УДК 004

Д.Бондаренко, магістр гр. КІ-23М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОЕКТУВАННЯ ТА ПОБУДОВИ ТОПОЛОГІЇ МЕРЕЖ У ЦЕНТРАХ ОБРОБКИ ДАНИХ ТА ДАТА-ЦЕНТРАХ

У статті розроблено програмне забезпечення, яке призначено для системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах. Метою розробки є дослідження та програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах. Об'єктом дослідження є процес проектування та побудови топології мереж у центрах обробки даних та дата-центрах. Предметом дослідження є методи проектування та побудови топології мереж у центрах обробки даних та дата-центрах. Методи дослідження базуються на методах побудови топології комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.АВ процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Еволюція центрів обробки даних стала одним із найважливіших досягнень сучасної комп'ютерної техніки. Оскільки організації продовжують оцифровувати величезні обсяги даних і покладатися на них, потреба в ефективній, масштабованій і надійній мережевій архітектурі центру обробки даних стає першорядною. Ця робота заглиблюється в тонкощі архітектури мережі центрів обробки даних, вивчаючи її компоненти, принципи проектування та нові тенденції.

Центр обробки даних є технологічним центром роботи сучасного підприємства. Центр обробки даних забезпечує критично важливу IT-інфраструктуру, необхідну для надання ресурсів і послуг співробітникам, партнерам і клієнтам у всьому світі.

Малий або середній бізнес часто може створити корисний «центр обробки даних» у межах шафи чи іншої зручної кімнати з невеликими змінами, якщо такі є. Однак величезний масштаб корпоративних обчислень вимагає великого виділеного простору, ретельно спроектованого для забезпечення потреб IT-інфраструктури в просторі, живленні, охолодженні, управлінні, надійності та безпеці.

У результаті центр обробки даних є найбільшим і найдорожчим активом, яким матиме бізнес – як з точки зору капіталовкладень, так і поточних операційних витрат. Бізнес- та IT-керівники повинні приділяти пильну увагу питанням, пов'язаним з проектуванням і будівництвом центру обробки даних, щоб забезпечити відповідність кінцевого об'єкта бізнес-потребам протягом усього життєвого циклу об'єкта та мінливих умов бізнесу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

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

– Огляд існуючих систем проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

– Дослідження системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

– Програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

Об'єктом дослідження є процес проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

Предметом дослідження є методи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

Методи дослідження базуються на методах побудови топології комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розглянемо призначення та структуру ЦОД. У будь-якому центрі обробки даних є два основні аспекти: об'єкт та IT-інфраструктура, яка знаходиться в об'єкті. Ці аспекти співіснують і працюють разом, але їх можна обговорювати окремо.

Об'єкт

Об'єкт – це фізична будівля, яка використовується для центру обробки даних. Простіше кажучи, центр обробки даних – це просто великий відкритий простір, де буде розгорнута інфраструктура. Хоча майже будь-який простір має потенціал для роботи певної IT-інфраструктури, належним чином спроектований об'єкт враховує такі фактори:

– **Простір.** Повинна бути достатня площа – проста міра квадратних футів або квадратних метрів – для розміщення всієї IT-інфраструктури, яку бізнес має намір розгорнути зараз і в майбутньому. Приміщення має бути розташоване на добре продуманій ділянці з доступними податками та доступом. Простір часто поділяють для різних цілей або типів використання.

– **Потужність.** Повинна бути достатня потужність – у ватах, часто до 100 мегават – для роботи всієї IT-інфраструктури. Електропостачання має бути доступним, *чистим* , тобто без коливань і збоїв, і надійним. Необхідно включити відновлювану та додаткову/допоміжну енергію.

– **Охолодження.** Величезна кількість електроенергії, що надходить до центру обробки даних, перетворюється на обчислення, тобто роботу, і багато тепла, яке потрібно відвести від IT-інфраструктури за допомогою звичайних систем HVAC, а також інших нетрадиційних технологій охолодження .

– **Безпека.** Враховуючи цінність центру обробки даних і його критичну важливість для бізнесу, центр обробки даних повинен передбачати контрольований доступ із застосуванням різноманітних тактик, починаючи від доступу співробітників до відеоспостереження.

– **Управління.** Сучасні центри обробки даних, як правило, включають систему керування будівлею (BMS), розроблену для того, щоб допомогти IT-керівникам і бізнесменам контролювати середовище центру обробки даних у режимі реального часу, включаючи нагляд за температурою, вологістю , рівнями живлення та охолодження, а також доступом і реєстрацією безпеки.

Великим підприємствам можуть знадобитися дуже великі центри обробки даних, як-от цей центр обробки даних Google у окрузі Дуглас, штат Джорджія.

Інфраструктура

Інфраструктура являє собою широкий спектр IT-обладнання, розгорнутого на об'єкті. Це обладнання, яке запускає програми та надає послуги бізнесу та його користувачам. Типова IT-інфраструктура включає такі компоненти:

– **Сервери.** На цих комп'ютерах розміщуються корпоративні програми та виконуються обчислювальні завдання.

– **Зберігання.** Підсистеми, такі як дискові масиви, використовуються для зберігання та захисту прикладних і бізнес-даних.

– **Мережа.** Обладнання, необхідне для створення бізнес-мережі, включає комутатори, маршрутизатори, брандмауери та інші елементи кібербезпеки.

– **Кабелі та стійки.** Милі дротів з'єднують між собою IT-обладнання , а фізичні серверні стійки використовуються для організації серверів та іншого обладнання в межах приміщення.

– **Резервне живлення.** Джерело безперебійного живлення (UPS), маховик та інші системи аварійного живлення мають вирішальне значення для забезпечення впорядкованої роботи інфраструктури в разі збою основного живлення.

– **Платформи управління.** Одна або кілька платформ керування інфраструктурою центру обробки даних (DCIM) необхідні для нагляду та керування IT-інфраструктурою, яка звітує про працездатність, доступність, потужність і конфігурацію системи.

Коли компанія вирішує спроектувати та побудувати центр обробки даних, основна увага приділяється проекту та будівництву об'єкта. Але IT-лідери також повинні розглянути інфраструктуру, яка входитиме в об'єкт для перевірки проекту.

Як спроектувати центр обробки даних

Немає обов'язкових або обов'язкових стандартів для проектування або будівництва центрів обробки даних. Центр обробки даних призначений для задоволення унікальних потреб бізнесу в цілому, а не навпаки. Однак основною метою будь-якого стандарту є створення спільної платформи передового досвіду. Існує низка поточних стандартів центру обробки даних, і підприємство може включити один або кілька стандартів або частини стандартів у проект центру обробки даних. Стандарти допомагають забезпечити належну увагу таким факторам, серед іншого:

– Концептуальний проект.
– Планування та планування приміщення.
– Вимоги до конструкції будівлі.
– Питання фізичної безпеки.
– Внутрішні пристрої (механічні, електричні, сантехнічні та пожежні системи).
– Операції та робочі процеси.
– Технічне обслуговування.

Нижче наведено лише деякі з основних стандартів проектування центрів обробки даних та інфраструктури:

– **Стандарт рівня Uptime Institute.** Стандарт Uptime Institute Tier зосереджується на проектуванні, будівництві та введенні в експлуатацію центру обробки даних і використовується для визначення стійкості об'єкта відповідно до чотирьох рівнів резервування/надійності.

– **ANSI/TIA 942-B.** Цей стандарт включає планування, проектування, будівництво та введення в експлуатацію будівель, а також протипожежний захист, IT та технічне обслуговування. Він також використовує чотири рівні рейтингів надійності, які впроваджують спеціалісти, сертифіковані BICSI.

– **Серія EN 50600.** Ця серія стандартів зосереджена на розробці IT-кабелю та мереж, а також містить різні концепції резервування інфраструктури та надійності, які приблизно базуються на Tier Standard Tier Institute Uptime Institute.

– **ANSI/BICSI 002-2019.** Документ під назвою «Найкращі практики проектування та впровадження центрів обробки даних» містить обговорення систем відведення тепла та охолодження, використання технологій літій-іонних акумуляторів, планування спільного розташування та підтримку ініціатив Open Compute Project.

– **ASHRAE .** Рекомендації ASHRAE , які не стосуються IT-центрів або центрів обробки даних, стосуються проектування та реалізації систем опалення, вентиляції, кондиціонування повітря, охолодження та інших суміжних сфер.

Стандарти рівня центрів обробки даних окреслюють те, що потрібно для забезпечення надійності та продуктивності.

Крім того, існує багато різноманітних нормативних та операційних стандартів, які можна застосовувати до центрів обробки даних. Нормативні стандарти включають HIPAA, GDPR, Закон Сарбейнса-Окслі, SAS 70 Тип I або II і Закон Грамма-Ліча-Блайлі. Операційні стандарти можуть включати ISO 9000 для якості, ISO 14000 для управління навколишнім середовищем, ISO 27001 для інформаційної безпеки, стандарт безпеки даних індустрії платіжних карток для безпеки платіжних карток і EN 50600-2-6 щодо управління та операційної інформації.

Хоча нормативні стандарти та практики безпосередньо не пов’язані з дизайном центру обробки даних, дотримання цих стандартів може гарантувати, що проект центру обробки даних відповідатиме нормативним зобов’язанням для бізнесу. Інші відповідні найкращі практики включають доступність об’єктів і робочого навантаження, управління бізнесом і безперервність бізнесу .

Організація фізичного простору та центру обробки даних

За своєю суттю центр обробки даних – це ретельно підготовлений склад, призначений для розміщення та експлуатації вимогливої IT-інфраструктури. Хоча центр обробки даних корпоративного класу може бути великою та складною справою, першочерговою проблемою є просто питання площі, вираженої у квадратних футах або квадратних метрах.

Мабуть, найбільш важливою та складною проблемою простору є правильний розмір центру обробки даних для бізнесу . Центри обробки даних неймовірно дорогі: надто малі, і центр обробки даних може не відповідати поточним або майбутнім потребам бізнесу; занадто великий, і величезний капітал може бути витрачений на надання невикористаного простору. Дуже важливо створити об’єкт, який пропонує потенціал для зростання, але оптимізує використання. Вибір розміру центру обробки даних іноді вважається мистецтвом. Безліч інших факторів, які слід враховувати в просторі центру обробки даних, включає наступне:

– **Освітлення.** Більшість освітлення центрів обробки даних слабке або вимкнене без присутності людини.

– **Температура.** Потреби в охолодженні можуть підтримувати низькі температури, тому людям може знадобитися захисний одяг.

– **Шум.** Вентилятори охолодження в десятках – навіть сотнях – серверів можуть створювати какофонію, яка потребує захисту слуху.

– **Вага** Обладнання є важким, і підлога повинна бути розроблена таким чином, щоб витримувати надзвичайну вагу. Особливі міркування щодо ваги можуть знадобитися для фальшпідлоги, які використовуються для обробки потоків охолоджуючого повітря.

Крім фізичного простору, проекти центрів обробки даних повинні включати ретельний розгляд розташування обладнання та макетів, тобто місця розміщення IT-інфраструктури в об’єкті. Найпоширенішою особливістю будь-якого макета центру обробки даних є серверна стійка, яку також називають *стійкою*. Стійка – це порожня металева рама зі стандартними відстанями та варіантами кріплення, призначена для розміщення стандартизованого IT-обладнання, яке встановлюється в стійку, наприклад серверів, підсистем зберігання даних, мережевого обладнання, кабелів, допоміжних систем живлення, таких як пристрої ДБЖ, і опцій введення/виведення, таких як клавіатури та монітори для адміністративного доступу.

На цьому зображенні IT-спеціаліст встановлює та обслуговує стійкі системи великої місткості в центрі обробки даних.

Стійки також відіграють важливу роль у схемах охолодження центрів обробки даних. Стелажі механізмів зазвичай організовуються для створення гарячих і холодних проходів , які можуть підвищити ефективність охолодження, забезпечуючи введення охолодженого повітря в *холодний коридор* , яке нагрівається механізмом і подається в *гарячий коридор* , де нагріте повітря може бути ефективно видалено з кімната. Організація проходів також може сприяти введенню додаткових дверей і заходів безпеки в кінцях кожного проходу, щоб обмежити доступ людей.

Безпека центру обробки даних

Безпека центру обробки даних зазвичай включає три різні аспекти безпеки доступу, безпеки об’єктів і кібербезпеки.

Безпека доступу

Будь-яке обговорення засобів центру обробки даних повинно включати розгляд фізичної безпеки. Фізична безпека – це управління людським персоналом і захист фізичного об’єкта та його IT-інфраструктури. При належному застосуванні безпека гарантує, що лише уповноважений персонал має доступ до об’єкта та спорядження, і що всі людські дії документуються. Безпека може включати наступний комплекс заходів:

- Доступ до закладу та навколо нього (включаючи зони обладнання).
- Ключовий доступ до певних стійок і серверів.
- Журнали для доступу співробітників і відвідувачів/постачальників.
- Супровід непрацюючих.
- Відеоспостереження.
- Персонал охорони на місці.

Охорона об'єкта

Фізична безпека також поширюється на цілісність середовища центру обробки даних, включаючи температуру, вологість і умови диму/пожежі/повені. Цим аспектом захисту центру обробки даних часто керує BMS, яка відстежує умови навколишнього середовища чи надзвичайні ситуації та повідомляє керівникам будівель.

Кібербезпека

Кібербезпека зосереджується на контролі доступу до корпоративних даних і програм, розміщених в IT-інфраструктурі центру обробки даних. Кібербезпека призначена для того, щоб лише належним чином автентифіковані користувачі могли отримати доступ до даних або використовувати програми, а також щоб про будь-які порушення повідомлялося та негайно усувалося. Наприклад, фізична безпека не дозволяє людині торкатися диска в центрі обробки даних, тоді як кібербезпека запобігає цій самій людині отримати доступ до даних на диску на відстані сотень миль через мережу. Кібербезпека використовує поєднання засобів захисту від зловмисного програмного забезпечення, керування конфігурацією, виявлення/запобігання вторгненням, реєстрації активності та інших інструментів, щоб контролювати мережеву активність і виявляти потенційні загрози.

Вимоги до потужності та продуктивності центру обробки даних

Потужність – це постійний виклик для будь-якого центру обробки даних корпоративного класу. Велике об’єкт може споживати близько 100 мегават – цього достатньо для забезпечення електроенергією близько 80 000 будинків. Power представляє найбільший єдиний Орех для центру обробки даних корпоративного класу; тому оператори центрів обробки даних висувають наступні вимоги до електроенергії:

- **Ємність.** Для роботи центру обробки даних має бути достатньо електроенергії.
- **Вартість.** Енергія повинна бути якомога дешевшою.
- **Якість.** Потужність має бути електрично чистою (тобто без небажаних електричних перешкод, стрибків напруги та стрибків).
- **Надійність.** Електропостачання має бути без перебоїв, відключень або інших збоїв.

Ці проблеми дедалі частіше вирішуються за допомогою місцевих і все більш відновлюваних джерел енергії, включаючи вітрову, сонячну та локальну генерацію.

Але для того, щоб бізнес розумів проблеми з електроживленням для будь-якого центру обробки даних, важливо, щоб дизайнери центрів обробки даних і ІТ-лідери розраховували потреби в електроенергії об'єкта та його ІТ-інфраструктури. Саме цей контрольний показник дає змогу бізнесу зрозуміти приблизну вартість електроенергії та обговорити потужності з регіональними комунальними службами.

Немає єдиного способу оцінки потреби в потужності. Для об'єкта потужність є простою оцінкою потреб у освітленні та опаленні, вентиляції та кондиціонуванні. Вимоги до потужності ІТ-інфраструктури можуть бути складнішими, оскільки вимоги до потужності сервера залежать від *робочого навантаження* , тобто того, скільки роботи виконують програми, і конфігурації кожного сервера, включаючи вибір ЦП, встановленої пам'яті та інших пристроїв розширення, таких як графічні процесори.

Традиційні оцінки потужності включають підходи на основі стійки та таблички.

Підхід на основі стійки зазвичай призначає стандартизовану оцінку потужності на стійку. Наприклад, ІТ-керівник може призначити приблизно від 7 кВт до 10 кВт на стійку. Якщо центр обробки даних планує розгорнути 50 стійок, оцінка потужності є простим кратним. Подібним підходом є загальна оцінка центру обробки даних у ватах на квадратний фут. Однак, оскільки цей підхід приділяє мало уваги обладнанню, встановленому в кожній стійці, він часто є найбільш неточним засобом оцінки потужності.

Підхід, заснований на паспортній табличці, дозволяє ІТ-лідерам складати вимоги до потужності, зазначені на паспортній табличці кожного сервера чи іншого ІТ-пристрою. Це більш детальний підхід, який зазвичай дає кращі оцінки. Тим не менш, потреба в потужності, зазначена на табличці кожного пристрою, може бути завідомо неточною та не враховувати роботу, яку пристрій виконує.

Більш сучасний підхід полягає у використанні фактичних вимірювань потужності на сервер, отриманих за допомогою ІТ-пристроїв керування живленням, таких як інтелектуальні блоки розподілу електроенергії , розташовані в кожній стійці. Фактичні вимірювання можуть дати найточніші оцінки та дати операторам центрів обробки даних краще зрозуміти, як потреби в електроенергії та витрати можуть коливатися залежно від вимог до робочого навантаження.

Нарешті, енергопостачання неминуче зазнає випадкових збоїв у виробництві та розподілі, тому центри обробки даних повинні включати один або кілька варіантів резервного або резервного живлення. Може бути встановлено кілька рівнів вторинної влади, залежно від того, від яких проблем бізнес має намір захищатися.

На рівні об'єкта центр обробки даних може включати резервні генератори, що працюють на дизельному паливі або природному газі, здатні забезпечувати роботу всього об'єкта протягом тривалого часу. Резервне живлення можна доповнити місцевими відновлюваними джерелами енергії, такими як сонячні чи вітрові електростанції. На рівні ІТ-інфраструктури стійки можуть включати опції ДБЖ, які забезпечують короткочасне резервне живлення від батареї, щоб уможливити впорядковане відключення системи, коли збої в електроживленні стають неминучими.

Конструкція постійного ДБЖ з подвійним перетворенням при нормальному живленні від мережі.

Конструкція ДБЖ із подвійним перетворенням у разі збою електроживлення.

Системи охолодження ЦОД

Потужність, що надходить до центру обробки даних, перетворюється на роботу, яку виконує ІТ-інфраструктура, а також на небажаний побічний продукт: тепло. Це тепло має бути видалено з серверів і систем, а потім виведено з центру обробки даних. Отже, системи охолодження є критичною проблемою для проектувальників і операторів центрів обробки даних.

Є дві основні проблеми з охолодженням. По-перше, це кількість необхідного охолодження , яка в кінцевому підсумку визначає розмір або потужність підсистем HVAC центру обробки даних. Однак розробники повинні зробити переклад із споживаної потужності центру обробки даних у ватах (Вт) у потужність охолодження, виміряну в тоннах (т), тобто кількість теплової енергії, необхідної для розтоплення однієї тонни льоду при 32 градусах за Фаренгейтом за одну годину. . Типовий розрахунок спочатку вимагає перетворення ватів у британські теплові одиниці (BTU) на годину, які потім можна перетворити на тонни:

Вт x 3,41 = BTU/год

BTU/год / 12 000 = т

Ключовим є розуміння вимог до потужності центру обробки даних у ватах і запланованої масштабованості, тому важливо правильно підібрати розмір підсистеми охолодження будівлі. Якщо система охолодження занадто мала, центр обробки даних не зможе вмістити або масштабувати очікувану кількість IT-інфраструктури. Якщо система охолодження занадто велика, це буде дорогою та неефективною послугою для бізнесу.

Другим питанням охолодження центрів обробки даних є ефективне використання та поводження з охолодженим і нагрітим повітрям. Для звичайного людського приміщення введення охолодженого повітря з одного вентиляційного отвору та випуск нагрітого повітря з іншого викликає змішування та усереднення температури, що забезпечує достатній комфорт для людини. Але цей звичайний підхід до дому та офісу погано працює в центрах обробки даних, де стійки з обладнанням створюють надзвичайно високу температуру в концентрованих просторах. Стійки надзвичайно гарячого спорядження вимагають обережного подачі охолодженого повітря, а потім навмисного стримування та видалення нагрітого вихлопу. Дизайнери центрів обробки даних повинні уникати змішування гарячого та холодного повітря, яке забезпечує комфорт у приміщеннях з кондиціонером.

Проблеми з розподілом тепла ще більше посилюються через використання коливань густини потужності між стійками. Традиційні сервери можуть бути досить однаковими за енергоспоживанням і кінцевою щільністю потужності/охолодження. Однак передове обладнання, таке як обладнання гіперконвергентної інфраструктури, може забезпечити значно більшу щільність потужності порівняно з простором у стійкі. Це призводить до потенційних гарячих точок у просторі стійки, які розробники системи живлення та охолодження повинні враховувати та врахувати.

Розробники регулярно звертаються до обробки повітря в серверній кімнаті за допомогою схем утримання, наприклад планування гарячих/холодних коридорів. Розглянемо два ряди стелажів для обладнання, де тильні сторони звернені одна до одної (див. схему «Центр обробки даних з гарячими та холодними проходами»). Холодне повітря від системи ОВК подається в проходи перед кожним рядом стелажів, тоді як нагріте повітря збирається та виводиться із загального гарячого проходу. Для запобігання змішуванню нагрітого повітря з охолодженим додаються додаткові фізичні бар’єри. Такі схеми стримування пропонують дуже ефективне використання потужності ОВК.

У центрах обробки даних, які не використовують конструкцію гарячого/холодного проходу, блоки охолодження не завжди здатні ефективно охолоджувати обладнання.

У центрах обробки даних, сконструйованих навколо гарячих/холодних проходів, блоки охолодження можуть більш ефективно охолоджувати обладнання.

Інші підходи до охолодження включають системи кондиціонування повітря *в кінці ряду* та *у верхній частині стелажа* , які вводять охолоджене повітря в частини ряду стелажів і випускають нагріте повітря в гарячі проходи.

Деякі центри обробки даних навіть застосовують нові технології рідинного охолодження, які занурюють IT-обладнання в ванну з охолодженими електрично нейтральними рідинами, такими як мінеральні масла. Охолоджувач рідини невеликий і енергоефективний, і рідини можуть запропонувати в рази більшу ефективність теплопередачі, ніж повітряне охолодження . Однак рідинне охолодження стикається з

іншими проблемами, включаючи витоки/затоплення, корозію частин або сприйнятливість до проникнення рідини, фільтрацію рідини та чистоту та безпеку людини.

На цій діаграмі показані основні концепції кімнатних, рядних і стійкових архітектур охолодження. Сині стрілки вказують на відношення шляхів первинного охолодження до приміщення.

Ефективність і стійкість ЦОД

Сучасні занепокоєння щодо впливу на навколишнє середовище викидів вуглекислого газу від виробництва електроенергії спонукали багато організацій зробити новий акцент на ефективності та стійкості центру обробки даних.

Ефективність – це, по суті, міра виконаної роботи в порівнянні з кількістю енергії, яка використовується для виконання цієї роботи. Якщо вся ця вхідна енергія успішно перетворюється на корисну роботу, ефективність становитиме 100%. Якщо жодна з цієї вхідної енергії не призводить до успішної роботи, ККД дорівнює 0%. Компанії прагнуть підвищити ефективність до 100%, щоб кожен долар, витрачений на енергію, сприяв корисній роботі центру обробки даних.

Такі показники, як ефективність енергоспоживання (PUE), допомагають організаціям оцінювати ефективність. PUE розраховується як потужність, що надходить до центру обробки даних, поділена на потужність, що використовується в IT-інфраструктурі. Це дає простий коефіцієнт, який наближається до 1,0, коли ефективність наближається до 100%, і відповідний відсоток виражається як ефективність інфраструктури центру обробки даних. Підприємства можуть покращити коефіцієнт PUE, зменшивши кількість енергії для використання, не пов’язаного з IT, наприклад, зменшивши освітлення та охолодження в приміщеннях, не пов’язаних із IT, і запровадивши інші енергоефективні конструкції будівель.

Ефективність енергоспоживання – це показник, який використовується для оцінки ефективності центру обробки даних.

Стійкість – ще одна проблема. Виробництво електроенергії створює забруднення, яке, як вважається, спричиняє зміну клімату та погіршує здоров’я планети. Створення сталого або екологічного центру обробки даних означає прагнення до нульових викидів вуглецю для потужності, яка рухає центри обробки даних. *Чистий нуль* означає, що енергію отримують з відновлюваних джерел, які не додають в атмосферу вуглекислого газу.

У деяких випадках підприємство може наблизитися до нуля, використовуючи енергію з екологічно чистих джерел , таких як сонячні чи вітрові електростанції. В інших випадках електроенергію можна придбати у постачальників електроенергії, здатних уловлювати або відновлювати еквівалентну кількість вуглекислого газу, що виділяється під час виробництва енергії, що забезпечує нульовий чистий викид. Щоб досягти чистого нуля, підприємства повинні прийняти енергозбереження, енергоефективність – наприклад, ініціативи PUE – і поновлювані екологічно чисті джерела енергії.

Зменште споживання енергії для зберігання даних, щоб працювати в екологічно чистішому центрі обробки даних.

Інші проблеми сталого розвитку включають практику утилізації та переробки. IT-обладнання створює значні відходи у вигляді пакувальних матеріалів. Нове спорядження все частіше виготовляється з використанням біорозкладаних пакувальних матеріалів із мінімальним вмістом токсинів, які легко руйнуються у потоці відходів.

Практика утилізації застарілого та знятого з експлуатації обладнання може додати до потоку відходів метали та неорганічні – потенційно токсичні – компоненти. Багато організацій перепрофільовують старе обладнання, щоб продовжити термін служби переміщеного обладнання в інших несуттєвих ролях, або навіть дарують використане обладнання іншим підприємствам.

Найкращі практики проектування ЦОД

Не існує єдиного способу проектування центру обробки даних, і існує незліченна кількість конструкцій, які задовольняють унікальні потреби кожного бізнесу. Але такі стратегії можуть створити центр обробки даних із надзвичайною ефективністю та стійкістю:

– **Виміряйте енергоефективність.** Оператори ЦОД не можуть керувати тим, що вони не вимірюють. Використовуйте такі показники, як PUE, щоб контролювати ефективність центру обробки даних. PUE має бути безперервним вимірюванням, яке проводиться через часті проміжки часу протягом усього року, оскільки сезони та погода можуть впливати на споживання електроенергії.

– **Розгляньте креативний дизайн простору.** Замість традиційного великого відкритого простору для IT-обладнання подумайте про більш відокремлений або розділений простір центру обробки даних. Це може включати зони, які можна залишити порожніми, якщо вони непотрібні, використовувати для розміщення різних типів обладнання з подібними вимогами до живлення/охолодження або інших підходів для зменшення вимог до живлення та охолодження.

– **Перегляньте потік повітря.** Охолодження має важливе значення для безпечної роботи IT-інфраструктури, але необхідно керувати повітряним потоком і оптимізувати його. Це може включати обмеження змішування гарячого/холодного повітря, використання схем утримання гарячого/холодного коридору та навіть використання заглушок для покриття невикористаних отворів стійки, що запобігає надходженню охолодженого повітря до місць, де не охолоджується жодне обладнання.

– **Підвищити температуру.** Чим холодніше в серверній кімнаті, тим вона енергоємніша та дорожча. Замість того, щоб підтримувати серверну кімнату холодніше, оцініть ефект фактичного підвищення температури. Наприклад, замість того, щоб запускати холодний коридор при температурі від 68 до 72 градусів за Фаренгейтом, розгляньте можливість запуску холодного проходу при температурі від 78 до 80 градусів за Фаренгейтом. Більшість IT-обладнання може витримувати високу температуру таким чином, якщо обладнання працює при постійній температурі.

– **Спробуйте альтернативне охолодження.** Система HVAC може бути стандартною для центрів обробки даних, але розгляньте способи зменшити або усунути залежність від традиційного HVAC. Наприклад, центри обробки даних у прохолодніших кліматичних умовах можуть зменшити використання систем опалення, вентиляції, вентиляції та кондиціонування повітря та запровадити в приміщення холодніше зовнішнє повітря, що називається *природним охолодженням* . Подібним чином HVAC можна доповнити або замінити чиллерами з водяним охолодженням, тобто *економайзерами* , або іншими технологіями теплообміну, які споживають набагато менше енергії.

– **Покращити розподіл енергії.** Енергоефективність центрів обробки даних часто втрачається через неефективність пристроїв керування та розподілу електроенергії, таких як трансформатори обладнання, PDU та обладнання ДБЖ. Використовуйте високоефективний механізм розподілу електроенергії та мінімізуйте механізм – обидва вони призведуть до меншої кількості кроків – змін напруги та струму – і можливостей для втрати потужності.

Проблеми проектування ЦОД

Хоча не існує єдиної єдиної формули для проектування та будівництва центрів обробки даних, існують численні постійні проблеми, з якими стикаються проектувальники та оператори центрів обробки даних. Нижче наведено кілька широких міркувань і проблем.

– **Масштабованість.** Центр обробки даних – це довготривала установка, яка може працювати десятиліттями. Однак центри обробки даних, що працюють сьогодні, можуть суттєво відрізнятися від центрів обробки даних через десятиліття чи два. Розробники повинні розглянути способи обробки сьогоднішніх робочих навантажень і послуг, а також розглянути, як ці ресурси мають масштабуватися в майбутньому. Завдання полягає в тому,

щоб забезпечити простір для зростання простору, потужності та охолодження, одночасно зменшуючи витрати на таку потужність, поки вона не знадобиться.

– **Гнучкість.** Центр обробки даних чимось нагадує потужний виробничий цех: обладнання встановлюється на місце, але його неможливо перемістити та змінити, коли потреби змінюються. Нездатність перемикати передачі та перемикати проходи може перешкодити підприємствам адаптуватися та змінюватися відповідно до нових вимог бізнесу. Завдання полягає в тому, щоб задовольнити потреби в змінах без простоїв або дорогого та трудомісткого редизайну.

– **Стійкість.** Бізнес покладається на свій центр обробки даних. Якщо дата-центр не працює, бізнес не працює. Перебої в електропостачанні, збої в роботі мережі, екологічні катастрофи і навіть хакерські атаки та інші зловмисні акти можуть вивести з ладу центр обробки даних. Розробники стикаються з проблемою розуміння найпоширеніших загроз і розробки належної стійкості до цих загроз.

– **Зміна.** Нові обчислювальні технології та нові вимоги постійно розробляються та впроваджуються. Розробники центрів обробки даних повинні розглянути, як адаптувати та впроваджувати часто непередбачувані зміни без необхідності фундаментального перепроектування IT-інфраструктури для кожної зміни.

Програмне забезпечення та інструменти для керування інфраструктурою центру обробки даних

Центри обробки даних – це складні організми, які вимагають постійного моніторингу та управління як на рівні об’єкта, так і на рівні IT-інфраструктури. Оператори центрів обробки даних зазвичай використовують інструменти DCIM, щоб забезпечити перспективу роботи як об’єкта, так і інфраструктури. Набір загальних завдань керування, необхідних для роботи центру обробки даних, включає наступне:

– **Спостереження та нагляд.** Завдання спостереження включають моніторинг потужності, температури та вологості в об'єкті. Спостереження в інфраструктурі може включати доступну ємність, тобто які системи використовуються, а які вільні; працездатність програми для моніторингу належної роботи ключових робочих навантажень підприємства; і загальний час безвідмовної роботи або доступність. Завдання спостереження зазвичай пов’язані з системами сповіщень і квитків для встановлення пріоритетів і усунення проблем у міру їх виявлення.

– **Безпека.** Значні інструменти та інфраструктури розгортаються для безпеки центру обробки даних. Фізична безпека передбачає електронний доступ і все більш «розумне» відеоспостереження, таке як розпізнавання обличчя за допомогою ШІ. ШІ може допомогти визначити, чи повинен хтось бути в кімнаті з обладнанням і хто ця особа. Багато додаткових інструментів допомагають IT-адміністраторам і фахівцям із безпеки захищатися від мережевих атак, вторгнень у систему, зловмисного програмного забезпечення та неправомірних дій співробітників.

– **Підготовка та санація.** Управління центром обробки даних також включає завдання підготовки, такі як процеси аварійного відновлення та резервного копіювання, а також можливості міграції робочого навантаження для забезпечення своєчасного виконання завдань системного обслуговування. Завдання з відновлення включають регулярне обслуговування, а також періодичне оновлення системи, усунення несправностей системи та ремонт.

– **Місткість і спроможність.** Інструменти керування даними можуть контролювати поточну ємність, тобто використані та вільні ресурси, і допомагають операторам центрів обробки даних відстежувати використання, щоб планувати збільшення ємності. Вони також допомагають підтримувати регулярні вдосконалення можливостей центру обробки даних, такі як оновлення системи, оновлення технологій і впровадження нових технологій центру обробки даних.

Управління є ключовим елементом гарантії бізнес-послуг і угод про рівень обслуговування (SLA). Багато центрів обробки даних пов'язані певною формою SLA – або з внутрішніми департаментами чи відділами, або із зовнішніми діловими партнерами та клієнтами. Моніторинг і керування за допомогою DCIM та інших інструментів є важливими для гарантування дотримання SLA або виявлення порушень SLA, які можна негайно виділити та виправити. Крім того, комплексний моніторинг і управління допомагають забезпечити безперервність роботи та аварійне відновлення, що може бути життєво важливим для сучасних нормативних зобов'язань.

Центри обробки даних і хмарні обчислення

Технології хмарних обчислень змінили обличчя сучасних корпоративних обчислень. Часи, коли бізнесу необхідно було побудувати та запустити власний повноцінний центр обробки даних як важливу вартість ведення бізнесу, минули, і їх замінили сторонні послуги, які надають глобальні постачальники IaaS, PaaS і SaaS. Сьогодні робочі навантаження та служби можна запускати в загальнодоступній хмарі так само легко і часто за таку саму або меншу вартість, ніж виконання цих робочих навантажень у традиційному центрі обробки даних.

Компанія може вибрати приватну хмару в своєму центрі обробки даних. Це може допомогти привнести в IT-операції такі переваги, як хмара, наприклад гнучкість і самообслуговування. Вибір впровадження приватної хмари не змінює значним чином дизайн або робочі аспекти центру обробки даних. На практиці приватна хмара використовуватиме те саме апаратне забезпечення та інфраструктуру, що й інші робочі навантаження. Приватна хмара вмикається шляхом додавання рівня спеціалізованого програмного забезпечення або структури, наприклад OpenStack.

Вибір використання хмари може сильно вплинути на загальний розмір, обсяг і витрати, пов'язані з центром обробки даних. Деякі з найпрогресивніших «хмарних» компаній, що працюють сьогодні, можуть відмовитися від виділеного центру обробки даних на користь проектування та розгортання всіх робочих навантажень у загальнодоступній хмарі.

Однак більшість підприємств вирішують підтримувати певну кількість робочих навантажень у локальному центрі обробки даних, де бізнес безпосередньо контролює робоче навантаження та свою інфраструктуру. У цих випадках використання хмари може дозволити компанії виконувати менш критичні, експериментальні або тимчасові робочі навантаження в хмарі. Це потенційно може зменшити обсяг простору, обладнання, масштабованість і витрати, необхідні для традиційного локального центру обробки даних.

Розробка структурної схеми

Розглянемо механізми роботи TRILL і SPB. У міру того, як мережі Ethernet стають все більшими, алгоритм spanning-tree стає дедалі більшою проблемою, насамперед через те, що корисні зв'язки відключаються, а резервування втрачається. У високопродуктивній мережі, наприклад у центрі обробки даних, відключені зв'язки є витраченим ресурсом. Другорядною проблемою є те, що у випадку збою зв'язку створення нового дерева та відновлення підключення за допомогою сполучного дерева може зайняти багато секунд.

Щоб вирішити ці проблеми, зараз існують протоколи, які *дозволяють* Ethernet мати активні петлі в топології, забезпечуючи першокласне використання *всіх* каналів. Ідея полягає в тому, щоб створити таблиці пересилання в комутаторах Ethernet – або принаймні в деяких з них – які направляють кожен пакет за найкоротшим шляхом – або принаймні наближеним до найкоротшого шляху – на основі всіх доступних посилань. Це вже давно є основним продуктом у світі IP (9 алгоритмів маршрутизації та оновлення), але, безперечно, є розривом із традицією на рівні локальної мережі.

Тут є два конкуруючих протоколи: TRILL (Transparent Interconnection of Lots of Links) і SPB (Shortest-Path Bridging). TRILL задокументовано в [RP04] і RFC 6325 [https://tools.ietf.org/html/rfc6325.html] і супутніх документах, тоді як SPB стандартизовано IEEE 802.1aq [en.Wikipedia.org/wiki/IEEE_802.1aq] . Тут ми зосередимося на TRILL.

І TRILL, і SPB передбачають, що спочатку лише кілька комутаторів будуть достатньо розумними, щоб виконувати маршрутизацію за найкоротшим шляхом, так само, як колись лише кілька комутаторів реалізували алгоритм spanning-tree. Але з часом цілком імовірно, що більшість, якщо не всі комутатори Ethernet, будуть знати про найкоротший шлях. У високопродуктивних центрах обробки даних особливо ймовірно, що переадресація буде заснована на TRILL або SPB.

У TRILL комутатори Ethernet, які підтримують TRILL, відомі як Router-Bridges або RBridges (терміни RSwitches і TRILL Switches також можуть бути доречними). Між RBridges знаходяться *Legacy Ethernet* (звані «лінками» в [RP04] і RFC 6325 [https://tools.ietf.org/html/rfc6325.html] , хоча цей термін вводить в оману); Застарілі мережі Ethernet складаються з максимальної кількості підмереж хостів Ethernet і комутаторів, які не підтримують TRILL. Намір RBridges полягає в тому, щоб розділити весь Ethernet на відносно невеликі Legacy Ethernet. У кінцевому випадку, коли *всі* комутатори є RBridges, Legacy Ethernet є просто окремими хостами. На наведеній нижче діаграмі чотири RBridges ізолюють Legacy Ethernet 1, 2, 3 і 4, хоча Legacy Ethernet 5 представляє певний ступінь неефективності розділення.

Кожна успадкована мережа Ethernet обирає *один* підключений RBridge, який представлятиме її. Вище є унікальний вибір для LE1–LE4, але LE5 має прийняти рішення. Цей обраний RBridge відомий як *призначений RBridge* або DRB. Кожна успадкована мережа Ethernet будує власне охоплююче дерево, можливо (хоча і не обов’язково), яке базується на визначеному мосту RBridge.

Трафік від Legacy Ethernet назовні, як правило, пересилатиметься через призначений RBridge; підключення до інших RBridges не використовуватимуться. Ідея полягає в тому, щоб пакети від однієї застарілої мережі Ethernet до іншої доставлялися спочатку до DRB вузла джерела, а потім до DRB вузла призначення за допомогою справжньої переадресації за найкоротшим шляхом між RBridges, а звідти до вузла призначення. Звичайно, в кінцевому випадку, коли кожен комутатор є RBridge, трафік пройде найкоротший шлях від початку до кінця.

Єдиним винятком із цього правила щодо пересилання через призначений RBridge є те, що DRB може делегувати це завдання пересилання іншим RBridges для різних VLAN у межах Legacy Ethernet. Якщо це зробити, кожна VLAN завжди використовуватиме той самий RBridge для всього зовнішнього трафіку.

Друга частина процесу полягає в тому, щоб кожен з RBridges з’ясував загальну топологію; тобто кожен створює повну карту всіх RBbridges та їхніх взаємозв’язків. Це робиться за допомогою *протоколу оновлення маршрутизації стану зв’язку* , описаного в розділі 9.5 Алгоритм оновлення маршрутизації стану зв’язку . З двох основних протоколів стану зв’язку, IS-IS та OSPF, TRILL вибрав перший, оскільки його легше адаптувати до налаштувань, у яких, як тут, вузли не обов’язково мають IP-адреси. Кожен RBridges надсилає відповідні «пакети стану зв’язку», використовуючи багатоадресну розсилку та використовуючи бази даних для кожного RBridge, щоб гарантувати, що ці пакети не перенаправляються нескінченно. Ці пакети стану зв’язку можна порівняти з повідомленнями Hello spanning-tree. Щойно кожен RBridge має повну карту всіх RBridges, кожен RBridge може розрахувати оптимальний маршрут до будь-якого іншого RBridge.

Оскільки призначені RBridges бачать пакети зі своїх застарілих мереж Ethernet, вони вивчають MAC-адреси активних хостів усередині за допомогою звичайного протоколу навчання Ethernet. Потім вони діляться цими адресами з іншими RBridges, використовуючи протокол стану зв’язку IS-IS, тому інші RBridges зрештою дізнаються, як досягти більшості, якщо не всіх адрес Ethernet, присутніх у загальній мережі.

Однак для доставки до раніше невідомих пунктів призначення все ще потрібно використовувати резервне заповнення. З цією метою RBridges узгоджують між собою охоплююче дерево, що охоплює всі RBridges. Будь-який пакет із невідомим адресатом передається вздовж цього охоплюючого дерева, а потім, коли пакет досягає призначеного

мосту RBridge для застарілої мережі Ethernet, розповсюджується вздовж охоплюючого дерева цього Ethernet. Цей процес також використовується для доставки широкомовних і багатоадресних пакетів.

Коли RBridges спілкуються один з одним, вони узгоджують компактні двобайтові адреси – відомі як «ніки» – один для одного, проти стандартних шестибайтових адрес Ethernet. Це економить місце в комунікаціях RBridge-to-RBridge.

Під час проходження пакетів між RBridges додається спеціальний заголовок TRILL. Цей заголовок містить поле підрахунку переходів, інакше воно не присутнє в Ethernet, що означає, що будь-які пакети, спіймані в тимчасових циклах маршрутизації, зрештою будуть відхилені. IS-IS іноді може генерувати такі петлі маршрутизації, хоча це рідко.

Заголовок TRILL також містить псевдоніми джерела та призначення RBridges. Це означає, що фактичне пересилання пакетів між RBridges не включає MAC-адресу хоста призначення; який використовується лише після того, як пакет досягне призначеного RBridge для призначення Legacy Ethernet, після чого заголовок TRILL видаляється.

Якщо зв’язок між двома RBridges дає збій, то кінцеві точки зв’язку надсилають повідомлення про оновлення IS-IS, щоб сповістити всі інші RBridges про збій. Потім інші RBridges можуть перерахувати свої таблиці пересилання, щоб не використовувати пошкоджене посилання. Час відновлення зазвичай становить менше 0,1 секунди, що приблизно в сто разів більше, ніж час відновлення spanning-tree.

TRILL підтримує використання кількох однакових шляхів для покращення пропускної здатності між двома RBridges; *див.* 9.7 ECMP . У високопродуктивному центрі обробки даних ця функція дуже важлива.

Як і TRILL, SPB використовує IS-IS між мостами, що підтримують SPB, щоб знайти найкоротші шляхи, і інкапсулює пакети зі спеціальним заголовком, коли вони переміщуються між RBbridges. SPB не включає кількість переходів у заголовок інкапсуляції; замість цього він ретельніше контролює пересилання. SPB також використовує оригінальну MAC-адресу призначення для переадресації між RBbridge.

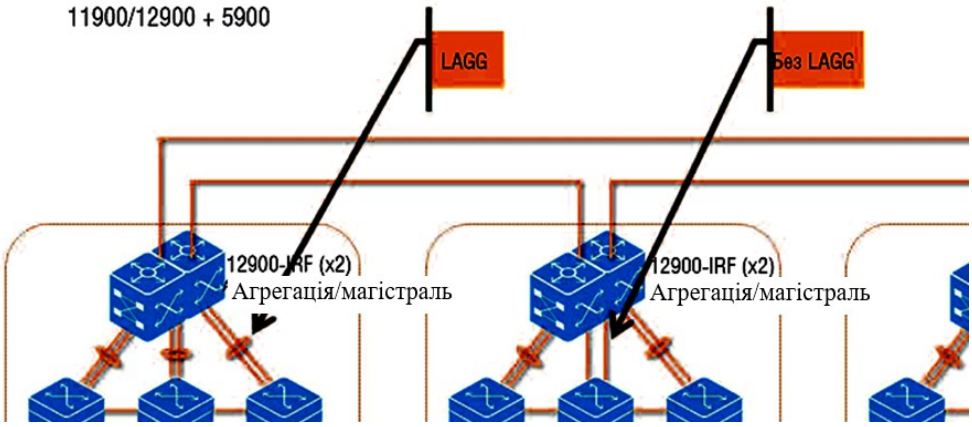

Рисунок 1 – Структурна схема системи

Якщо порівнювати TRILL і SPB з іншими технологіями, що забезпечують у ЦОД зв'язаність на другому рівні, то коротко підсумувати ці розходження можна в такий спосіб. Захист від петель забезпечують і традиційні технології, зокрема STP, але збіжність TRILL/SPB у випадку збоїв на порядок краще, ніж у традиційних мережах, а ефективність використання доступних каналів зв'язку (балансування навантаження) досягається в TRILL/SPB природно й просто (на відміну від тої ж STP). Ще раз нагадаю, оскільки це дуже важливо, що TRILL і SPB – це стандартизовані протоколи, і їхнє використання дозволяє реалізувати мультивендорні рішення.

Обидві технології мають певні розходження:

– Підтримка множинних шляхів передбачається в обох протоколах.

– МАСштабованість – TRILL підтримує 4 тис. VLAN, однак уже опублікований RFC, у якому описаний механізм підтримки 16 млн VLAN; в SPB уже підтримується до 16 млн VLAN. По розмірі мережі TRILL сьогодні масштабуються до приблизно 100 пристроїв (мається на увазі Routing Bridge), SPB потенційно може поєднувати до 1000 пристроїв.

– В TRILL свій формат кадру, а SPB використовує стандартний кадр MAC-in-MAC (стандарт IEEE 802.1ah).

– У контрольній площині обидва протоколи використовують IS-IS, однак TRILL поки не підтримує чітку прив'язку VLAN до сервісу, що утрудняє «розтягування» сервісу між пристроями.

– Обидва протоколи мають досить швидку збіжність – близько 100 мс.

– В SPB шляхи симетричні, в TRILL таке буває не завжди.

– Для багатоадресної передачі в TRILL використовуються уніфіковані дерева (не більше п'яти-шести на домен), а в SPB дерево розраховується для кожного вхідного вузла (ingress node), що ефективніше в плані розподілу трафіку, але більш затратне з погляду обчислень.

– На відміну від SPB, поточний варіант OAM в TRILL не підтримується.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

– Досліджена система проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

– На основі отриманих результатів досліджень створена програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних та дата-центрах.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання проектування та побудови топології мереж у центрах обробки даних та дата-центрах. 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., Yenchev, 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., Zaicenko 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.