/DevOps єдине уявлення про свою інфраструктуру (включаючи сервери, програми, показники та інші служби).
- Настроювані інформаційні панелі.
- Сповіщення про критичні проблеми.

- Підтримка понад 250 інтеграцій продуктів.
- Автоматично збирає та аналізує журнали, затримку та рівень помилок.
- Дозволяє отримати доступ до API.
- Підтримує програми, написані такими мовами, як Java, Python, PHP, .NET, Go, Node і Ruby.



Інформаційна панель Datadog

Альтернативні інструменти моніторингу Datadog включають такі рішення, як Science Logic і Zenoss Service Dynamics.

Science Logic – це інструмент моніторингу IT-інфраструктури, який забезпечує орієнтовану на хмару систему моніторингу, яка може контролювати бази даних і продуктивність програм. Science Logic також може контролювати приватні, загальнодоступні та багатохмарні хмари, мережі, сховище, апаратне забезпечення та гіпервізори.

Zenoss Service Dynamics IT-аналітичне програмне забезпечення моніторингу, яке може контролювати мережі, сховища, сервери, хмару, бази даних або гіпервізори. Service Dynamics доступний лише локально; версія SaaS пропонується через Zenoss як послуга (ZaaS). ZaaS пропонує ті самі можливості моніторингу, що й Service Dynamics.

1.3. Обґрунтування вибору підходів, технологій для створення інформаційних управляючих систем. Постановка задачі

Задачі управління послугами відносять класу слабоструктурованих задач, вони є досить складними і вимагають спеціальної підтримки. Тому застосування спеціальних програмних засобів при здійсненні управління є необхідною складовою цього процесу.

Основною метою створення ІС є підвищення якості рішень щодо управління послугами, моніторинг їх якості, пошук прихованих знань щодо проблеми.

Узагальнюючи досвід щодо створення подібних систем, пропонується виокремити наступні етапи проектування ІС.

1. Дослідження проблемної області та формування вимог до системи.

2. Вибір технології проектування системи.

3. Визначення функціональних можливостей ІС.

4. Проектування компонентів ІС.

Розглянемо детально ці етапи.

Дослідження проблемної області та формування вимог до системи.

На даному етапі описується перелік труднощів і "вузьких місць", специфічних для роботи даної системи. До основних труднощів можна віднести:

1) неможливість прогнозувати процес;

3) труднощі з обробкою даних, необхідних для ПР;

4) проблеми з аналізом і формуванням логічного висновку;

5) труднощі з візуалізацією результатів;

6) неточність процесу еврістичних суджень.

Вибір технології проектування системи.

Вибір технології проектування залежить від виду самої ІС.

Технологія проектування інформаційної системи– це комплекс методологічних підходів і засобів проектування, а також засобів організації

проектування (управління процесом створення і модернізації проекту інформаційної системи).

В основі технології проектування лежить технологічний процес, який визначає дії, їх послідовність, склад виконавців, засоби і ресурси, необхідні для виконання цих дій. Технологічний процес проектування будь якої інформаційної системи в цілому ділиться на сукупність послідовно-паралельних, зв'язаних і супідрядних ланцюжків дій, кожна з яких може мати свій предмет. Дії, які виконуються при проектуванні системи, можуть бути визначені як неподільні технологічні операції або як підпроцеси технологічних операцій. Вибираючи конкретну технологію створення ІС, необхідно керуватися наступними вимогами:

– створений за допомогою цієї технології проект повинен відповідати вимогам замовника;

– вибрана технологія повинна максимально відображати весь цикл життя проекту;

– вибрана технологія повинна забезпечувати мінімальні трудові і вартісні витрати на проектування і супровід проекту;

– технологія повинна бути основою зв'язку між проектуванням і супроводом проекту;

– технологія повинна сприяти зростанню продуктивності праці проектувальника;

– технологія повинна забезпечувати надійність процесу проектування і експлуатації проекту;

– технологія повинна сприяти простому веденню проектної документації.

Прийнято виділяти два основні класи технологій створення ІС: канонічна і індустріальна технології. Індустріальна технологія проектування, у свою чергу, розбивається на два підкласи: автоматизоване (з використанням CASE-технологій) і типове (параметрично-орієнтоване або модельно-орієнтоване) проектування. Використання індустріальних технологій проектування не виключає використання канонічної технології.

При канонічному проектуванні ІС відображаються особливості ручної технології індивідуального проектування, яке здійснюється на рівні виконавців без використання яких-небудь інструментальних засобів, що дозволяють інтегрувати виконання елементарних операцій. Як правило, канонічне проектування застосовується для невеликих локальних систем.

В основі канонічного проектування лежить каскадна модель життєвого циклу ІС.

Канонічний підхід до проектування ІС має також назву ресурсно-функціонального підходу – в його основу покладено ресурсно-функціональну декомпозицію діяльності економічного об’єкта, для якого створюється система.

При застосуванні індустріального автоматизованого підходу до проектування ІС прийнято розрізняти наступні підходи індустріального автоматизованого проектування ІС: структурно-орієнтований, об’єктно-орієнтований, процесно-орієнтований та агентно-орієнтований.

Структурно-орієнтований підхід базується на структурно-орієнтованій декомпозиції економічного об’єкта, для якого розробляється ІС. Така декомпозиція здійснюється шляхом структурного аналізу - методу дослідження системи, який починається з її загального огляду, потім деталізується, набуваючи ієрархічної структури з усе більшою кількістю рівнів.

Для цілей структурного аналізу традиційно використовуються три групи засобів, що ілюструють:

– функції, які система повинна виконувати;

– відношення між даними;

– поведінку системи залежно від часу (аспекти реального часу).

Серед різноманітних графічних нотацій, що використовуються для розв’язання перелічених задач, у методологіях структурного аналізу найчастіше і ефективно застосовуються такі:

– DFD (Data Flow Diagrams) – діаграми потоків даних (ДПД) спільно зі словниками даних і специфікаціями процесів (міні-специфікаціями);

– ERD (Entity–Relationship Diagrams) – діаграми "суть–зв’язок";

– STD (State Transition Diagrams) – діаграми переходів станів.

Суть об’єктно-орієнтованої методології зводиться до об’єктної декомпозиції предметної області, що подається у вигляді сукупності об’єктів, які взаємодіють між собою за допомогою передачі повідомлень. Даний підхід не є протиставленням структурному підходу, більше того, фрагменти методологій структурного аналізу (а саме його базові моделі: DFD, ERD і STD) використовуються під час об’єктно-орієнтованого аналізу для моделювання структури і поведінки самих об’єктів.

Процесно-орієнтований підхід базується на новому напрямку в теорії менеджменту економічними об’єктами – реінжинірингу бізнес-процесів. Бізнес-процеси – це ділові, адміністративні, технологічні процедури функціонування підприємства, до яких належать: документообіг, управління фінансовими, матеріальними потоками, персоналом, організаційно-господарськими і технологічними процесами, процесами проектування виробів і т. ін. Кардинальне якісне переосмислення та кількісне перепроектування всіх бізнес-процесів в рамках конкретного економічного об’єкту і є реінжинірингом бізнес-процесів. По суті реінжиніринг передбачає аналіз та оптимізацію бізнесів-процесів заради досягнення економічним об’єктом стратегічних цілей. Його методологічною основою є системний і структурний аналіз, теорія управління великими системами, а також методи керування якістю, промислова інженерія тощо [32].

Суть агентно-орієнтованого підходу до створення ІС полягає в тому, що така інформаційна система проектуються та реалізуються як сукупність програмних агентів (software agent) або як мультиагентна система.

В основі типової технології або RAD-технології (rapid application development - технології швидкої розробки додатків) проектування лежить спіральна модель життєвого циклу ІС. Згідно цієї технології ІС розробляється шляхом розширення програмних прототипів, повторюючи шлях від деталізації вимог до деталізації програмного коду.

Визначення функціональних можливостей ІС.

На цьому етапі пропонується порядок роботи користувача з системою, описується розподіл дій між персоналом і технічними засобами при різних ситуаціях розв'язання задачі. Також на цьому етапі наводиться опис основних функцій ІС.

Проектування компонентів ІС.

Відповідно обраних методів проектування на даному етапі проектуються база даних, база моделей та інтерфейс користувача. Зазначимо, що при проектуванні користувацького інтерфейсу важливо обґрунтувати механізм організації взаємодії користувачів із системою (формальний діалог, природна мова чи графічний діалог) та описати основні вимоги до користувацького інтерфейсу системи виходячи із трьох аспектів: мови дій, мови відображення й інформації, яку повинен знати користувач, щоб вести діалог з системою).

На основі проведеного аналізу предметної області та викоритсання сучасних технологій і інформаційних систем приходимо до висновку, що розробка системи буде проводитись на основі згального досвіду та досвіду фірми.

РОЗДІЛ 2 ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ПОСЛУГАМИ ІНТЕРНЕТ-ПРОВАЙДЕРА

2.1. Структура і характеристика системи

Інформаційна система управління послугами клієнтів провайдера IT-інфраструктур вирішує різноманітні задачі, пов'язані з наданням та керуванням IT-послугами клієнтам. Основні задачі, які вона вирішує, включають:

1. Запити на послуги: ІСУП приймає та реєструє запити на різні IT-послуги від клієнтів. Це може включати запити на розгортання нових систем, зміни конфігурації, відновлення послуг після виникнення проблем та багато іншого.

2. Управління життєвим циклом послуги: ІСУП допомагає управляти життєвим циклом IT-послуг від початкового планування до впровадження та наступного управління. Вона допомагає відстежувати етапи розробки, тестування, впровадження та експлуатації послуги.

3. Керування запитами та зверненнями: ІСУП дозволяє клієнтам подавати запити та звернення щодо питань, проблем, скарг або замовлень. Вона автоматизує процеси прийому, реєстрації, маршрутизації та відстеження цих запитів для забезпечення швидкого та ефективного вирішення.

4. Управління рівнем сервісу: ІСУП допомагає провайдеру IT-послуг забезпечувати встановлені рівні сервісу (SLA) для своїх клієнтів. Вона дозволяє відстежувати та керувати часом відповіді, часом відновлення послуги, пріоритетами та іншими параметрами, щоб гарантувати, що встановлені рівні сервісу виконуються.

5. Моніторинг та звітність: ІСУП забезпечує моніторинг IT-послуг і IT-інфраструктури для виявлення проблем, відстеження продуктивності та надання звітності клієнтам і провайдеру. Вона може збирати дані про доступність, використання ресурсів, показники продуктивності та інші метрики для аналізу та вдосконалення процесів.

6. Управління знаннями: ІСУП може служити як центральний репозиторій знань, де зберігаються і діляться документація, інструкції, шаблони, бази знань

та інші ресурси, необхідні для надання IT-послуг. Вона допомагає забезпечити доступ клієнтам до необхідної інформації та сприяє ефективному обміну знаннями всередині організації.

7. Автоматизація процесів: ІСУП дозволяє автоматизувати багато повторюваних процесів, таких як створення та відстеження замовлень, управління запитами, надання звітності тощо. Це допомагає підвищити ефективність та швидкість обробки запитів клієнтів.

8. Управління контрактами та фінансами: ІСУП допомагає вести облік контрактів з клієнтами, включаючи управління термінами, умовами, вартістю та платежами. Вона також може надавати інформацію про використання ресурсів та витрати на надання послуг клієнтам.

Основні можливості роботи з системою показані на рис. 2.1

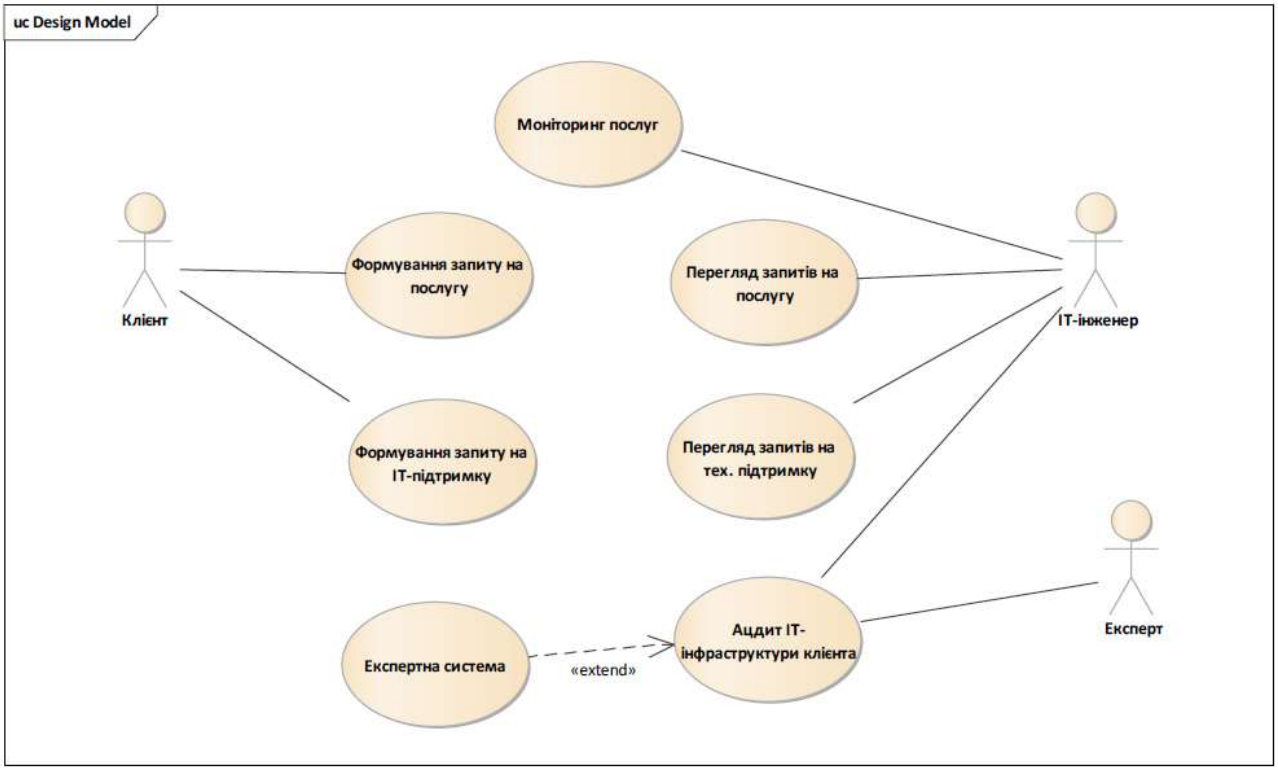


Рис. 2.1 – Діаграма варіантів використання інформаційної системи управління послугами IT-провайдера

Клієнт може звернутися на веб-сайт IT-провайдера і залишити заявку на послугу архітектурного рішення. На сайті пропонується конфігуратор для вибору типу сервера (рис. 2.2).

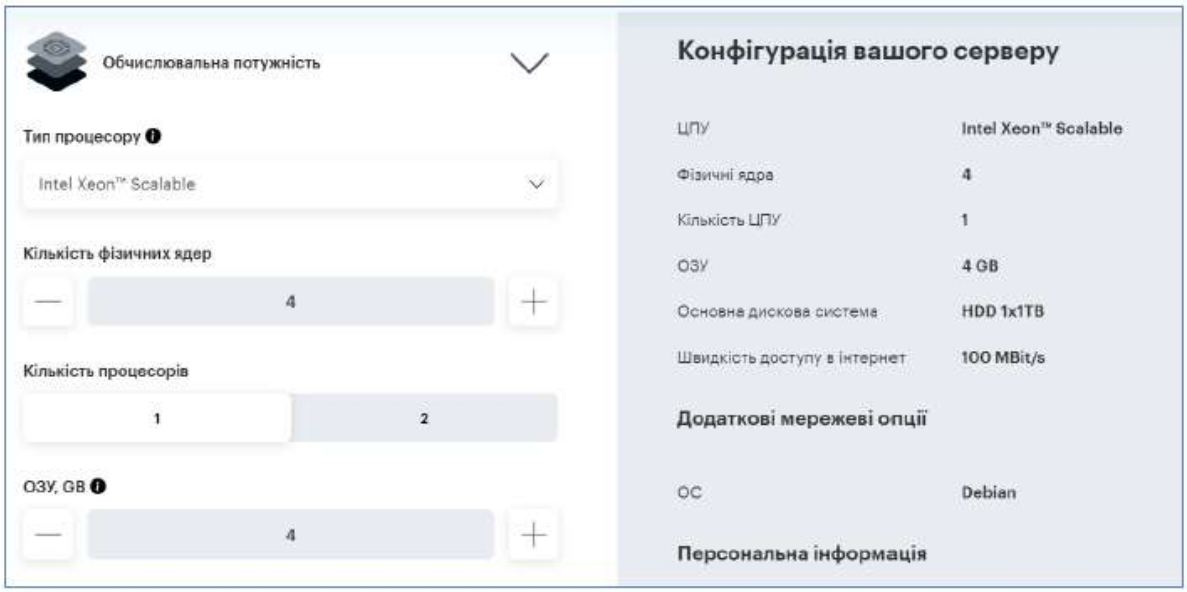


Рис.2.2 – Конфігуратор сервера

На рисунку 2.3 показано процес виконання замовлень у разі, якщо клієнт обрав стандартний чи не стандартний сервер.

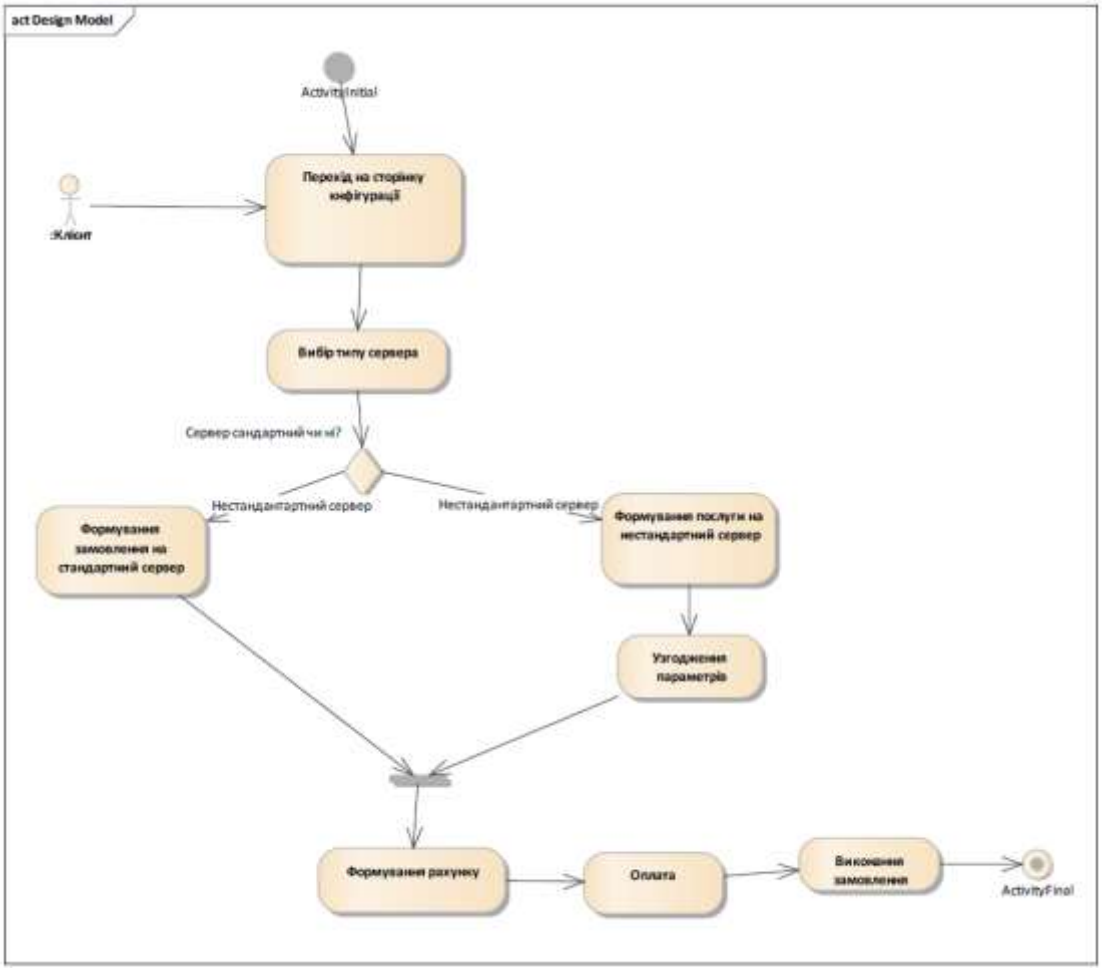


Рис. 2.3 Алгоритм роботи формування замовлення клієнтом

На рисунку 2.4 – робота з клієнтом в разі його вибору на нестандартний сервер. на рисунку 2.5 – на стандартний.

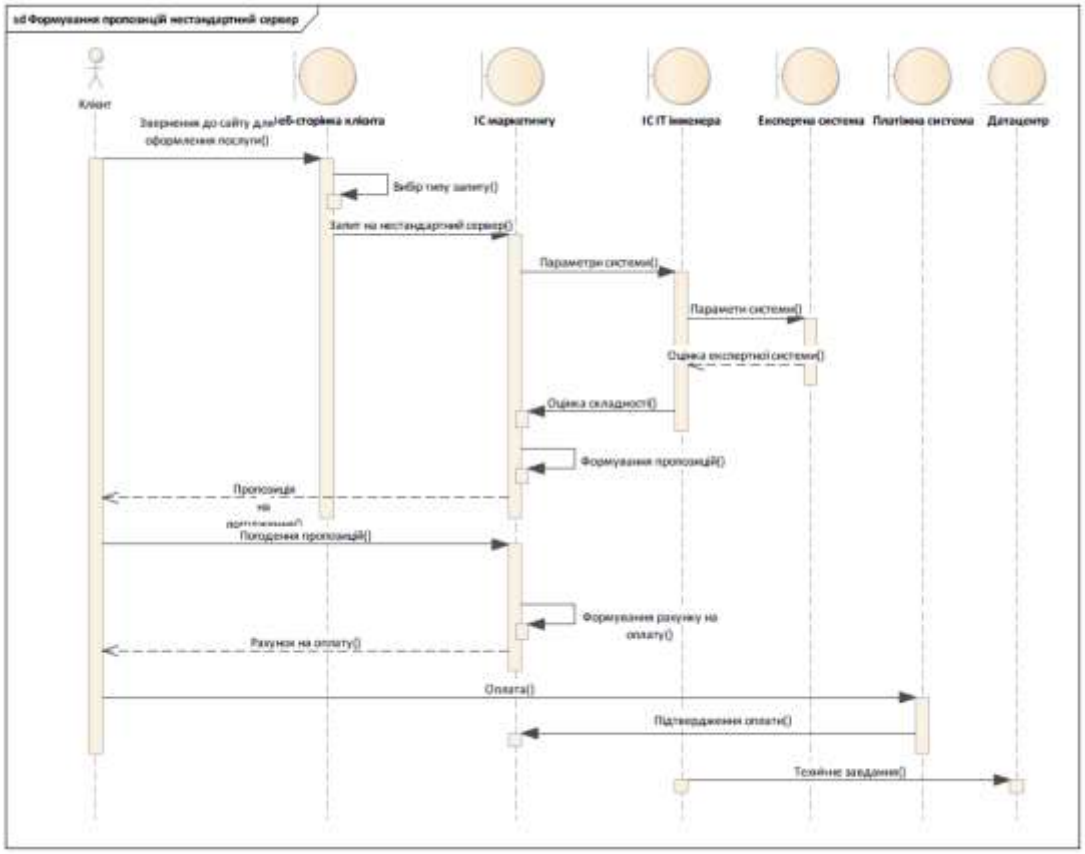


Рис. 2.4.Формування замовлення при виборі клієнтом нестандартного серверу

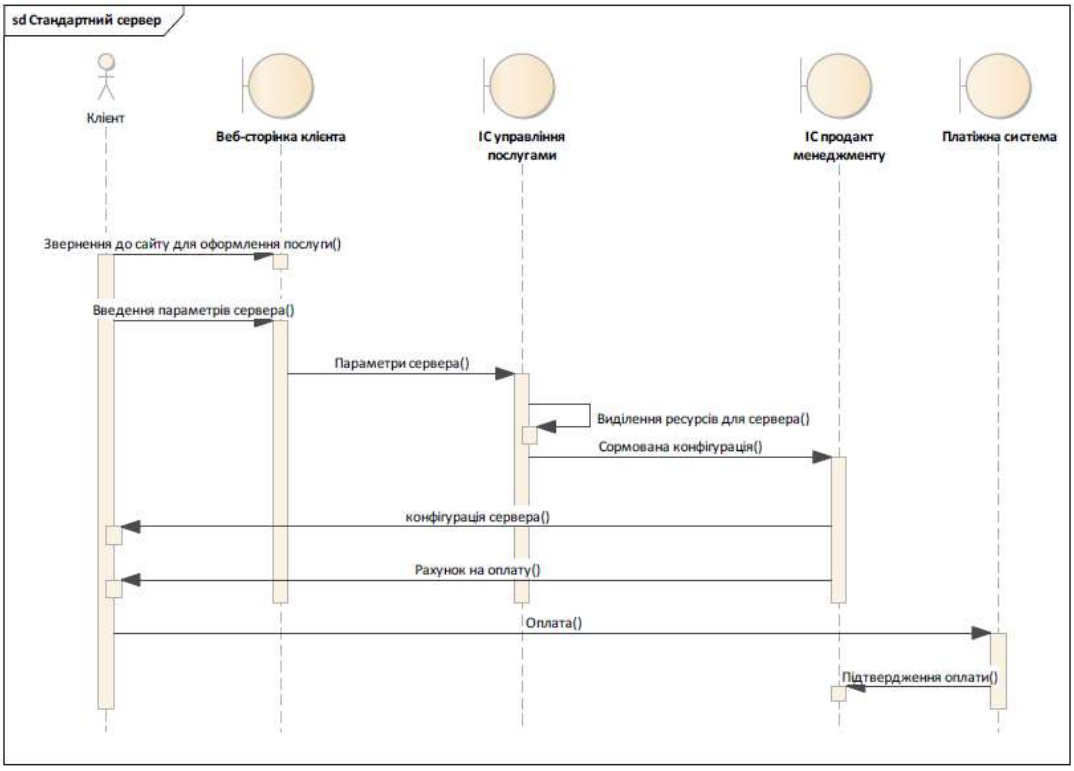


Рис.2.5. Формування замовлення при виборі клієнтом стандартного серверу

Клієнт також може обрати послугу моніторингу IT-структури. В такому випадку його заявка після попереднього узгодження параметрів моніторингу та оплати передається до експертної системи, яка і здійснює моніторинг (рис. 2.6.)

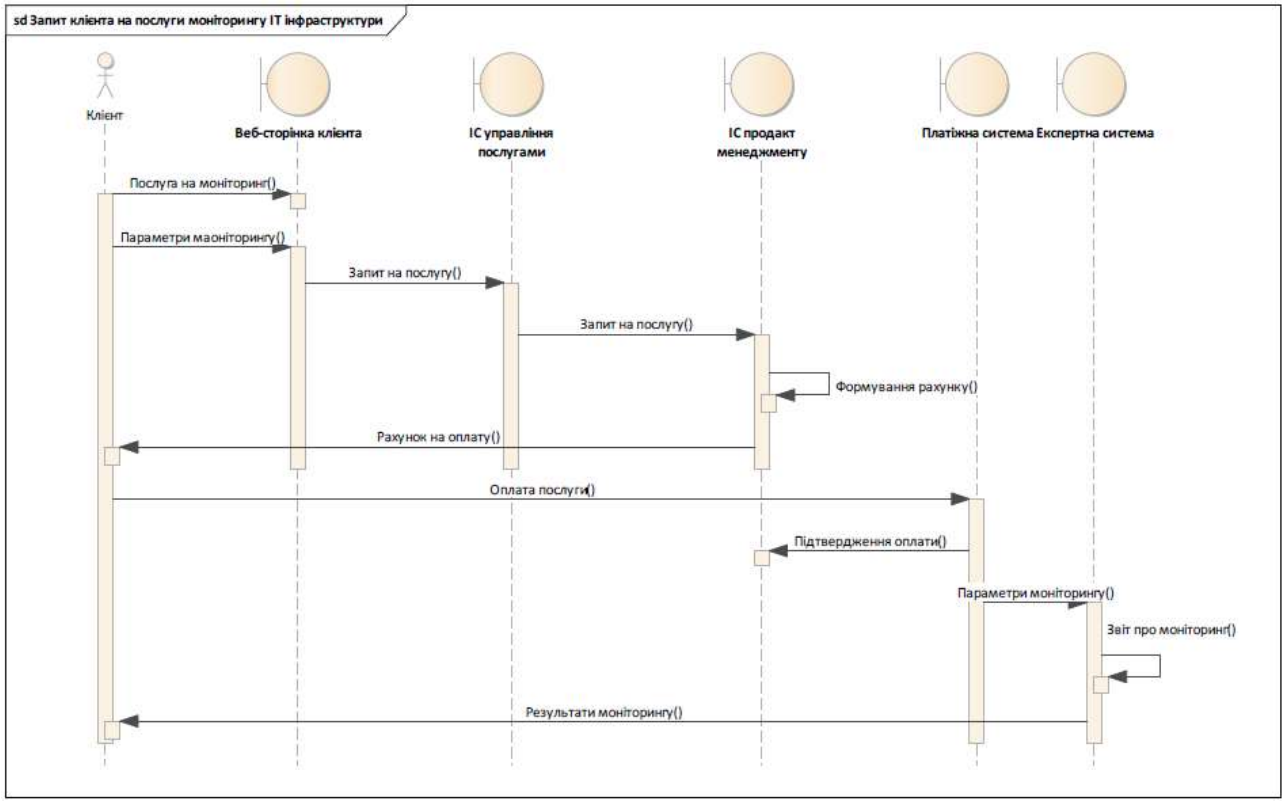


Рис. 2.6. Формування замовлення при виборі клієнтом послуги на моніторинг IT-структури

2.2. Методи та моделі інформаційної системи з управління послугами IT-провайдера

При укладанні угоди про узгодження рівня надання послуг внутрішні IT-підрозділи часто зіткнуться з тим, що штрафи за збої зазвичай є непродуктивними та втратою часу. Немає сенсу звільняти працівників, які управляють центром обробки даних, просто через те, що додаток працює повільно. Підприємства можуть передавати додатки для розміщення на серверах постачальників послуг, але виникає проблема вимірювання метрик, визначених угодою про рівень надання послуг.

Варто також відмітити, що оцінка якості надання послуг IT-інфраструктурою зазвичай здійснюється експертами однобічно, не узагальнюючи загальну картину. Наприклад, якість надання послуг IT-інфраструктурою може бути вплинута не тільки подіями та процесами, що відбуваються в самій системі після її створення та впровадження, але й самим процесом проектування та розробки системи. Це є логічним, оскільки якість впровадження системи має вплив на її функціонування в майбутньому. Тому дуже важливо, щоб компанія довіряла свою безпеку спеціалістам, які мають експертизу в цій галузі.

Багато підприємств мають розподілену мережу серверів, сховищ, мереж і застосунків, які надаються їхніми партнерами як сервіс. Кожен з цих партнерів вимагає укладення окремої угоди про рівень надання послуг (SLA). Угода про рівень надання послуг повинна забезпечувати досягнення необхідного рівня обслуговування в першу чергу. Вона повинна відображати, як система працювала у минулому, як вона працює зараз і як вона повинна працювати у майбутньому.

Прогнозний моніторинг є ключовим елементом успішного дотримання угоди про рівень надання послуг. Наприклад, одним з показників SLA може бути прийнятна швидкість реагування на скарги кінцевих користувачів. В угоді може бути зазначено, що середнє значення реакції протягом години в 500 мілісекунд є прийнятним. Початкове значення може бути 300 мс, що нижче встановленого погодинного періоду угоди. Однак з часом час реакції може повільно зростати, наприклад, до 350 мс, 405 мс, а потім до 470 мс. Якщо ми спостерігатимемо лише за значенням одного параметра, то всі ці значення можуть знаходитись у межах прийнятних параметрів. Але, якщо спрогнозувати стан системи в майбутньому, можна побачити, що час реакції стане проблемою до порушення угоди про рівень надання послуг.

Таким чином, прогнозний моніторинг і уважне спостереження за метриками дозволяють виявляти проблеми та передбачати їх перед порушенням угоди про рівень надання послуг.

Для підтримки рівня надання послуг на узгодженому рівні необхідно виявляти тенденції та вживати заходів до того, як буде порушена угода про рівень надання послуг. Одним з найкращих рішень у таких випадках є налаштування системи, що в довгостроковій перспективі призведе до покращення значень метрик. Наприклад, це може включати оптимізацію коду або масштабування обладнання.

Важливо також визначити причину проблеми. Чи сповільнюється час реакції через проблеми з додатком або через збільшення кількості користувачів? Якщо програма неефективна, можна визначити першопричину, наприклад, витік пам'яті, і спробувати оптимізувати її на рівні програмного коду. Якщо проблема пов'язана зі збільшенням кількості користувачів, потрібно масштабувати ресурси центру обробки даних для даного додатку.

Врахування цих факторів дозволить вживати необхідні заходи з покращення і уникнути порушення угоди про рівень надання послуг, забезпечуючи стабільну та ефективну роботу системи.

Особливістю інтелектуальної системи управління послугами провайдера IT-інфраструктур є моніторинг і аналіз не лише показників щодо надання послуг, а й аналіз технічного стану обладнання та мережі, аудит та надання експертиз щодо його функціонування.

При здійсненні аудиту важливо визначити порогові значення метрик (показників)

В більшості випадків, визначення порогових значень метрик для аудиту IT-інфраструктури є відповідальністю мережевого адміністратора. Виключенням є порогові значення, встановлені в промислових стандартах (TIA/EIA) та документах регулюючих органів, наприклад Міністерство цифрової трансформації України. Зазвичай вони стосуються метрик, що характеризують якість передачі даних (QoS), Всі інші, включаючи рекомендації Oracle, Microsoft тощо, є просто рекомендаціями.

Будь які метрики необхідно адаптовувати до потреб мережі підприємства.

Існують такі методи визначення (адаптації) порогових значень:

– факторний аналіз;

– метод базових ліній.

– регресійний аналіз - визначення залежності часу реакції бізнес-додатків від значень метрик, що характеризують стан IT-інфраструктури.

Сьогодні найбільш поширеним методом визначення порогових значень є метод Базових Ліній. Базова Лінія - це метрика або набір метрик, які характеризують нормальну (звичайну) роботу IT-інфраструктури. Щоб побудувати Базову Лінію, потрібно статистично обробити результати вимірювань, отриманих протягом тривалого періоду часу, наприклад, протягом місяця, і отримати "середнє" значення, яке вважається нормою.

Значення, яке перевищує (абсолютно) норму, наприклад, на 10%, 30% або 50% (інтуїтивно визначається) - вважається пороговим значенням, що відповідає оцінці "погано".

У багатьох системах моніторингу мережі Базові Лінії будуються автоматично. Існує багато способів обчислення та представлення Базових Ліній. У простих системах моніторингу - це може бути середнє значення метрики, відображене у вигляді прямої лінії, що перетинає графік вимірюваної метрики. У професійних системах - це кілька статистичних оцінок, "прив'язаних" до часу.

Це означає, що значення Базової Лінії, наприклад, о 7:00 і о 11:00, є двома різними значеннями. На Рисунках 1 і 2 показані приклади Базових Ліній, які автоматично обчислюються продуктами ProLAN. Базова Лінія 20 оцінює метрики в інтервалах по 20 хвилин і має вигляд таблиці. Базова Лінія 60 оцінює метрики в інтервалах по 60 хвилин і має вигляд трьох графіків: середнє значення, перцентиль 75 (відкидаються 25% найгірших значень) та перцентиль 90 (відкидаються 10% найгірших значень).

Перевагою методу базових ліній є його простота. Недоліком є те, що не завжди зрозуміло, яке відхилення від норми вважати інцидентом.

Другий спосіб визначення порогових значень ґрунтується на залежності часу реакції бізнес-додатків (End to End Response Time, E2E RT) від метрик, які відображають стан IT-інфраструктури.

Ідея методу полягає в наступному. Протягом представницького періоду вимірюється E2E RT та метрики стану IT-інфраструктури, після чого будується залежність E2E RT від метрик стану IT-інфраструктури, які мають найбільший вплив на E2E RT (визначаються за допомогою факторного аналізу). Знаючи таку залежність та бажане значення E2E RT, легко визначити відповідні порогові значення метрик IT-інфраструктури.

Цей підхід дозволяє дуже точно визначати порогові значення. Метод підтримується, зокрема, продуктом Trend Analyst.

Однак, незважаючи на те, що цей метод є дуже ефективним, він використовується не часто. Причиною є лінь та неуміння (або небажання) вимірювати E2E RT. Вимірювання E2E RT є важливим питанням, якому варто приділяти більше уваги.

Важливо зазначити, що несвідомість або незацікавленість вимірювати E2E RT є однією з причин, чому метод не використовується широко, хоча він дуже ефективний. Продукти ProLAN пропонують різні методи вимірювання E2E RT, які можуть бути використані залежно від потреб і можливостей, такі як Transaction Simulation та Application Instrumentation. Проте, метод Client Instrumentation, який дозволяє отримувати значення E2E RT безпосередньо з операційної системи MS Windows на стороні клієнта, знаходиться на етапі розробки. Крім того, метод Network Sniffing, який дозволяє отримувати значення E2E RT з аналізу мережевого трафіку, підтримується аналізатором протоколів GigaStor, який є розповсюдженим продуктом компанії ProLAN.

Загалом, використання цього методу для визначення порогових значень метрик стану IT-інфраструктури є точним та ефективним підходом, але вимагає свідомого підходу до вимірювання E2E RT та використання відповідних інструментів.

Факторний аналіз продуктивності додатка полягає у співставленні часу реакції додатка зі "здоров'ям" IT-інфраструктури, де працює додаток, для визначення факторів, що мають найбільший вплив на роботу додатка та оцінки цього впливу.

Час реакції додатка (RT App) можна описати такою моделлю:

RT App = F (TC, RT-IS)

TC - "чистий" час виконання коду додатка.

RT-IS - час реакції IT-інфраструктури, де працює додаток.

RT-IS = F (OHD, RT-Network, RT-Server, RT-Client)

OHD - величина накладних витрат мережевих протоколів. OHD = F (OHD1, OHD2, … OHDn);

де: OHD1 - кількість протокольних підтверджень (Turns);

OHD2 - час передачі сигналу по каналах зв'язку (RTT) та тощо.

RT-Network - час реакції мережі. RT-Network = F (RTN1, RTN2, … RTNn); де RTN1 - використання портів; RTN2 - кількість помилок передачі даних та ін.

RT-Server - час реакції сервера. RT-Server = F (RTS1, RTS2, … RTSn); де RTS1 - використання процесорів; RTS2 - використання дискової системи та ін.

RT-Client - час реакції клієнта. RT-Client = F (RTC1, RTC2,… RTCn); де RTC1 - використання процесорів; RTC2 - кількість одночасно працюючих додатків тощо.

Значимість кожного фактора (OHD, RT-Network, RT-Server, RT-Client) різна для різних додатків. Наприклад, на час реакції додатка, що базується на протоколах

CIFS і MAPI, найбільший вплив мають OHD і RT-Network, на час реакції клієнт-серверного додатка – RT-Server і т.д.

Щоб забезпечити необхідний час реакції додатка, потрібно визначити значимість (вагу) кожного фактора, вибрати найбільш значимий фактор і встановити, як час реакції додатка залежить від нього. Наприклад, якщо найбільш значимим фактором є RT-Network, то визначити, як час реакції залежить від використання портів, кількості помилок передачі даних тощо.

Для визначення значимого фактора необхідно провести кореляційний аналіз між часом реакції додатка і метриками, що характеризують здоров'я IT-інфраструктури (OHD1-OHDn, RTN1-RTNn, RTS1-RTSn, RTC1-RTCn). Для визначення того, як час реакції залежить від найбільш значимого фактора, необхідно провести регресійний аналіз. Програма Trend Analyst дозволяє автоматизувати вирішення цих завдань.

Якщо під час факторного аналізу виявиться, що найбільший вплив на час реакції додатка має OHD, то слід змінити топологію мережі або використовувати прискорювачі додатків (спеціальні пристрої, що підтримують Transparent Turns Reduction, Multiplexing, HTML Transformation та ін.). Якщо виявиться, що найбільший вплив має RT-Network, то слід або знизити корисне навантаження на мережу, або підвищити ефективну пропускну здатність мережі, або зробити обидві речі. Знизити навантаження можна за допомогою кешування та/або стиснення даних. Для цього також можна використовувати прискорювачі додатків. Підвищити ефективну пропускну здатність можна шляхом усунення дефектів і "вузьких місць" в мережі, а також застосування спеціальних технологій (pre-fetching, protocol proxy, TCP SACK, Window Acceleration тощо) Якщо виявиться, що найбільший вплив на час реакції додатка має RT-Server, то можна змінити архітектуру мережі, оновити сервер або використовувати спеціальні технології, наприклад, Load Balance.

Описані в даному розділі методи і моделі реалізовані в системі моніторингу за технічним станом IT-архітектури.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ПОСЛУГАМИ ІНТЕРНЕТ-ПРОВАЙДЕРА

3.1. Проектування бази даних для інформаційної системи з управління послугами IT-провайдера

Для інформаційної системи управління послугами IT провайдера розроблена база даних, яка вміщує інформацію про клієнта, про його замовлення та про технічні характеристики його IT-інфраструктури.

Було розроблена логічна модель, яка показана на рис. 3.1.

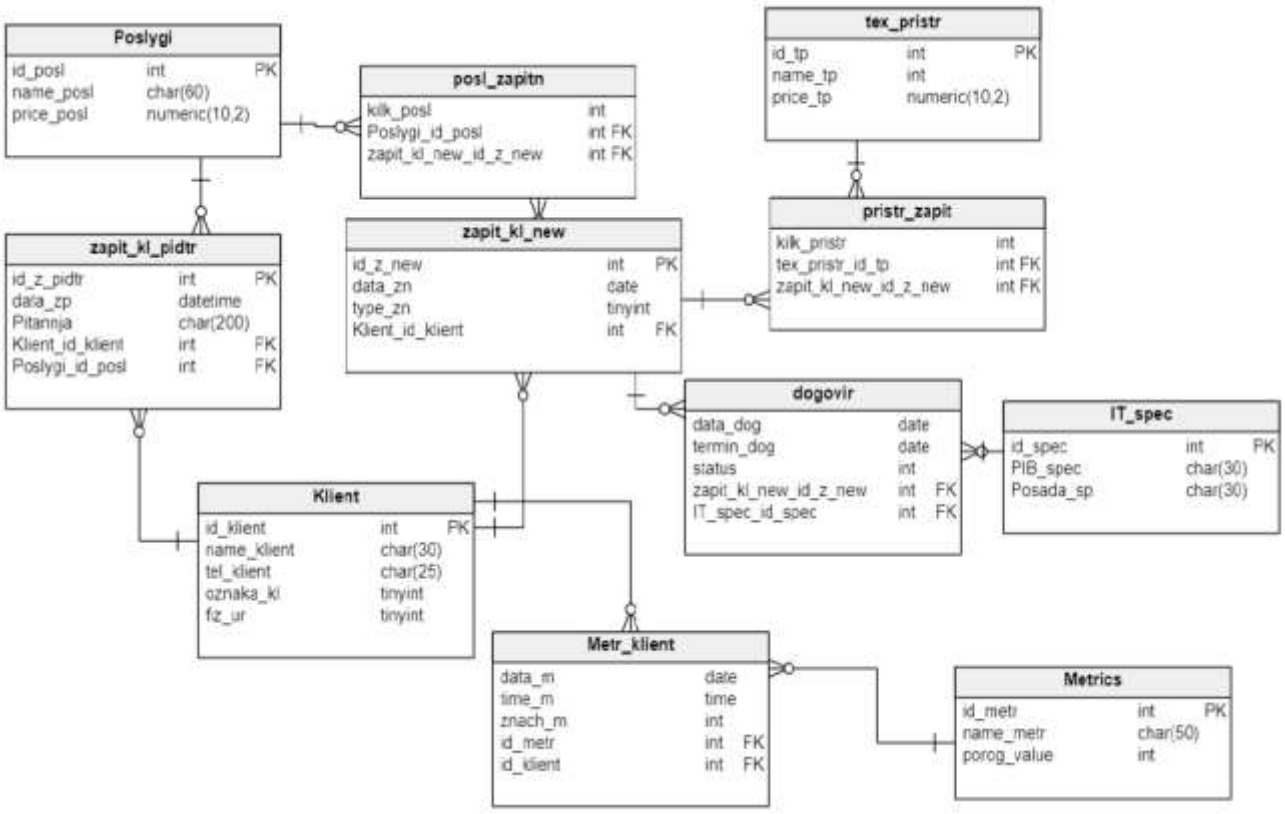


Рис. 3.1 – Логічна модель бази даних

Фізична реалізація бази даних у середовищі Microsoft SQL Server 2019.

Схема бази даних, відображена на фізичній моделі, показана на рисунку 3.2.

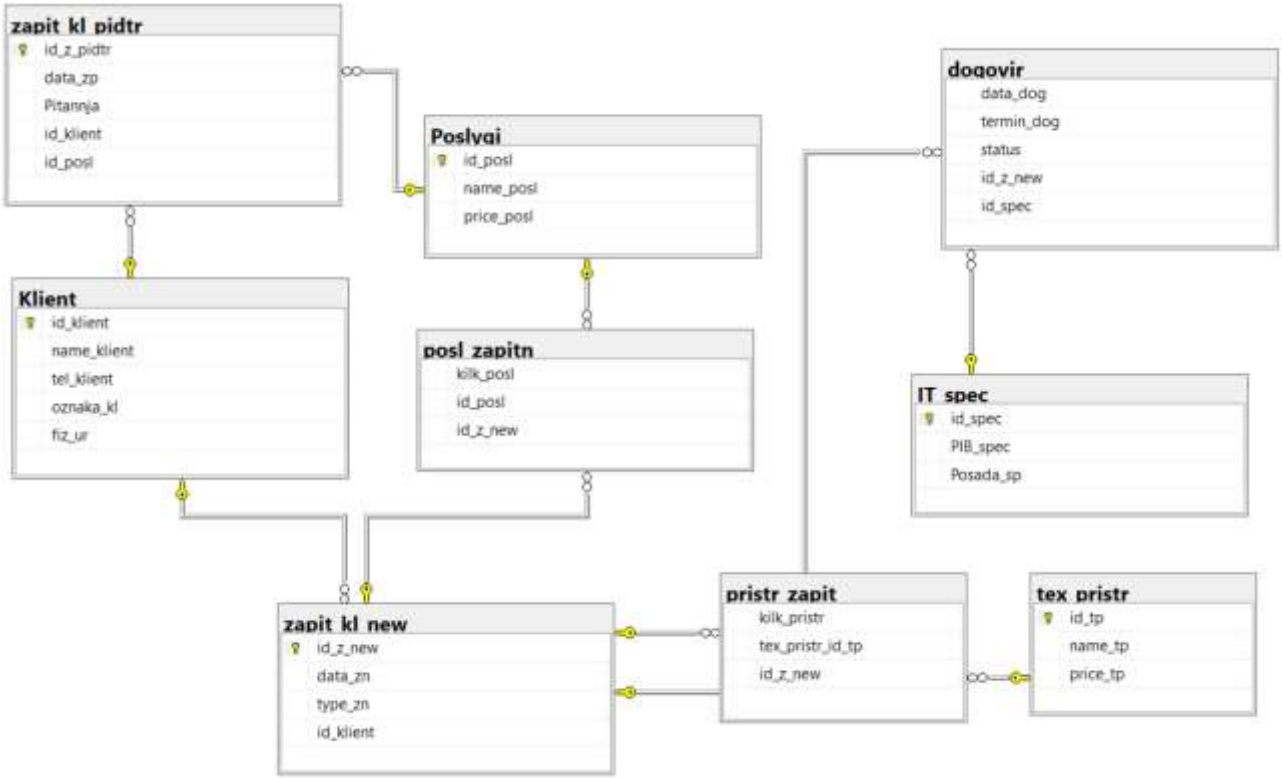


Рис. 3.2 – Фізична модель бази даних

Зміст інформаційних масивів показаний у вигляді структури інформаційних масивів в Табл. 3.1 – 3.7.

Опис масиву "Довідник послуг"

Найменування масиву – Довідник послуг

Ідентифікатор масиву – Poslygi

Найменування носія інформації – Жорсткий диск

Максимальний об’єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код покупця

Ідентифікатор індексного масиву – код послуги

Таблиця 3.1 Довідник послуг

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов'язкове поле	Індексне поле
Код послуги	id_posl	-	Integer	ПК	-	так	-
Назва послуги	name_posl	-	Char(60)	-	-	так	--
Ціна а послугу	price_posl	-	Number(10, 2)	-	-	так	

Опис масиву "Довідник клієнтів"

Найменування масиву – Довідник клієнтів

Ідентифікатор масиву – Klient

Найменування носія інформації – Жорсткий диск

Максимальний об'єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код клієнта

Ідентифікатор індексного масиву – код клієнта

Таблиця 3.2 Довідник клієнтів

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов'язкове поле	Індексне поле
Код клієнта	id_klient		Integer	PK	-	так	-
Назва клієнта	name_klient		Char(30)	-	-	так	-
Телефон клієнта	tel_klient		Char(25)	-	-	так	-
Ознака юр чи фіхз.особа	oznaka_kl		Byte	-	-	так	-

Опис масиву "Запит на нову послугу"

Найменування масиву – Запит на нову послугу

Ідентифікатор масиву –zapit_kl_new

Найменування носія інформації – Жорсткий диск

Максимальний об’єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код покупця

Ідентифікатор індексного масиву – код покупця

Таблиця 3.3 Запит на нову послугу

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов’язкове поле	Індексне поле
Код запиту	id_z_new	-	Integer	FK	-	так	ІНД -
Дата запиту	data_zn	-	Date	-	-	так	-
Тип сервера	type_zn	-	Byte	-	-	так	-

Опис масиву "Запит на клієнтську підтримку"

Найменування масиву – Запит на клієнтську підтримку

Ідентифікатор масиву –zapit_kl_pidtr

Найменування носія інформації – Жорсткий диск

Максимальний об’єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код покупця

Ідентифікатор індексного масиву – код покупця

Таблиця 3.4 Запит на клієнтську підтримку

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов'язкове поле	Індексне поле
Код запиту	id_z_pidtr	-	Integer	PK	-	так	-
Дата запиту	data_zp	-	DateTime	-	-	так	-
Суть питання	Pitannja	-	Char(200)	-	-	так	-

Опис масиву "Довідник технічних пристроїв"

Найменування масиву – Довідник технічних пристроїв

Ідентифікатор масиву –tex_pristr

Найменування носія інформації – Жорсткий диск

Максимальний об'єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код покупця

Ідентифікатор індексного масиву – код покупця

Таблиця 3.5 Довідник технічних пристроїв

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов'язкове поле	Індексне поле
Код пристрою	id_tp	-	Integer	PK	-	так	ІНД -
Назва пристрою	name_tp	-	Integer	-	-	так	-
Ціна	price_tp	-	Number(10, 2)	-	-	-	-

Опис масиву "Договір"

Найменування масиву – Договір

Ідентифікатор масиву dogovir

Найменування носія інформації – Жорсткий диск

Максимальний об’єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код покупця

Ідентифікатор індексного масиву – код покупця

Таблиця 3.6 Договір

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов’язкове поле	Індексне поле
дата договору	data_dog	-	Date	-	-	так	-
час офрмлення	termin_dog	-	Date	-	-	так	-
статус	status	-	Integer	-	-	так	-
код договору	id_dog	-	Integer	PK	-	так	-

Опис масиву "Довідник IT-спеціалістів"

Найменування масиву – Довідник IT-спеціалістів

Ідентифікатор масиву – Entity IT_spec

Найменування носія інформації – Жорсткий диск

Максимальний об’єм масиву – 1000000 записів

Довжина запису – 106 Байт

Метод організації – послідовний

Ключі упорядкування – код покупця

Ідентифікатор індексного масиву – код покупця

Таблиця 3.7 Довідник IT-спеціалістів

Найменування	Ідентифікатор у програмі	Ум. Позн. Форм.	Формат	PK\FK	Бізнес-правила		
					Умова на значення	Обов'язкове поле	Індексне поле
Код спеціаліста	id_spec	-	Integer	PK	-	так	-
ПІБ спеціаліста	PIB_spec	-	Char(30)	-	-	так	-
Посада	Posada_sp	-	Char(30)	-	-	так	-

3.2. Визначення показників для оцінки продуктивності системи

Важливою інтелектуальною компонентою інформаційної системи є розроблена система моніторингу, яка може вирішувати задачі аудиту і діагностики IT-інфраструктури підприємства. Була розроблена система моніторингу працездатності серверів Linux/UNIX.

Для цього, в першу чергу, необхіно визначити перелік показників, за якими ми будемо оцінювати систему та їх допустимі значення.

Цей тест використовується для оцінки продуктивності серверів з операційними системами, схожими на UNIX, включаючи GNU, Linux, Minix, OpenSolaris, Plan 9, BSD, FreeBSD, NetBSD, OpenBSD, AIX, HP-UX, IRIX, Mac OS X, LynxOS, QNX, SCO OpenServer, Solaris, Tru64 UNIX, UnixWare, Xenix і VxWorks.

Тест базується на використанні даних, наданих демоном SNMPD, який входить до складу пакета net-snmp для UNIX-подібних операційних систем. Порогові значення ґрунтуються на рекомендаціях від U.C. Davis, ECE Dept. Tom.

Вимірювані характеристики та порогові значення визначаються за наступними групами:

– доступність;

– використання пам'яті;

– процесори;

– інша статистика роботи системи;

– вільне місце на дисках.

Availability – доступність (%). Тестовий додаток періодично звертається до сервера по SNMP та отримує статистичну інформацію, тобто здійснює операцію отримання статистичної інформації. Операція може завершитись успішно або з помилкою. За кожний період усереднення даних обчислюється відсоткове співвідношення кількості успішних операцій отримання статистичної інформації до загальної кількості виконаних операцій.

Використання пам'яті .

Total Swap Size – загальний розмір Swap (kB). Віртуальна пам'ять системи - це сума оперативної пам'яті (RAM) і зарезервованого дискового простору (Swap). Swap використовується системою як тимчасове сховище сторінок пам'яті при нестачі вільної оперативної пам'яті. Зазвичай розмір Swap обирається удвічі більшим за розмір фізичної пам'яті, але це не є жорстким обмеженням. Для архітектури x86 розмір області Swap обмежений 2 ГБ. Деякі операційні системи використовують методику динамічного розширення розміру області Swap у разі її нестачі. Негативним фактором розміщення сторінок пам'яті в області Swap є додатковий час, який витрачається на виділення, запис і зчитування сторінок з пам'яті на диск і назад, що впливає на продуктивність системи та додатків.

Available Swap Space – доступний простір Swap (kB). Розмір вільної області Swap. Якщо в області Swap залишилося мало вільного місця, то операційній системі може не вистачати віртуальної пам'яті для запуску нового завдання або виділення нових ресурсів віртуальної пам'яті. У разі, якщо максимальний розмір області Swap не встановлений, операційна система буде динамічно його збільшувати. У такі моменти продуктивність сервера знижується. Якщо ж максимальний розмір області Swap встановлений, і цього розміру недостатньо, завдання не буде запущено через нестачу пам'яті.

Total Real/Physical Memory Size – загальний фізичний обсяг оперативної пам'яті (kB). Об'єм оперативної пам'яті на сервері.

Available Real/Physical Memory Space – доступний фізичний простір оперативної пам'яті (kB). Розмір вільної (не розподіленою системою) оперативної пам'яті, яка доступна операційній системі в момент вимірювання.

Minimum Amount of Free Swap – мінімальний розмір вільного простору в області Swap (kB). Якщо розмір вільного місця в Swap стає менше цього значення, то в тесті встановлюється дуже мало місця підкачки very little swap space left (серйозний дефіцит вільного простору у Swap). Поріг значення цієї характеристики автоматично встановлюється операційною системою сервера.

Total Shared Memory (kB) – загальний розмір спільної пам'яті (kB). Сумарний обсяг спільної пам'яті, що використовується процесами для зберігання та отримання даних і забезпечення комунікації між процесами. Існують також проблеми використання спільної пам'яті. Коли багато програм потребують швидкого доступу до пам'яті, збільшується ймовірність кешування пам'яті, що призводить до двох ускладнень:

– зв'язок процесор-пам'ять стає bottleneck (узким місцем). Спільна пам'ять, якою користуються процесори, мало масштабується.

– послідовність кешування: Кожного разу, коли інформація в кеші оновлюється одним процесором, зміна повинна бути відображена на інші процесори, інакше різні процесори будуть працювати з непов'язаними даними. З одного боку, такий протокол забезпечує надзвичайно швидкий доступ до спільної інформації між процесорами. З іншого боку, це призводить до надмірного навантаження і знижує продуктивність системи.

Total Buffered Memory – загальний розмір буферизованої пам'яті (kB). Сумарний обсяг пам'яті, який знаходиться в буферах між модулями пам'яті та системним контролером пам'яті.

Total Cached Memory – загальний розмір кешованої пам'яті (kB). Сумарний обсяг пам'яті, який кешується системою.

Very little swap space left flag. Прапорець майже повного вичерпання простору у Swap. Значення цієї характеристики автоматично встановлюється операційною системою сервера на одиницю, якщо майже немає вільного місця у Swap області пам'яті. В іншому випадку, значення дорівнює нулю.

Процесори:

Percentages of user CPU time – відсотки часу використання процесора користувачем.

Percentages of system CPU time – відсотки часу використання процесора системою.

Percentages of system CPU time – відсоток використання процесора у режимі системи.

Percentages of CPU Utilization – відсотки використання процесора. Сума відсотків використання процесора у режимі користувача і режимі системи.

Percentages of idle CPU time – відсоток часу простою процесора. Зазвичай, при низькому навантаженні, це значення дорівнює 100% мінус відсотки використання процесора. Але при значному навантаженні, відсоток простою може мати значення 0, і при цьому використання процесора не досягає 100%.

Інша статистика роботи системи.

Amount of memory swapped in from disk – кількість пам'яті, записаної з диска в Swap область (kB/s). Це вказує на швидкість, з якою система зберігає сторінки оперативної пам'яті на диск у разі її нестачі. Велике поточне значення цієї характеристики свідчить про зниження продуктивності системи.

Amount of memory swapped in from disk – кількість пам'яті, записаної у Swap-область за секунду (kB/s). Це значення відображає швидкість, з якою система зберігає сторінки оперативної пам'яті на диск при її нестачі. Велике поточне значення цієї характеристики свідчить про погіршення продуктивності системи.

Amount of memory swapped to disk (kB/s) Кількість пам'яті, прочитаної системою із Swap області (kB/s). Це вказує на швидкість, з якою система завантажує сторінки пам'яті з диска. Операційна система змушена

завантажувати дані з диска, якщо запитувані дані відсутні в кеш-пам'яті сервера. Велике поточне значення цієї характеристики свідчить про зниження продуктивності системи.

Blocks sent to a block device – блоки, відправлені на блочний пристрій (blocks/s). Кількість блоків інформації (розмір блоку можна вважати рівним 4 кБ), записаних на блочні пристрої (дискові пристрої системи), включаючи жорсткі диски, змінні носії, приводи DVD тощо. Велике значення цієї характеристики свідчить про значне навантаження дискової підсистеми сервера і, непрямо, про зниження продуктивності системи в цілому.

Blocks received from a block device – кількість блоків інформації, отриманих з блочних пристроїв (blocks/s). Велике значення цієї характеристики свідчить про значну навантаженість дискової підсистеми сервера і, в кінцевому рахунку, про зниження продуктивності системи в цілому.

Number of interrupts per second – кількість переривань в секунду. Це вказує на кількість преривань, які виникають на процесорі, включаючи переривання таймера, за одну секунду. Якщо кількість переривань перевищує 10 000 на секунду, це може свідчити про проблеми з пристроями (апаратні переривання) або про наявність помилок у програмному забезпеченні (у випадку програмних преривань). Використайте команду "procinfo" для виявлення номеру переривання, пов'язаного з проблемою, а також процесу, який з ним пов'язаний.

Number of context switches per second – кількість змін контексту в секунду. Це вказує на частоту переключень процесора для обслуговування роботи потоків процесів в системі. Значення цієї характеристики має значення тільки в контексті спільного аналізу декількох параметрів (наприклад, високе використання процесора, велика кількість переривань тощо).

Load Averages\Load-<n minutes> – середнє завантаження системи протягом 1, 5 і 15 хвилин (Load Averages\Load-<n minutes>). Операційна система сервера самостійно розраховує значення загрузки системи відповідно до рекомендацій U.C. Davis, ECE Dept. Загрузка системи обчислюється для інтервалів часу 1, 5 і

15 останніх хвилин. Порогові значення задаються на сервері у файлі конфігурації "snmpd.conf".

Вільне місце на дисках:

Available space on the disk ‘<volume name>’ (kB). Доступне місце на диску '<ім'я тома>' (kB). У файлі конфігурації "snmpd.conf" на сервері вказується список томів, для яких необхідно контролювати доступне місце. Також вказується порогове значення в кілобайтах.

Available space on the disk ‘<volume name>’ (%). Доступне місце на диску '<ім'я тома>' (%). Ця характеристика присутня, якщо порогове значення вказано не абсолютне значення в кБ, а відсоток вільного місця на диску.

Кількість процесів. У файлі конфігурації "snmpd.conf" на сервері вказується список імен процесів, кількість запущених екземплярів яких необхідно контролювати. Для кожного процесу може бути вказано максимальне та/або мінімальне порогове значення кількості процесів.

Number of processes <process name> – кількість процесів <ім'я процесу>. Показує поточну кількість процесів з вказаною назвою для порівняння з максимальним та мінімальним пороговим значеннями кількості процесів.

Size of file ‘<file path>’ – Розмір файлу '<шлях до файлу>' (kB). У файлі конфігурації "snmpd.conf" на сервері вказується список файлів, розміри яких необхідно контролювати. Опціонально, може бути вказано порогове значення розміру в кілобайтах.

Визначивши показники мережі, зпроєктуємо продукційну модель для експертної системи оцінювання працездатності мережі.

Для оцінювання безперебійної роботи сервера розробили базу правил, яку в подальшому реалізували в експертній системі. В таблицях 3.8-3.12 показана база правил для 10 характеристик системи.

Оцінка якості сервера визначається значеннями:

– погано, на екрані показники відображаються червоним кольором;

– на межі – на екрані мигаючий червоним;

– потребує уваги – жовтий колір;

– допустимо - мигаючий жовтий;

Таблиця 3.8 База правил для оцінки "погано"

№ зп	Характеристика	Одиниці вимірювання	Порогове значення	Оцінка якості
1.	Availability Доступність	%	< 90	Погано (червоний)
2.	Very little swap space left		> 0	
3.	Percentages of CPU Utilization		> 90	
4.	Amount of memory swapped in from disk	(kB/s)	> 5000	
5.	Amount of memory swapped to disk	(kB/s)	> 5000	
6.	Blocks sent to a block device	(blocks/s)	> 40000	
7.	Blocks received from a block device	(blocks/s)	> 40000	
8.	Load Averages\Load-1		> 10 (default)	
9.	Load Averages\Load-5		> 10 (default)	
10.	Load Averages\Load-15		> 10 (default)	

Таблиця 3.9 База правил для оцінки "на межі"

№ зп	Характеристика	Одиниці вимірювання	Порогове значення	Оцінка якості
1.	Availability Доступність	%	< 94	На межі (миготливий червоний)
2.	Very little swap space left		> 0	
3.	Percentages of CPU Utilization		> 70	
4.	Amount of memory swapped in from disk	(kB/s)	> 4000	
5.	Amount of memory swapped to disk	(kB/s)	> 4000	
6.	Blocks sent to a block device	(blocks/s)	> 30000	
7.	Blocks received from a block device	(blocks/s)	> 30000	
8.	Load Averages\Load-1		> 10 (default)	
9.	Load Averages\Load-5		> 10 (default)	
10.	Load Averages\Load-15		> 10 (default)	

Таблиця 3.10 База правил для оцінки "потребує уваги"

№ зп	Характеристика	Одиниці вимірювання	Порогове значення	Оцінка якості
1.	Availability Доступність	%	< 96	Потребує уваги (жовтий)
2.	Very little swap space left		> 0	
3.	Percentages of CPU Utilization		> 50	
4.	Amount of memory swapped in from disk	(kB/s)	> 3000	
5.	Amount of memory swapped to disk	(kB/s)	> 3000	
6.	Blocks sent to a block device	(blocks/s)	> 20000	
7.	Blocks received from a block device	(blocks/s)	> 20000	
8.	Load Averages\Load-1		> 10 (default)	
9.	Load Averages\Load-5		> 10 (default)	
10.	Load Averages\Load-15		> 10 (default)	

Таблиця 3.11 База правил для оцінки "допустимо"

№ зп	Характеристика	Одиниці вимірювання	Порогове значення	Оцінка якості
1.	Availability Доступність	%	< 99	Допустимо (мигаючий жовтий)
2.	Very little swap space left		> 0	
3.	Percentages of CPU Utilization		> 30	
4.	Amount of memory swapped in from disk	(kB/s)	> 2000	
5.	Amount of memory swapped to disk	(kB/s)	> 2000	
6.	Blocks sent to a block device	(blocks/s)	> 10000	
7.	Blocks received from a block device	(blocks/s)	> 10000	
8.	Load Averages\Load-1		> 10 (default)	
9.	Load Averages\Load-5		> 10 (default)	
10.	Load Averages\Load-15		> 10 (default)	

Таблиця 3.12 База правил для оцінки "добре"

№ зп	Характеристика	Одиниці вимірювання	Порогове значення	Оцінка якості
1.	Availability Доступність	%	> 99	Добре (зелений)
2.	Very little swap space left		< 1	
3.	Percentages of CPU Utilization		< 30	
4.	Amount of memory swapped in from disk	(kB/s)	< 2000	
5.	Amount of memory swapped to disk	(kB/s)	< 2000	
6.	Blocks sent to a block device	(blocks/s)	< 10000	
7.	Blocks received from a block device	(blocks/s)	< 10000	
8.	Load Averages\Load-1		< 10 (default)	
9.	Load Averages\Load-5		< 10 (default)	
10.	Load Averages\Load-15		< 10 (default)	

3.3. Реалізація інформаційної системи управління послугами інтернет-провайдера.

Для створення експерної системи була застосована мова CLIPS (C Language Integrated Production System) - це система інтегрованого продукційного середовища на основі мови програмування С. Вона широко використовується для розробки експертних систем, систем зіставлення правил та інтелектуальних додатків.

CLIPS надає зручні інструменти для моделювання знань, представлення правил і інференції на основі цих правил. Вона підтримує використання фактів, правил, шаблонів і функцій для розв'язання складних задач в різних галузях, включаючи експертні системи, діагностику, планування та інші.

CLIPS має гнучку архітектуру, яка дозволяє легко розширювати його функціональність за допомогою власних модулів та правил. Вона також

підтримує інтеграцію з іншими мовами програмування, такими як C++, Java та іншими, що робить її універсальним інструментом для розробки інтелектуальних додатків.

CLIPS є вільною і відкритою системою з відкритим вихідним кодом, що дає можливість розробникам використовувати, модифікувати і розповсюджувати його без обмежень. Вона має активну спільноту користувачів та розробників, яка забезпечує підтримку та розвиток системи.

Застосування CLIPS включають експертні системи для діагностики, планування, керування знаннями, інтелектуальний аналіз даних, автоматизацію прийняття рішень та багато іншого. Вона є потужним інструментом для розробки інтелектуальних додатків, які можуть ефективно використовувати знання та правила для вирішення складних проблем.

Мінімальні системні та технічні вимоги для виконання даного проекту зі сторони користувача та зі сторони компанії є обов`язковими для планування даного проекту в реалізацію. Баз даних характеристик можливі проблеми як на стадії користувача, який може використовувати застарілу ОС або техніку, або недостатньо потужна система з боку серверів у Дата-центрі, що спричинить падіння системи або перевантаження і зависання. Для клієнта мінімальними вимогами є:

– CPU – 1x Intel Celeron N3350 (1.1-2.4 GHz);

– RAM – 4 GB DDR3;

– 1x 500 GB SATA HDD;

– Інтегрована відеокарта HD Graphics 500.

Також потрібен стабільний доступ до глобальній мережі Internet бажано через інтернет провайдера, мобільний інтернет не має стабільного підключення що може привести до великих затримок між користувачем та серверами. Підійде стандартний маршрутизатор Wi-Fi з підтримкою швидкості 100 Mb/секунду з підтримкою стандартом зв`язку Wi-Fi 802.11b/g/a на частоті 2.4 ГГц. Після виходу в мережу він іде до обладнання у дата-центрі. Там є своє

мережеве обладнання, до якого під’єднується окрема машина. Мінімальними характеристиками даної машини для обробки даних та видачі результатів є:

– CPU – 1x Broadcom BCM2711, Quad core Cortex-72 (ARM v8) 64-bit SoC (1.5 GHz);

– RAM - 8 GB LPDDR4-2400 SDRAM;

– Підключення через 2.4 GHz and 5.0 GHz IEEE 802.11ac або Gigabit Ethernet;

– Micro-SD card або зовнішній розміром до 500 Gb;

– OpenGL ES 3.0 graphics.

Підлючення в такій системі може бути або через гігабітний дріт напряму або через Wi-Fi як резервне підключення. Усе підключення має форму – користувач по запиту із особистого кабінета – інтернет – сервер по запиту дає запит на потрібний віддалений сервер користувача. Сервер користувача може бути будь-якої форми і конфігурації.

Також не слід забувати що у дата-центрі розташований окремий сервер з даними користувачів, який постійно оновлюється реєстрацією або запитами на видалення записів, і у якому розташовані дані профілів робітників за для зручності роботи. Також автономна система живлення, яка не дає у випадку подання світла на якийсь проміжок часу і далі працювати усім серверам а також працівникам і клієнтам.

Треба розуміти, що сервер – це на одна стійка, а великий масив із десятків машин, як і користувачі це не 1 ПК, а велика кількість з`єднань з різних частин світу до їх серверів. Тому збільшення ланцюгу між Дата – центром та користувачем має під собою додаткові затрати а також втрату швидкості між клієнтом і його сервером. До того ж сервера мають декілька підмережей з різним пулом IP – адрес що приводить до висновку що сервер який відповідатиме на запити повинен знаходитись на самій першій ланці комутації щоб мати більш швидкий доступ до інших частин інфраструктури дата-центру.

Інтерфейс розробленої системи моніторингу показаний на рис.3.1-3.2.

Вимірювана метрика	Добре	Допустимо	Увага	На межі	Погано	Кількість точок
ucd_linux_test.[10.0.3.190] Host SNMP Availability (%)	>=99 94,1%	<99 5,94%	<96 5,94%	<94 5,94%	<90 5,94%	4241
ucd_linux_test.[10.0.3.190] Very little swap space left flag	<1 100%	n/a	n/a	n/a	>=1 0%	3994
ucd_linux_test.[10.0.3.190] Percentages of CPU Utilization	<=30 100%	>30 0%	>50 0%	>70 0%	>90 0%	3993
ucd_linux_test.[10.0.3.190] Amount of memory swapped in from disk (kB/s)	<=2 000 100%	>2 000 0%	>3 000 0%	>4 000 0%	>5 000 0%	3993
ucd_linux_test.[10.0.3.190] Amount of memory swapped to disk (kB/s)	<=2 000 100%	>2 000 0%	>3 000 0%	>4 000 0%	>5 000 0%	3993
ucd_linux_test.[10.0.3.190] Blocks sent to a block device (blocks/s)	<=10 000 100%	>10 000 0%	>20 000 0%	>30 000 0%	>40 000 0%	3993
ucd_linux_test.[10.0.3.190] Blocks received from a block device (blocks/s)	<=10 000 100%	>10 000 0%	>20 000 0%	>30 000 0%	>40 000 0%	3993

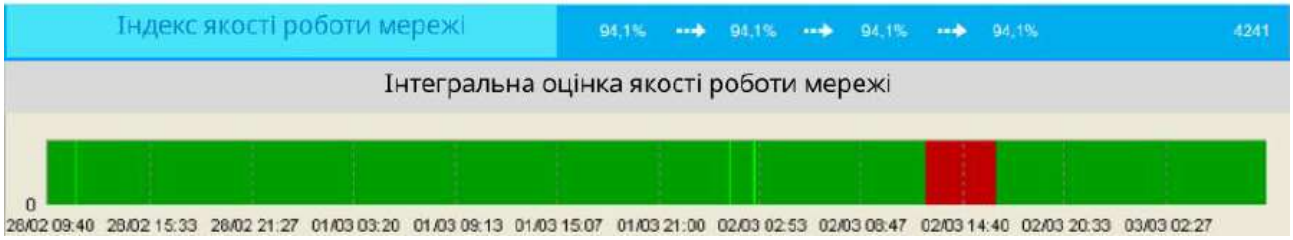


Рис. 3.1. Інтегральна оцінка якості роботи мережі

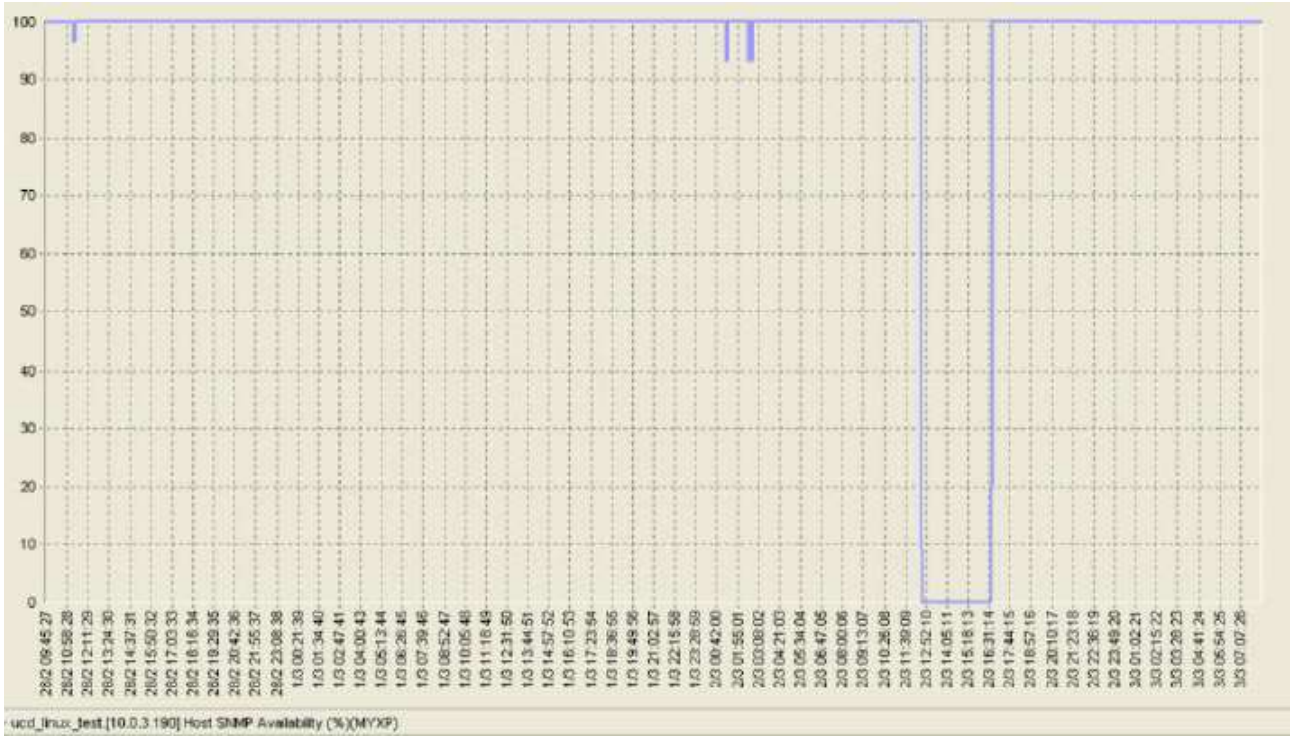


Рис. 3.2. Тест оцінки якості роботи мережі за методом базової лінії

ВИСНОВКИ

В кваліфікаційній роботі магістра досліджено питання проектування інформаційної системи з управління послугами провайдера IT-інфраструктур.

Досліджено теоретичні відомості щодо IT-інфраструктури, визначено, що IT-провайдери надають наступні послуги підприємствам, зокрема мережеві послуги, послуги конфігурації IT структури підприємства, послуги, пов’язані з розгортанням віртуального сервера.

Досліджено ринок українських IT провайдерів, визначено, на IT-ринку небагато підприємств, які надають послуги IT-провайдера.

Дослідження існуючих інформаційних систем показали, що в більшості випадків провайдери IT-інфраструктур надають послуги конфігурації стандартного та нестандартного сервера. Проте, визначено, клієнти також мають запит на моніторинг пристроїв, в той час як існуючі інформаційні системи такої функції не мають.

Отже, є потреба у створенні нової інформаційної системи, яка б дозволила не лише приймати запит на конфігурацію, але й здійснювала моніторинг IT-інфраструктури замовника.

В роботі розроблена база знань, на основі якої розроблена система моніторнгу IT-інфраструктури клієнта, яка дає можливість слідкувати за технічним станом мережі і пристроїв клієнта.

СПИСОК ЛІТЕРАТУРИ

1. Кулаков Ю.О. Комп’ютерні мережі: навч. посіб./ Ю.О. Кулаков, І.А. Жуков. – К.: вид-во Нац.авіц.ун-ту «НАУ-друк», 2009. – 392 с.
2. Буров Є.В. Комп’ютерні мережі: підручник. – Львів: «Магнолія 2006», 2010. – 262 с.
3. Лозінова Г. М. Комп'ютерні мережі: Навч. посібник. - К.: Кондор, 2003.
4. Валецъка Т. М. Комп'ютерні мережі: Апаратні засоби. Навч. посібник. К.: Ельга, 2004.
5. Стрихалюк Б. М. Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. – Львів: Львівська політехніка, 2017. – 121 с.
6. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. — CRC Press, 1996. — 794 p.
7. Бурячок В.Л., Толюпа С.В., Семко А.А. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник], К.: ТОВ «СІК ГРУП Україна, 2015. – 345 с.
8. Третяк М.О. Пристрій кодування на основі матричного коду з перевіркою на парність / М.О. Третяк, О. В. Д’яченко, Т. О. Протасова // ФЕЕ–2021: матеріали та програма міжнародної науково-технічної конференції студентів та молодих вчених, Суми, 19–23 квітня 2021. – С. 101.
9. Стеклов В.К., Беркман Л.Н. Нові інформаційні технології: транспортні мережі телекомунікацій. – К.: Техніка, 2004. – 488 с.
10. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. / П.П. Воробієнко, Л.А.Нікітюк, П.І.Резніченко. – К.: САММІТ-КНИГА, 2010. - 708 с.
11. Celik, F., A. Zengin and B. Cobanglu, 2013. Discrete event simulation-based performance evaluation of internet routing protocols. Turk. J. Electr. Eng. Co., 21: 1720-1736.

12. Pethe, R.M. and S.R. Burnase, 2011. Technical era language of the networking-EIGRP. Int. J. Eng. Sci. Technol., 3: 1-5.

13. James F. Kurose. "Computer Networking:: A Top-Down Approach", Prentice Hall, 5th Edition, pp.420-450, 2010.

14. Nefkens P-J. Phase Three: Design, Deploy, and Extend. In: Transforming Campus Networks to Intent-Based Networking. Cisco Press; 2019.

15. Бачинский В.А., Гіоргізова-Гай В.Ш., Вибір протоколу динамічної маршрутизації в корпоративній IP-мережі // Системні дослідження та інформаційні технології, №1, 2015 – 100с.

16. Vishal sharma; Rajneesh Narula; Sameer khullar."Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols", International Journal of Computer Applications (0975 – 8887), (April 2012) , Volume 44, No13.

17. Don Xu and Ljiljana Trajković, Performance Analysis of RIP, EIGRP, and OSPF using OPNET // Simon Fraser University, Canada, 2011

18. Natalia Olifer and Victor Olifer, "Computer Networks: Principles, Technologies and Protocols for Network Design", Wiley; pp. 220-240, 3th. Edition, 2006

19. Introduction to EIGRP [Електронний ресурс] // Cisco Systems, Inc. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gatewayrouting-protocol-eigrp/13669-1.html

20. Mustafa Abdulkadhim, Routing Protocols Convergence Activity and Protocols Related Traffic Simulation With It’s Impact on the Network, International Journal of Computer Science Engineering and Technology, Vol.5, Issue 3, March 2015 – 40-43 p.

21. R. Prasad and F. J. Velez, WiMAX Networks: Techno-Economic Vision and Challenges, Netherlands: Springer, 2010, doi:10.1007/978-90-481-8752-2.

22. Mohsin Masood, Mohamed Abuhelala, prof. Ivan Glesk, A comprehensive study of Routing Protocols Performance with Topological Changes in the Network // University of Strathclyde, Scotland UK, 2015

23. Enhanced Interior Gateway Routing Protocol // Cisco [електронний ресурс] - http://docwiki.cisco.com/wiki/Enhanced_Interior_Gateway_Routing_Protocol

24. Documentation Python Tutorials – Modules // Python [електронний ресурс] - https://docs.python.org/2/tutorial/modules.html

25. S. Alexander, R. Droms, "DHCP Options and BOOTP Vendor Extensions", March 1997, http://www.faqs.org/rfcs/rfc2132.html

26. J. Moy, "OSPF Version 2", April 1998, http://www.faqs.org/rfcs/rfc2328.html

27. T. Bradley, C. Brown, A. Malis, "Inverse Address Resolution Protocol", September 1998, http://www.faqs.org/rfcs/rfc2390.html

28. S. Bradner, J. McQuaid, "Benchmarking Methodology for NetworkInterconnect Devices", March 1999, http://www.faqs.org/rfcs/rfc2544.html

29. J. Klensin, "Simple Mail Transfer Protocol", April 2001, http://www.faqs.org/rfcs/rfc2821.html

30. P. Resnick, "Internet Message Format", April 2001, http://www.faqs.org/rfcs/rfc2822.html

31. R. Bush, D. Karrenberg, M. Kosters, R. Plzak, "Root Name Server

32. Operational Requirements", June 2000, http://www.faqs.org/rfcs/rfc2870.html

33. T. Hain, "Architectural Implications of NAT", November 2000, http://www.faqs.org/rfcs/rfc2993.html

34. P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", January 2001, http://www.faqs.org/rfcs/rfc3022.html

35. C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", June 2001, http://www.faqs.org/rfcs/rfc3068.html

36. S. Cheshire, B. Aboba, E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", May 2005, http://www.faqs.org/rfcs/rfc3927.html

37. T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", January 2005, http://www.faqs.org/rfcs/rfc3986.html

38. J. Weil, V. Kuarsingh, C. Donley, C. Liljenstolpe, M. Azinger, "IANA-Reserved IPv4 Prefix for Shared Address Space", April 2012, http://www.faqs.org/rfcs/rfc6598.html

39. Програма мережної академії Cisco CCNA Exploration 4.0 "Routing Protocols and Concepts" – електронний курс, 2009р.

40. Павликевич, М. Телекомунікаційні мережі. Ч. 2 Мережі IP [Текст] : лекції для студентів спеціальності 7.092402 "Інформаційні мережі зв’язку" / М. Павликевич. – Львів : Національний університет "Львівська політехніка", 2009. – 216 с.

ДОДАТКИ