

УДК 004

О.Щельник, магістр гр. КІ-23М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ ІНФРАСТРУКТУРОЮ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи керування інфраструктурою ЦОД. Метою розробки є дослідження та програмна реалізація системи керування інфраструктурою ЦОД. Об'єктом дослідження є процес керування інфраструктурою ЦОД. Предметом дослідження є методи керування інфраструктурою ЦОД. Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування інфраструктурою ЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Системи керування інфраструктурою ЦОД дозволяють власникові ЦОД одержати повне подання про те, що відбувається на об'єкті.

Таке різноманітне господарство, яким є сучасний обчислювальний центр, або, у сучасній термінології, центр обробки даних, вимагає однакового керування. Однак численні підсистеми, з яких складається його інфраструктура, традиційно контролювалися за допомогою окремих спеціалізованих систем керування. Системи керування інфраструктурою ЦОД покликані якщо не замінити, то об'єднати їх всі, щоб власник ЦОД міг мати повне подання про те, що відбувається на об'єкті.

В останні роки ринок систем керування інфраструктурою ЦОД (Data Center Infrastructure Management, DCIM) бурхливо розвивається, а найближчі перспективи виглядають ще більш райдужними. По оцінках Navigant Research, в 2023 році його обсяг склав 663 млн доларів (при цьому враховувалися продажі програмного забезпечення й послуг). Відповідно до недавно опублікованого дослідження MarketsandMarkets, за період з 2023 по 2029 рік ринок DCIM виросте з 307 млн до 3,14 млрд доларів. Таким чином, його середньорічний ріст складе 47,33%. На думку аналітиків цього агентства, основним драйвером росту є потреба в забезпеченні високої доступності й стійкого розвитку центрів обробки даних.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування інфраструктурою ЦОД.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування інфраструктурою ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем керування інфраструктурою ЦОД.
- Дослідження системи керування інфраструктурою ЦОД.
- Програмна реалізація системи керування інфраструктурою ЦОД.

Об'єктом дослідження є процес керування інфраструктурою ЦОД.

Предметом дослідження є методи керування інфраструктурою ЦОД.

Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Усього лише п'ять років тому ринок систем керування інфраструктурою дата-центра (DCIM) тріпотів від захвату: першим адептам була надана

можливість скористатися функціями моделювання й перегляду у високому дозволі поетажних планів і стійок, розташованих усередині дата-центра.

На першому етапі розвитку ринку DCIM це було воістину вражаючим досягненням: створити точну модель дата-центра за допомогою одного лише зображення, яким можна маніпулювати на екрані монітора й виводити в різних формах залежно від цілей документування. Більш ніж десяток розроблювачів перших DCIM видавали на-гора одну демоверсію за іншою, при цьому головним критерієм якості в рекламних проспектах вказувався ступінь реалістичності зображення стійок.

Кінцеві користувачі оцінили результати візуалізації, надані ранніми версіями DCIM, але проте, вони чекали більшого: нова технологія повинна була допомагати в рішенні комерційних завдань. У деяких випадках можливість легко моделювати й документувати свою IT-структуру була сама по собі достатньою, і рішення купувалася винятково як засіб візуалізації, але ринок чекав, коли ж виявить себе комерційна цінність цієї концепції.

У другій, сучасній фазі розвитку технології DCIM завдання з'єднання DCIM-моделі із зовнішнім миром у реальному часі стала ключовою. Основна комерційна цінність будь-якого рішення DCIM полягає в тому, наскільки добре воно інтегрується із загальною системою керування дата-центром (яка включає керування будинком). Мова йде не тільки про джерела живлення й датчики температури, але й про повний процес керування інформаційними сервісами й системами (ITSM). Чим більше інформації, тим якісніше прийняті на її основі рішення. У світі, орієнтованому на створення рентабельних Каталогів Сервісів, можливість такого підключення стає єдиним способом розрахувати реальні витрати, пов'язані з наданням тих або інших послуг.

Націлена на зниження експлуатаційних витрат, система DCIM сьогодні – чи не краще рішення по оптимізації дата-центра і його поточних операцій. DCIM використовується для забезпечення й реалізації найкращих методів, а також стандартизації роботи підприємства й всіх його дата-центрів. DCIM створює найбільш експлуатаційно-придатні структури, де всі використовувані процеси створення й підтримки інформаційних систем можуть бути оптимізовані, захищені й відтворені незалежно від того, хто їх створив і де вони перебувають на будь-якому етапі розвитку підприємства.

Сьогодні можна спостерігати деякі ключові тенденції в комплексі DCIM. Тут я приведу десять із них.

Два аспекти керування

На сьогоднішній момент сформувалися дві основні групи пропозицій у сегменті ринку DCIM:

- керування інформаційними ресурсами в стійках протягом тривалих тимчасових проміжків;
- керування механічними, електричними елементами й водопровідною арматурами, або керування енергопостачанням і охолодженням об'єкта.

Більшість розроблювачів починають визнавати наявність обох груп і необхідність розробляти такі рішення, які стерли б границю між ними. Сьогодні кожен вендор, працюючи над рішенням, фокусується, як правило, на одному аспекті, у більшості випадків лише неспішно переборюючи границю між ними, щоб в обмеженому обсязі задовольнити потреби іншої сторони. Чи вдасться звести ці аспекти воедино? Час покаже. Надія є, але поки створити реальне рішення для такої єдиної платформи DCIM не вдається жодному із гравців.

DCIM як інструмент стратегії

У міру того як відношення до технології мінялося (від опції до предмета першої необхідності), більшість кінцевих користувачів зрозуміли, що DCIM повинна стати не просто ще одним тактичним інструментом, але й частиною стратегії керування.

Дата-центри протягом останнього років росли, поступово розширюючи свого функціонала з появою кожного нового інструмента. Сьогоднішній тренд – мислити стратегічно й знаходити більше продуктивні рішення для всіх зацікавлених осіб. Найбільш успішні проекти показали, що від впровадження DCIM починають вигравати широкі шари

користувачів багатьох галузей, внаслідок чого відношення до DCIM міняється від «непогано б мати» до «необхідно мати». Деякі з нині діючих впроваджених DCIM-моделей використовуються сотнями клієнтів зі сфери інформаційних технологій, фінансів, інфраструктурних проєктів, навіть управлінського сектора вищої ланки. DCIM проявляє себе щонайкраще, якщо вона розглядається як стратегічний інструмент, і її ефективність прямо може бути пов'язана з витратами на будівництво й зміст дати-центра.

Статус Системи Зберігання Даних

У міру посилення взаємного проникнення цифрових технологій у дата-центрі споживачі мають потребу у всі меншій кількості інструментів. Стало тенденцією шукати більше зроблені рішення, у яких використовується принцип обміну даними. Інструменти, що вимагають дублювання даних, поступово відмирають. Інтеграція на рівні конвергентної інфраструктури (CI) має критичне значення. У найбільш успішних DCIM-інсталяціях інтеграція репозиторія DCIM з іншими системами настільки висока, що DCIM сама по собі стала розглядатися як «система записів», або «база даних» активів дати-центра.

Фактично DCIM стає самою точною моделлю дата-центра, у багатьох випадках навіть більше точною, ніж бухгалтерські реєстри.

Зміни в дата-центрі через реінжиніринг процесів

Дата-центри завжди були площадками, на яких відбуваються зміни: там увесь час щось міняється. Бездоганно-прозорий дизайн дати-центра швидко перетворюється в хаотичне накопичення відновлень, які погано задокументовані й часто зовсім неефективні. Сьогоднішній тренд – перспективне планування всіх змін, які відбудуться в дати-центрі.

По ідеї, ефективність дата-центра не буде падати, якщо використовується стругаючи система керування змінами. Якщо зміни параметрів виробляються за допомогою системи керування змінами (яка є частиною DCIM), ця модель завжди буде залишатися точним відбиттям стану самого дата-центра й дозволить підтримувати його в оптимізованому стані. Таким чином, сьогодні тенденція полягає в тому, щоб шукати рішення комерційних питань шляхом аналізу DCIM-моделі, а не в процесі блукання між рядами стійок дата-центра в надії одержати відповіді лише на підставі спостереження за тим, що відбувається в серверному залі.

Ріст популярності SaaS

Хоча впровадження DCIM спочатку розглядалося як рішення локальне, багато розроблювачів уже тоді почали пропонувати програмне забезпечення як сервіс (SaaS). Можливості DCIM як сервісу стають ідентичними локальному рішенню окремого розроблювача.

Причина цього тренда, тобто використання SaaS-версії DCIM, криється в тому, в тому, що пропозиція у вигляді сервісу SaaS можна віднести в статтю операційних витрат, а не капітальних витрат. Хоча процес прийняття ринком цих сервісів може бути однаковий, проте існує думка, що пропозиції SaaS більше відкриті й гнучкі. Важливо помітити, що в той час як DCIM традиційно відносять до сегмента сервісів, підхід до реалізації DCIM безпосередньо на площадці, або у вигляді SaaS-варіанта повинен бути однаковим, якщо ви хочете успішно впровадити цю систему.

DCIM – більше не «річ у собі»

У той час як раніше функціональність досягалася за рахунок окремо взятих можливостей, нині особливо важливою є інтеграція в системи керування ІТ-інфраструктурою (ITSM), включаючи керування змінами й керування конфігураційними базами даних (CMDBs). Сьогоднішня тенденція – побудувати більше високий рівень інтеграції на етапі вибору DCIM-провайдеру. Інтеграція в системи ITSM необхідна для того, щоб зробити DCIM стратегічною частиною інфраструктури керування дата-центром. Взагалі, підхід до впровадження DCIM без обліку подальшої інтеграції залишився далеко в минулому.

Перспективи використання DCIM у співвідношенні з іншими ключовими інструментами керування тепер повністю прогнозуються з першого дня розробки проєкту.

Тісна інтеграція із засобами віртуалізації

На сьогоднішній день уже більше половини серверів у світі віртуалізовані. Таким чином, має сенс тісно інтегрувати найбільш успішні DCIM-рішення з топовими галузевими віртуальними платформами.

Тенденція сьогодні – шукати рішення, що дозволяють одержати в реальному часі подання про статус віртуального сервера на кожному з фізичних пристроїв. DCIM повинна забезпечувати зображення контрольованого вузла і його операційних систем у режимі реального часу. Зараз прагнуть використовувати зв'язану картину віртуалізації для планування навантаження від операційної системи до сервера, і, в остаточному підсумку, до необхідних фізичних ресурсів (приміщення, енергопостачання, охолодження).

Ріст використання убудованих датчиків

Завдання контролювати параметри середовища в дата-центрі існували завжди, але рішення були громіздкими й дорогими. Сьогодні виробники ІТ-Устаткування шукають рішення, що дозволяють вбудовувати апаратні датчики в кожний пристрій промислового класу, що випускається ними. Ці датчики можуть надавати звіт про енергоспоживання, про температуру усередині різних зон дата-центра й про фізичну безпеку. Тенденція полягає в тому, щоб найбільше ефективно використовувати убудовані датчики й комбінувати їх з додатковими (звичайно бездротовими) для тих пристроїв, які не перебувають на площадці основного встаткування.

Точна оцінка активів конвергентної інфраструктури

Серед корпоративних дата-центрів простежується тенденція до забезпечення процесів перевірки й балансування з метою увесь час зберігати впевненість в тому, що DCIM-модель точно відбиває ситуацію в серверному залі. Такий подвійний контроль приймає різні форми, від перевірки вручну з використанням електронних таблиць, до використання бездротового зчитувача штрихкоду й/або локальних технологій, заснованих на автоматизованому використанні радіочастотних міток (RFID). Можлива навіть комбінація інформації, отриманої візуальним способом, з даними від системи виявлення або від коннекторів конфігураційної бази CMDB.

У кожному разі, є тенденція до підвищення точності відображення моделей дата-центрів будь-якими можливими засобами, через ITSM-інтеграцію, інтеграцію із системою віртуалізації, а також за допомогою технологій, наявних на самій площадці.

Загальнокорпоративне впровадження DCIM

Рішення DCIM спочатку пропонувалися як засіб візуалізації десятки стійок. З ростом комерційної ефективності зі стратегічної точки зору масштаб впровадження DCIM значно розширився, аж до того, що деякі постачальники DCIM-рішень тепер обслуговують десятки тисяч стійок у десятках дата-центрів.

Не варто забувати, що в рамках DCIM-пропозиції всі об'єкти, включаючи ті що розташовано усередині іншого будинку, модульні, а також комерційні ЦОД з сервісами колокейшен, розглядаються як площадки дати-центра. Іноді можна зустріти десятки площадок, які потрібно сукупно представити в єдиному DCIM-рішенні. Сьогоднішні рішення прагнуть охопити все компоненти, у будь-якому масштабі, незалежно від їхнього фізичного розташування.

У цей час ми спостерігаємо розвиток технології DCIM, що відбуває в основному завдяки зрушенню від ідеї дата-центра як тактичного набору функцій до дата-центру – добре осмисленому стратегічному інструменту. Постачальники DCIM розуміють, що їм потрібно фокусуватися на високоефективній послугі в декількох підсистемах, а не заспокоюватися на досягненнях у сфері підвищення деталізації картинки. Кінцеві користувачі тепер повинні формулювати свої індивідуальні вимоги до DCIM набагато більш докладно, ніж коли-або в минулому. Фактично, від ІТ-організацій тепер вимагають чітко роз'яснити состав портфеля сервісів, виділяючи кожний сервіс в окремий рядок каталогу. Система DCIM стає життєво важливим компонентом у створенні таких елементів каталогів сервісів, оскільки її завдання зрештою зводиться до керування витратами.

Отже, як же виглядає наступна фаза розвитку DCIM? Очевидно, це буде контроль і оркестровка. Це зрівноважить моделювання й зв'язність, удосконалені в перших двох фазах, і привнесе новий рівень автоматизації з використанням електронних систем керування, що замінюють участь людини при прийнятті рішень.

У більшості випадків пристрої автоматизації стають засобом виконання складних наборів правил, заснованих на більших обсягах метричної інформації. Незважаючи на те, що наступна фаза буде визрівати набагато довше внаслідок різноманітності середовища провайдерів послуг дата-центрів, саме ця фаза DCIM дозволить знизити рівень витрат до бажаного.

Розробка структурної схеми

Як ми вже відзначали, представлені на ринку рішення DCIM мають самих різних корінь. У числі перших на перспективі цього ринку звернули увагу постачальники структурованих кабельних систем, оскільки в більшості з них уже були інтелектуальні напівавтоматизовані системи для керування кабельними з'єднаннями. При величезній кількості фізичних з'єднань у ЦОД наявність актуального кабельного журналу є серйозною підмогою, якщо необхідно, наприклад, визначити, які перекомутації потрібні для підключення нових серверів. Традиційний підхід, коли системний адміністратор тримає в пам'яті всі зроблені комутації або в найкращому разі веде кабельний журнал в електронному виді, у сучасній віртуалізованому середовищі чреватий численними помилками. Уникнути їх допомагають зручні інструменти, які надаються системами керування кабельною інфраструктурою.

Спеціально розроблена програма, що враховує необхідну послідовність операцій на кожному етапі, допоможе значно спростити весь цей процес, у тому числі й при будівництві нового ЦОД. Компанія TE Connectivity пропонує відразу дві системи моніторингу кабельних з'єднань – AMPTRAC і Quareo, у яких використовуються різні принципи ідентифікації з'єднань. Якщо в AMPTRAC для детектування з'єднань застосовується традиційна технологія дев'ятого провідника, то в Quareo – технологія Connection Point Identification. В останньому випадку у вилку кожного коннектора вбудовується мікрочип, а в гнізді комутаційної панелі розташовуються додаткові ламелі, які при підключенні цієї вилки зчитують інформацію й реєструють її в ПЗ.

На чипи заводським способом заноситься наступна інформація про комутаційний шнур: категорія, довжина, колір, полярність і т.д. Аналогічні відомості втримуються й у комутаційній панелі. У системі не передбачається використання центральних сканерів – кожна панель і кожний крос мають свій IP-адресу, так що до них можна звернутися з Web-Браузера, навіть не використовуючи спеціальне ПЗ. І в качані, і в гнізді комутаційної панелі є лічильник підключень, що по здійсненні заданої кількості підключень подасть сигнал про необхідність проведення регламентних робіт.

Даний підхід дозволив мінімізувати тимчасові й трудові витрати. Опираючись на схожі принципи, у даній роботі розробимо власне ПЗ Infrastructure Configuration Manager (ICM), що для всіх елементів бази даних (не тільки пасивного й активного встаткування, але також кімнат, кабінетів, поверхів, будинків, лотків і т.д.) може генерувати QR-код.

Код може бути роздрукований і наклеєний на встаткування. Потім QR-коди зчитуються убудованою камерою мобільного пристрою за допомогою додатка ICM Mobile і розпізнаються, а інформація із сервера ICM по даному об'єкті або встаткуванню, отримана по каналах Wi-Fi, виводиться на екран. Таким чином, всі операції по адмініструванню можна відслідковувати, зміни в конфігурації з'єднань – документувати, а потрібна інформація, наприклад про поточний статус будь-якого кінцевого пристрою, оперативно виводиться на екран пристрою.

ICM може застосовуватися і як окреме програмне рішення, і разом із системами моніторингу кабельних з'єднань, які компанія TE Connectivity пропонує (у цьому випадку підвищується ступінь автоматизації операцій комутації й гарантується актуальність

інформації в базі даних). За допомогою API воно може бути інтегроване у вищестоящі системи керування мережею (NMS) і інфраструктурою ЦОД (DCIM).



Рисунок 1 – Структурна схема системи

Ідентифікація точок з'єднання (Connection Point Identification – CPID) якраз забезпечується за рахунок використання мікрочіпів. Дані мікрочіпи містять інформацію про фізичні характеристики шнура, включаючи порядковий номер з'єднувача, тип, клас, довжину тощо, що відноситься до підключених комутаційних шнурів. При підключенні ця інформація зчитується і реєструється в базі даних ICM за допомогою вбудованого в панель сканера.

Ізраїльська компанія Ri Technologies першою запропонувала систему інтерактивного керування СКС ще в 2002 році. З тих пір вона постійно неї вдосконалювала, і в результаті з'явилася принципово нова система PV+. Розроблювачам удалося перебороти традиційний недолік СІУ для СКС, через якого вони виявлялися надмірно дорогими в реалізації: уперше подібна система дозволяє обійтися без кросс-коннекта.

Через необхідність застосування кросс-коннекта доводилося піклуватися про виділення для нього місця в шафі й придбання додаткових розподільних панелей, що, у свою чергу, вело до додаткових прямих і непрямих витрат. Ri розробила спеціальну вставку з мікрочипом і діодом для установки в порти активного встаткування. За допомогою вставки ідентифікуються порти активного встаткування й, якщо потрібне виконання операцій підключення/кроссування, здійснюється їхнє індивідуальне підсвічування. Інтерконнект можна використовувати як для оптики, так і міді.

На основі рішення програмної оболонки PV+ був розроблений продукт CenterMind, що згодом компанія має намір розвинути в повноцінну систему DCIM. Поки ж, крім адміністрування кабельної підсистеми, CenterMind дозволяє контролювати ще дві апаратні підсистеми: P+ для моніторингу живлення за допомогою інтелектуальних панелей живлення (Power Distribution Unit, PDU) і G+ для контролю навколишнього середовища – температури, вологості, протікання і т.д.

Крім контролю пасивних з'єднань, CenterMind «уміє» автоматично виявляти встаткування, у тому числі детектувати підключення авторизованих/неавторизованих пристроїв. Наприклад, можна задати, що до конкретної розетки дозволено підключати тільки пристрою з певними адресами й іменами. (По суті, у цій частині вона дублює можливості системи керування активним мережним устаткуванням.) Модуль автоматичного виявлення Automated Discovery дозволяє скласти точну візуальну карту центра обробки даних з усіма стійками, шафами, комутаторами, серверами й іншими пристроями. На карті відображається інформація про фізичне розташування пристроїв, з'єднання між ними, про IP- і MAC-адреси, тип і ім'я хоста.

Інструментарій для планування ємності, виділення ресурсів і керування життєвим циклом активів допомагає оптимальним образом розмістити нове встановлюване обладнання з обліком таких змінних, як місце, живлення, охолодження, доступні порти й т.п. Наприклад, при розміщенні сервера досить вибрати відповідну модель із великого списку

підтримуваного встаткування (якщо потрібної моделі в списку ні, те її можна туди внести самостійно). Система сама врахує вагу пристрою, габарити, кількість необхідних інформаційних розеток, рівень енергоспоживання й запропонує оптимальне місце для його розміщення.

Через відсутність деяких компонентів CenterMind поки не можна назвати повноцінної DCIM – зокрема, вона не дозволяє контролювати систему кондиціювання. Однак за допомогою наявного комплекту SDK її можна об'єднати з іншими системами рівня систем керування будинком (Building Management System, BMS).

Повний облік і контроль

Спроби впровадження платформи DCIM часом закінчуються невдачею через неможливість виявляти й урахувати всі активи, конфігурації й дані про статус серверів, систем зберігання, мережного встаткування, інженерних і інших допоміжних систем, особливо у випадку успадкованих архітектур. Процес збору даних вручну надмірно витратний, забирає багато часу й чреватий помилок. Однак без реальної картини поточного стану ЦОД неможливо побудувати повноцінну модель центра обробки даних, а виходить, рішення по оптимізації процесів експлуатації й модернізації ЦОД можуть виявитися необґрунтованими й помилковими.

Різні підсистеми ЦОД, наприклад обчислювальна й телекомунікаційна, тісно взаємозалежні, і багато замовників хотіли б документувати їх в одному середовищі. Необхідні засоби їм надає програмний пакет FNT Command німецької компанії FNT Software. Компанія споконвічно створювала семирівневу (збіг із числом рівнів OSI випадково) модель даних, що охоплює й IT-інфраструктуру (IT-модули), і телекому-складові, і інженерні системи. При документуванні ЦОД можна вносити всі необхідні дані й атрибути самого будинку й інженерної інфраструктури, урахувати наявні фізично активи (де коштують стійки й перебуває те або інше «важке» устаткування), указувати логічні з'єднання поверх існуючих фізичних і т.п. Якщо в обчислювальному середовищі або середовищі передачі даних є віртуалізовані системи, їхньої характеристики теж можна документувати із прив'язкою до фізичних активів, і т.д. – аж до рівня додатків і бізнес-сервісів.

Якщо інформація вже представлена в електронному виді, її можна імпортувати в систему. При наявності можливості підключатися до встаткування по SNMP або інших протоколах система автоматично збирає необхідну інформацію (можлива інтеграція з наявними засобами моніторингу). Із системою поставляється бібліотека встаткування на 60 тис. одиниць – телекомунікаційні пристрої, сервери, кабелі й багато чого іншого. При відсутності встаткування в базі даних воно буде додано в рамках технічної підтримки. Мобільний клієнт дозволяє сканувати штрих-коди й працювати з RFID-мітками.

Система містить потужний модуль планування. При підготовці змін завжди можна одержати інформацію про поточний статус системи, подивитися на план поверху або стійки й сформулювати вбрання на роботу, що буде деталізований і з потрібної гранулярністю виданий виконавцям. Дуже часто ця функціональність використовується як база для розрахунків за роботи, зроблені зовнішніми організаціями, або контролю їхньої якості й строків виконання. Крім того, система дозволяє спрогнозувати, до чого можуть привести заплановані зміни.

Найчастіше впровадженню подібних систем перешкоджає їхня дорожнеча. FNT Software пропонує привабливу модель ліцензування: незалежно від масштабу ЦОД ліцензування здійснюється по кількості користувачів, що мають право на перегляд і внесення змін (останні дорожче), – ні стійки, ні встаткування не враховуються. Систему FNT Command доцільно впроваджувати при наявності 100 і більше стійок.

У кожному разі порахувати ROI від впровадження такої системи непросто. На підприємстві Volkswagen Group, де рішення FNT використовується вже 10 років, IT-відділ обґрунтував його необхідність у такий спосіб. Керівництво вимагало забезпечити зниження операційних витрат на 5% у рік, а цього можна було домогтися тільки шляхом автоматизації типових дій співробітників, тому що звільняти їх або змушувати працювати позаурочно законодавство не дозволяє. Оскільки не можна поліпшити операційну діяльність, не

задокументував споконвічний стан всієї IT і телекомунікаційної інфраструктури (із чимсь треба порівнювати), вивід про впровадження FNT напрошувався сам собою. У результаті поставлена перед IT-Фахівцями бізнес-завдання успішно виконується.

Обґрунтування інвестицій в DCIM

Дотепер багато компаній не до кінця розуміють, які вигоди вони одержать від впровадження DCIM. Відповідно до опитування, проведеному серед 825 керівників американських компаній, відповідальних за прийняття рішень у сфері IT, 90% з них хотіли б мати можливість явного розрахунку й аналізу повернення вкладень для обґрунтування своїх інвестицій. Щоб допомогти їм підготувати таке формальне обґрунтування, Emerson Network Power (при участі Forrester Research) розробила калькулятор ROI.

Методологія, що використовує Forrester Research, називається Total Economy Impact (TEI). Вона дозволяє поряд з витратами й вигодами враховувати стратегічні переваги й потенційні ризики. При її застосуванні передбачається більше широкий погляд на те, як впровадження рішення вплине на бізнес: що зміниться для користувача, наскільки підвищиться його ефективність, чи зручно йому буде вирішувати варті перед ним завдання (зокрема, чи скоротиться час установки сервера), чи прискориться вивід продуктів на ринок і т.д. Специфіка моделі складається в обліку потенційних ризиків і неминучої невизначеності: у рамках проведеного дослідження визначається, яка ймовірність того, що розрахована віддача виявиться недосягнутою, очікувані переваги не будуть отримані або для реалізації проекту знадобиться більше засобів, чим передбачено в затвердженому бюджеті. Таким чином, аналіз ризиків завершує аналіз TEI.

Як здійснюється аналіз? У першу чергу проводиться всебічна оцінка (due diligence), тобто разом із замовником фахівці Emerson виявляють проблемні місця, потреби ЦОД і т.д. Після цього опитуються різні групи співробітників, на роботу яких може вплинути впровадження нового рішення. Велика кількість людей передають у ЦОД інформацію й витягають неї. Це можуть бути фахівці з експлуатації, що займаються організацією ЦОД, корпоративні співробітники, для яких ЦОД надає критичні бізнес-сервіси, менеджери З-рівня, що намагаються витягти статистику про тенденції й т.д.

У кожній групі виникають свої питання щодо функціонування ЦОД: в одних стратегічні, в інших операційні. Залежно від виконуваної ролі їм потрібно зрозуміти, яку сміність буде потрібно додати в майбутньому, наскільки ефективно працює ЦОД, потрібно чи вносити зміни, як треба реагувати на ті або інші події й т.д. Інтерв'ю з ними проводяться з погляду бізнес-вигід. На підставі зібраних і узагальнених даних складається фінансова модель. При цьому як база для порівняння використовується еталонний приклад (benchmark), що був складений за результатами проекту для великого банку з декількома ЦОД.

Ми робимо аналіз TEI, тому що ринок DCIM вимагає такого обґрунтування. Ми знаємо, як важко менеджерам ЦОД показати цінність DCIM для бізнесу. DCIM-калькулятор Emerson допоможе їм представити можливі вигоди. Оскільки ми збираємо дані, які надають нам замовники, довіра до отриманих результатів дуже високо. Ми не оперуємо віртуальними цифрами, щоб зрозуміти, які будуть переваги.

DCIM на практиці

У першу чергу переваги від впровадження DCIM здатні одержати великі центри обробки даних із сотнями стійок. Однак, як показує приклад Microsoft Technology Center (MTC), де використовується DCIM-система Schneider DC Expert, ця система може виявитися корисна й у великій серверній.

У центрі представлене різне партнерське встаткування, що часто обновляється. При цьому необхідно забезпечувати рівномірне завантаження стійок (дорога електроенергія повинна витрачатися ефективно), а також документувати підключення пристроїв, оскільки схеми комутації постійно міняються. За інфраструктуру відповідає всього одна людина, тому система моніторингу інфраструктури автоматизована й ретельно продумана.

Наявність системи моніторингу дозволяє швидко ідентифікувати події й оперативно вживати заходів по усуненню несправності, які виконуються по більшій частині в

автоматичному режимі (за винятком серйозних аварій, таких як протикання води, про що оперативно повідомляються інженерні служби будинку). Наприклад, вихід з ладу циркуляційного насоса може бути компенсований включенням резервного, а поломка чиллера або недостатній рівень холоду – включенням ще одного чиллера.

Для оперативної оцінки стану інфраструктури використовуються панелі моніторингу: відповідна графіка виводиться на монітори, установлені при вході в ЦОД, і замовники можуть бачити реальні дані. Наприклад, на підставі інформації про збільшення вологості можна зробити вивід про занадто активну роботу уволожувача й необхідності коректування його налаштувань. На Рисунку 6, наприклад, видно, що система повідомляє про відмову однієї з батарей.

Для моніторингу додатків використовуються дві системи – StructureWare Data Center Expert і System Center Operations Manager, які інтегруються за допомогою Management Pack. Міжрядні кондиціонери InRow і ІБЖ Symmetra становлять основу ЦОД, тому використання Expert для моніторингу інженерної інфраструктури представляється логічним. Expert виводить звіти на панелі моніторингу й направляє повідомлення. При відсутності реакції на них (наприклад, температура продовжує рости) сервери починають автоматично відключатися, починаючи з менш важливих, – аж до припинення роботи всього ЦОД щоб уникнути більше важких наслідків. За прийняття таких мір відповідає System Center Operations Manager, він же здійснює моніторинг додатків.

Надалі планується підвищити ефективність використання електроенергії за рахунок перерозподілу віртуальних машин між шафами шляхом інтеграції StructureWare Data Center Expert з Microsoft System Center Virtual Machine Manager.

В останні кілька років системи DCIM удосконалювалися швидкими темпами, на ринку представлені рішення різного масштабу й призначення. Вони покликані надати адміністраторам повну інформацію про функціонування центра обробки даних і полегшити планування його подальшого розвитку. DCIM спрощує керування ЦОД і допомагає оптимізувати його інфраструктуру з метою підвищення ефективності використання енергії, устаткування й доступних площ. Однак на цьому шляху необхідно усунути ще цілий ряд перешкод.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування інфраструктурою ЦОД.

Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем керування інфраструктурою ЦОД.
- Досліджена система керування інфраструктурою ЦОД.
- На основі отриманих результатів досліджень створена програмна реалізація системи керування інфраструктурою ЦОД.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання керування інфраструктурою ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
2. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
3. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.

4. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». *CEUR Workshop Proceedings Volume 3156*, 2022, Pages 390-399.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings. Volume 2740*, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings Volume 2608*, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019*. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407*.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings, Vol 2588*, P. 90-106, 2019.
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings Volume 2353*, CEUR Workshop Proceedings 2019, Pages 618-629.
23. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78*.
24. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.