**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

**Воєнна академія імені Євгенія Березняка**

Зайцев О.В., Попов М.О., Лисецький Ю.М.

# ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМНОМУ ЗВЕДЕНОМУ АНАЛІЗІ ІНФОРМАЦІЇ ВІД РІЗНОТИПНИХ ДЖЕРЕЛ

Монографія

lam&k
издательство

Київ–2024

УДК 681.3:004.07
ББК 32.85:32.988-5
Л63

*Рекомендовано до друку Вченою радою*
*Воєнної академії імені Євгенія Березняка*
*(протокол № 2 від 28.02.2024 р.)*

***Автори:***
*Зайцев О.В.* – кандидат технічних наук, доцент;
*Попов М.О.* – доктор технічних наук, професор, член-кореспондент НАН України;
*Лисецький Ю.М.* – доктор технічних наук, доцент.

***Рецензенти:***
*Бідюк П.І.* – доктор технічних наук, професор, професор кафедри математичних методів системного аналізу Навчально-наукового комплексу «Інститут прикладного системного аналізу» Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» МОН України;
*Циганок В.В.* – доктор технічних наук, старший науковий співробітник, завідувач відділу інтелектуальних технологій підтримки прийняття рішень Інституту проблем регістрації інформації НАН України;
*Мосов С.П.* – доктор військових наук, професор, професор кафедри авіації та авіаційного пошуку і рятування Інституту державного управління та наукових досліджень з цивільного захисту.

Л63 Інформаційно-комунікаційні технології в системному зведенному аналізі інформації від різнотипних джерел: монограіфія / Зайцев О.В., Попов М.О., Лисецький Ю.М. – Київ : ЛАТ&К, 2024. 224 с.

Монографія присвячена проблемі системного зведеного аналізу інформації від різнотипних джерел та ролі і місцю в цьому процесі інформаційно-комунікаційних технологій. Визначено математичний апарат зведеного аналізу інформації: теорія Байеса, теорія свідчень Демстера-Шейфера та ін. Досліджена технологія hard and soft data fusion для задач зведеного аналізу інформації різнотипних джерел. Значна увага приділена застосуванню інформаційно-комунікаційніх технологій для розв’язання задач системного зведеного аналізу інформації від різнотипних джерел. Запропоновано технология аналітичної обробки різнотипної інформації та інструментальній засіб її автоматизації. Розроблено оригінальний алгоритм аналізу та пошуку кореневої аварії в мережі, а також інструментальній засіб моніторингу та автоматизації обробки інцидентів в ІТ-інфраструктурі.

Моногрфія буде корисною для слухачів та ад'юнктів вищих військових навчальних закладів, науковців, науково-педагогічних працівників, аналітиків всіх рівнів і фахівців діяльність яких пов'язана з аналізом і аналітичною обробкою різнотипної інформації та інформаційно-телекомунікаційними технологіями.

ISBN 978-617-7699-49-0 

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AAA – Authentication, Authorisation and Accounting (процес надання доступу та контролю над ним).

AAS – Adaptive Antenna System (адаптивна антенна система).

ACL – Access Control List (набір текстових висловів, які дозволяють чи щось забороняють).

ACINT – Acoustic intelligence (акустична розвідка).

ADM – Method of Architecture Development (метод розробки архітектур).

AIE – Applied Information Economics (прикладна інформаційна економіка).

AM – Accounting Management (управління розрахунками з користувачами та постачальниками послуг).

AMQP – Advanced Message Queuing Protocol (відкритий протокол передачі повідомлень між компонентами системи).

API – Application Programming Interface (програмний інтерфейс програми, інтерфейс прикладного програмування).

APIC-EM – Cisco Application Policy Infrastructure Controller (контролер інфраструктури прикладний політики Cisco).

ARPANet – Advanced Research Projects Agency Network (комп'ютерна мережа, створена в 1969 році в США Агентством Міністерства оборони США з перспективних досліджень і стала прототипом мережі Інтернет).

ASIC – Application Specific Integrated Circuit (інтегральна схема спеціального призначення).

BFD – Bidirectional Forwarding Detection (протокол мережі для виявлення помилок з'єднання між двома маршрутизаторами).

BGP – Border Gateway Protocol (протокол динамічної маршрутизації).

BI – Business Intelligence (позначення комп'ютерних методів та інструментів для організацій, що забезпечують переведення транзакційної ділової інформації в людину-читану форму).

BLE – Bluetooth Low Energy (бездротова технологія Bluetooth із низьким енергоспоживанням).

BM – Business Management (управління бізнесом).

BPR – Business Process Reengineering (реінжиніринг бізнес-процесів).

BSC – Balanced Scorecard (система збалансованих показників).

BSS – Business Support System (система підтримки бізнесу).

BURA – Backup, Recovery and Archive (резервне копіювання, відновлення та архівування).

BYOD – Bring your own device (концепція, прийнята для позначення співробітників, які приносять свої власні обчислювальні пристрої на робоче місце для використання та підключення до корпоративної мережі).

Cadbury – Internal Control over Financial Reporting (опис фінансів і внутрішнього обліку).

CBT – VMware Changed Block Tracking (технологія, яка дозволяє стороннім продуктам для резервного копіювання повернути список блоків, що змінилися з моменту останньої копії).

CCMP – Cloud Collaboration Management Portal (веб-портал для забезпечення керування хмарними взаємодіями).

CDP – Continuous Data Protection (технології безперервного захисту даних).

CEM – Customer Experience Management (сприйняття послуги користувачем).

CERT – Computer Emergency Response Team (національний центр протидії кіберзагроз).

CIR – Committed Information Rate (гарантована смуга пропускання).

CiscoWorks LMS – CiscoWorks LAN Management Solution (сімейство програмних продуктів для спрощення налаштування, моніторингу і діагностики мережевий інфраструктури).

CM – Collection Management (управління збором).

COM – Configuration Management (управління конфігурацією мережі).

CMX – Cisco Connected Mobile Experiences (технологія Cisco для аналізу бездротових мереж , що дозволяє будувати звіти).

CoAP – ConstrainedApplication Protocol (широко використовуваний протокол для взаємодії між IoT-пристроями або IoT-пристроями та зовнішнім середовищем).

COBIT – Control Objectives for Information and Related Technology (Контрольні Об'єкти для Інформаційної й суміжної Технологій).

COMINT – Communications intelligence (розвідка комунікацій).

COO – Concept of Operations (концепція використання системи).

COSO – Committee of Sponsoring Organizations (комітет спонсорських організацій).

CPE – Customer Premises Equipment (обладнання у приміщенні клієнта).

CSIRT – Computer Security Incident Response Team (комп'ютерна група реагування на надзвичайні ситуації).

CTM – Cisco Transport Manager (система керування оптичними мережами).

CWMP – CPE WAN Management Protocol (протокол, призначений для дистанційного керування абонентським обладнанням через глобальну мережу).

DaaS – Desktop-as-a-Service (робочий стіл як послуга).

DAF – Distributed Access Fabric («тканина» розподіленого доступу, технологія Cisco).

DARE – Dynamic Reconfiguration (динамічна реконфігурація ресурсів сервера).

DAS – Direct-Attached Storage (система зберігання даних із прямим підключенням).

DBMS – Database Management System (система управління базами даних).

DCE – Data Communication Equipment (обладнання оператора зв'язку).

DDoS – Distributed Denial of Service (атаки, спрямовані на відмову в обслуговуванні).

DHCP – Dynamic Host Configuration Protocol (протокол, що відповідає за динамічне налаштування вузла мережі з використанням моделі OSI ).

DMT – Discrete Multitone Modulation (дискретна багатотональна модуляція).

DNA – Digital Network Architecture (відкрита масштабована програмна архітектура, що дозволяє покращити роботу корпоративної мережі).

DNS – Domain Name System (комп'ютерна розподілена система для отримання інформації про домени).

DTE – Data Terminal Equipment (обладнання, що перетворює користувальницьку інформацію дані для передачі по лінії зв'язку і здійснює зворотне перетворення).

DTLS – Datagram Transport Layer Security (протокол датаграм безпеки транспортного рівня).

DWDM – Dense Wave Division Multiplexing (технології передачі та ущільнення оптичних каналів).

EAI – Enterprise Application Integration (інтеграційна шина додатків).

EC-GSM – Extended Coverage GSM (система стільникового зв'язку для Інтернету речей, з великим радіусом дії та малим енергоспоживанням).

EDB – Enterprise Data Bus (корпоративна шина даних).

EDR – Enterprise Data Replication (реплікація корпоративних даних).

EE – Information Economics (інформаційна економіка).

EID – Electronic Identification (електронна ідентифікація).

EIGRP – Enhanced Interior Gateway Routing Protocol (удосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco).

EII – *Enterprise Information Integration* (інтеграція корпоративної інформації).

ELINT – Electronic intelligence (електронна розвідка)

EMS – Element Management System (система керування елементами мережі).

EPP/EDR – Endpoint Protection Point/Endpoint Detection&Response (платформа захисту кінцевих точок/захист кінцевих точок від складних загроз).

ERP – Enterprise Resource Platform (управління ресурсами підприємства).

ESB – Enterprise Service Bus (сервісна шина підприємства).

ESX – Elastic Sky X Integrated (ПЗ для віртуалізації рівня підприємства, запропоноване VMware як компонент VMware vSphere).

ETL – Extract, Transformation, Loading (витяг, перетворення, завантаження).

eTOM – enhanced Telecommunications Operations Map (розширена карта процесів телекомунікаційного оператора).

ETSI – European Telecommunications Standards Institute (Європейський інститут телекомунікаційних стандартів – некомерційна організація зі стандартизації телекомунікаційної промисловості в Європі).

EV-DO – Evolution-Data Only, Evolution-Data Optimized (технологія передачі даних, що використовується в мережах стільникового зв'язку стандарту CDMA).

FCAPS – Fault, Configuration, Accounting, Performance & Security (управління відмовами, конфігураціями, обліком, продуктивністю, безпекою).

FCoE – Fibre Channel over Ethernet (протокол, який переносить фрейми Fibre Channel через Ethernet, інкапсулюючи кадри Fibre Channel в Jumbo-кадри Ethernet-а).

FFT – Fast Fourier Transformation (швидке перетворення Фур'є).

FHRP – First Hop Redundancy Protocol (родина протоколів, призначених для створення надмірності шлюзу за умовчанням).

FIB – Forwarding Information Base (таблиця для швидкого пересилання пакетів).

FM – Fault Management (управління усуненням відмов).

FMS – Fault Management System (система керування усуненням відмов).

GoCo – Guidance on Control (посібник з контролю й призначена для внутрішнього аудита).

GRE – Generic Routing Encapsulation (протокол тунелювання мережевих пакетів, розроблений компанією Cisco).

GRT – Instant Granular Recovery Technology (загальна інкапсуляція маршрутів).

GTP – GPRS Tunneling Protocol (група комунікаційних протоколів з урахуванням IP).

HA – High Availability (режим високої доступності).

HCI – Hyper-Converged Infrastructure (гіперконвергентна інфраструктура).

HDFS – Hadoop Distributed File System (розподілена кластерна система).

HDPS – Hitachi Data Protection Suite (засоби реплікації, відновлення після збоїв та резервних копій для хмарних та локальних середовищ).

HSDPA – High-Speed Downlink Packet Access (швидка пакетна передача даних від базової станції до мобільного телефону).

HSUPA – High Speed Uplink Packet Access (швидка пакетна передача даних від мобільного телефону до базової станції).

HTTP – HyperText Transfer Protocol (протокол передачі гіпертексту).

HUMINT – Human intelligence (агентурна розвідка).

IA – Impact Analysis (аналіз впливу змін).

IaaS – Infrastructure-as-a-Service (інфраструктура як послуга ).

ICMP – Internet Control Message Protocol (протокол міжмережевих керуючих повідомлень).

IEEE – Institute of Electrical and Electronics Engineers (Інститут інженерів електротехніки і електроніки).

iFFT – Inverse Fast Fourier Transformation (зворотне перетворення Фур'є).

IGMP – Internet Group Management Protocol (протокол управління групами інтернету).

IID – Iterative and Incremental Development (модель ітеративної та інкрементальної розробки).

ILM – Information Lifecycle Management (концепція управління життєвим циклом інформації).

IMINT – Image intelligence (видова розвідка).

IMS – Inventory Management System (інформаційна модель ресурсів мережі).

INTREP – Intelligence Report (розвідувальні повідомлення).

INTSUM – Intelligence Summaries (короткі розвідувальні звіти).

IoT – Internet of Things (Інтернет речей).

IP/MPLS – Internet Protocol/Multiprotocol Label Swtiching (комутація по міжмережевому протоколу/багатопротокольна комутація по міткам).

IPCC – Internet Protocol Contact Center (контакт-центр, робота якого базується на міжмережевому протоколі).

IPinIP – IP in IP (протокол IP-тунелювання, який інкапсулює один IP-пакет в інший IP-пакет).

IRDA – InfraRed Data Association (інфрачервоний порт).

ISO – International Standardization Organization (Міжнародна організація по стандартизації).

ITIL – Information Technology Infrastructure Library (саме поширене в світі керівництво по управлінню IT-послугами).

ITU – International Telecommunication Union (Міжнародний спілка електрозв'язку).

ITU-T – International Telecommunication Union, Telecommunication sector (сектор стандартизації Міжнародного спілки електрозв'язку).

IVR – Interactive Voice Response (інтерактивне голосове меню).

iWAN – Intelligent Wide Area Network (рішення компанії Cisco для програмно-обумовленою глобальною мережі).

JISR – Joint Intelligence, Surveillance and Reconnaissance (Об’єднані Розвідка, Спостереження й Тактична розвідка).

KVM – Kernel-based Virtual Machine (програмне рішення, що забезпечує віртуалізацію серед Linux на платформі x86).

L2TP – Layer 2 Tunneling Protocol (протокол тунелювання другого рівня).

LAN – Local Area Network (локальна мережа).

LCA – Life Cycle Architecture (архітектура життєвого циклу).

LCO – Life Cycle Objectives (цілі і зміст життєвого циклу).

LDP – Label Distribution Protocol (протокол розподілу міток).

LFIB – Label Forwarding Information Base (база міток, до якої звертається мережевий процесор).

LISP – Locator/Identifier Separation Protocol (протокол поділу локатора/ідентифікатора).

LLD – Low Level Design (базовий опис принципів функціонування розгорнутої мережі).

LoRa – Long Range Radio (протокол глобальної мережі з низьким енергоспоживанням).

LoRaWAN – Low Power Wide Area Network (широкополосний мережевий протокол малої потужності, призначений для бездротового підключення «речей», до регіональних, національних, глобальних мереж).

LoWPAN – Low power Wireless Personal Area Networks (бездротові мережі з обмеженими енергоресурсами).

LPWAN – Low-power Wide-area Network (енергоефективна мережа далекого радіусу дії).

IRM – Intelligence Requirements Management (управління вимогами до розвідки).

LSP – Label Switched Path (шлях комутації міток).

M2M – machine-to-machine (технології міжмашинної взаємодії).

MAN – Metropolitan Area Network (міська обчислювальна мережа).

MASINT– Measurement and signature intelligence (параметрична та сигнатурна розвідка).

MDS – Metadata Server (сервер метаданих).

MIMO – Multiple Input Multiple Output (множинні входи, множинні виходи).

MIR – Maximum Information Rate (максимальна смуга пропускання).

MOF – Microsoft Operations Framework (серія посібників від Microsoft, спрямованих на допомогу IT-фахівцям у розробці та впровадженні надійних та економічних IT-послуг).

MPLS – Multiprotocol Label Switching (багатопротокольна комутація за мітками).

MQTT – Message Queuing Telemetry Transport (спрощений мережевий протокол, що працює поверх TCP/IP, орієнтований обмінюватися повідомленнями між пристроями за принципом видавець-передплатник).

MSA – Microsoft System Architecture (посібник Microsoft з проектування архітектури системних додатків).

NAI – Named Area of Interest (найменованих зон інтересу розвідки).

NAS – Network Attached Storage (сервер для зберігання даних на файловому рівні).

NB-CIoT – Narrow Band Cellular IoT (стандарт стільникового зв'язку для пристроїв телеметрії з низькими обсягами обміну даними).

NB- IoT – Narrow Band Internet of Things (стандарт стільникового зв'язку для пристроїв телеметрії з низьким обсягом обміну даними).

NBMA – None-Broadcast Multiple Access (мережа, у якій може бути велика кількість пристроїв, але відсутня можливість відправки широкомовної розсилки, яку отримають всі пристрої).

NE – Network Element (мережевий елемент).

NETCONF – Network Configuration Protocol (мережевий протокол конфігурації).

NFV – Network Functions Virtualisation (віртуалізація мережевих функцій).

NGOSS – New Generation Operations Systems and Software (концепція телекомунікаційної галузевої організації TM Forum, що описує підхід до розробки, впровадження та експлуатації прикладного програмного забезпечення для підприємств електрозв'язку).

NGN – Next Generation Networks (мережі наступного покоління).

NIIA – Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (архітектура взаємодії розвідки, спостереження і тактичної розвідки НАТО).

NIP – Network Implementation Plan (описує конфігураційні установки обладнання, описаного в LLD).

NLOS – Non-Line of Sight (неповна видимість).

NM – Network Management (управління мережею).

NMS – Network Management System (система управління мережею).

NRFU – Network Ready For Use (методика тестових робіт, тестування вузла та мережі загалом).

NSFNet – National Science Foundation Network (комп'ютерна мережа Національного фонду науки США, утворена в 1984 році і служила каркасом Інтернету на початку 1990-х рр.).

OADM – Optical Add Drop Multiplexer (оптичний мультиплексор введення/виводу).

OFDM – Orthogonal Frequency-Division Multiplexing (мультиплексування з ортогональним частотним поділом каналів).

OFDMA – Orthogonal Frequency-Division Multiple Access (розрахований на багато користувачів варіант OFDM-технології).

OMA-DM – Open Mobile Alliance (OMA) Device Management (DM) (протокол управління пристроями , визначений робочої групою Open Mobile Alliance Device Management).

ONF – Open Network Foundation (ініціатива корпорації Intel зі створення уніфікованої відкритої архітектури для складних високопродуктивних обчислювальних систем та дата-центрів).

ONE – Open Network Environment (відкрита мережева середа).

OSI – Open System Interconnection (базова еталонна модель взаємодії відкритих систем).

OSINT – Open source intelligence (розвідка з відкритих джерел).

OSPF – Open Shortest Path First (протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology) і використовує для знаходження найкоротшого шляху алгоритм Дейкстри).

OSS – Operation Support System (система операційної підтримкм)

OVSDB – Open vSwitch Database Management Protocol (протокол управління базами даних).

PaaS – Platform-as-a-Service (платформа як послуга).

PDoS – Permanent Denial of Service (неможливість використання пристрою).

PIR – Piority Intelligence Requirements (вигляді першочергових вимог до розвідки).

PKI – Public Key Infrastructure (інфраструктура відкритих ключів).

PM – Performance Management (контроль продуктивності мережі).

PMI – Project Management Institute (Інститут управління проектами).

PMS – Performance Management System (система керування продуктивністю).

QoS – Quality of Service (технологія надання різним класам трафіку різних пріоритетів в обслуговуванні).

OSI – Open Systems Interconnection (взаємозв'язок відкритих систем).

RAID – Redundant Array of Independent Disks (технологія віртуалізації даних для об'єднання кількох фізичних дискових пристроїв у логічний модуль).

RCA – Root Cause Analysis (аналіз першопричини проблеми).

RCT – Microsoft Resilient Change Tracking (технологія Microsoft, яка використовується для резервного копіювання віртуальних машин).

REST – Representational State Transfer (архітектурний стиль взаємодії компонентів розподіленої програми у мережі).

RFID – Radio Frequency Identification (спосіб автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в так званих транспондерах, RFID-мітках).

RHHI – Red Hat Hyperconverged Infrastructure (інтегрована платформа для обчислень та зберігання даних від компанії Red Hat).

RHVH – Red Hat Virtualization Host (спеціально розроблена ОС на базі Red Hat Enterprise Linux).

ROBO – Remote Office/Branch Office (видалені офіси та/або філії).

RSVP – Resource ReSerVation Protocol (протокол резервування мережевих ресурсів).

SaaS – Software as a Servise (програмне забезпечення як послуга).

SAC – Systems Auditability and Control (Система Аудитоспособности й Контролю).

SAN – Storage Area Network (мережа зберігання даних).

SASs – Statement's on Auditing Standards (Звід Стандартів Аудита).

SATA – Serial Advanced Technology Attachment (послідовний інтерфейс обміну даними із накопичувачами інформації).

SD-Access – Software-Defined Access (реалізація компанією Cisco концепції мережевої фабрики для кампусної мережі з централізованими

засобами управління, автоматизації та оркестрації, а також моніторингу та аналітики).

SDH – Synchronous Digital Hierarchy (система передачі даних, заснована на синхронізації за часом передавального та приймаючого пристрою).

SDI – Software-Defined Infrastructure (програмно-визначена інфраструктура).

SDN – Software-Defined Networking (програмно-визначувана мережу).

SDS – Software-Defined Storage (програмно-визначуване сховище даних).

SELinux – Security-Enhanced Linux (реалізація системи примусового контролю доступу, яка може працювати паралельно із класичною виборчою системою контролю доступу).

SGT – Security Group Tag (мітки безпеки).

SIGINT – Signals Intelligence (радіорозвідка).

SIEM – Security information and event management (об'єднання двох термінів, що позначають область застосування програмного забезпечення: SIM, Security information management; управління інформацією про безпеку, та SEM, Security event management – керування подіями безпеки).

SIMO – Single Input Multiple Output (антена технологія для бездротової передачі даних, коли приймач використовує кілька антен).

SIP – Session Initiation Protocol (протокол передачі даних, що описує спосіб встановлення та завершення користувальницького Інтернет-сеансу, що включає обмін мультимедійним вмістом).

SLA – Service Level Agreement (угода про рівень обслуговування).

SM – Security Management (забезпечення безпеки роботи мережі).

SNA – Shared Nothing Architecture (архітектура розподілених обчислень).

SNIA – Storage Networking Industry Association (Промислова асоціація мереж зберігання даних).

SNMP – Simple Network Management Protocol (протокол, який використовується для керування мережевими пристроями).

SOA – Service Oriented Architecture (сервісно-орієнтована архітектура).

SOFDM – Scalable Orthogonal Frequency-Division Multiplexing (масштабоване мультиплексування з ортогональним частотним поділом каналів).

SOFDMA – Scalable Orthogonal Frequency-Division Multiplexing Access (масштабований OFDM-доступ).

SSID – Service Set Identifier (символьна назва бездротової точки доступу Wi-Fi, що служить для ідентифікації її серед інших точок).

SSL – Secure Sockets Layer (шар захищених сокетів, криптографічний протокол, який має на увазі більш безпечний зв'язок).

STAR – Surveillance, Target Acquisition, Reconnaissance (співставлення, порівняння з даними з інших джерел, оцінювання джерел на надійність).

STP – Spanning Tree Protocol (канальний протокол).

SUPINTREP – Supplementary Intelligence Reports (додаткова доповідь з розвідки).

sVirt – Secure Virtualization (безпечна віртуалізація).

TCP – Transmission Control Protocol (один із основних протоколів передачі Інтернету, призначений керувати передачею даних).

TCPED – Task, Collect, Pprocess, Exploit, Disseminate (вимоги, збір, обробка, використання, поширення).

TCP/IP – Transmission Control Protocol/Internet Protocol (мережевая модель передачі, представлених у цифровому вигляді).

TLS – Transport Layer Security (протокол захисту транспортного рівня).

DTLS – Datagram Transport Layer Security (протокол датаграм безпеки транспортного рівня).

TMN – Telecommunications Managment Network (система управління мережами оператора зв'язку).

TNA – Technology Neutral Architecture (набір рішень щодо інтеграції та впровадження мережевих рішень).

TOM – Telecommunications Operations MAP (типова структура бізнес-процесів з управління надання послуг).

UCS – Cisco Unified Computing System (система уніфікованих обчислень від Cisco).

UDP – User Datagram Protocol (протокол користувальницьких датаграм).

UMTS – Universal Mobile Telecommunications System (технологія стільникового зв'язку, розроблена ETSI для впровадження 3G у Європі).

VADP – Vmware vStorage API for Data Protection (розширена підтримка резервного копіювання віртуальних машин на хостах VMware ESX).

VAS – Value Added Services (послуги, які приносять додатковий дохід).

VLAN – Virtual Local Area Network (віртуальна локальна мережу).

VM – Virtual Machine (віртуальна машина).

VMS – Virtual Managed Services (віртуальні керовані послуги).

VPN – Virtual Private Network (віртуальна приватна мережа).

VRF – Virtual Routing and Forwarding (технологія для реалізації на базі одного фізичного маршрутизатора кількох віртуальних).

VSS – Virtual Switching System (технологія віртуалізації комутаторів від компанії Cisco).

VXLAN – Virtual eXtensible Local Area Network (технологія мережної віртуалізації, створена для вирішення проблем масштабованості у великих системах хмарних обчислень).

WAF – Web Application Firewall (сукупність моніторів та фільтрів, призначених для виявлення та блокування мережевих атак на веб-додаток).

WAN – Wide Area Network (глобальна обчислювальна мережа).

WDM – Wavelength Division Multiplexing (мультиплексування з розподілом по довжині хвилі).

Wi-Fi – Wireless Fidelity (технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11).

WiMAX – Worldwide Interoperability for Microwave Access (одна з технологій бездротового широкосмугового доступу до Інтернету).

WLAN – Wireless Local Area Network (локальна бездротова мережа).

WLC – Wireless LAN C ontroller (контролер локальної бездротової мережі).

WMAN – Wireless Metropolitan Area Network (бездротова мережа масштабу міста).

WORM – Write Once Read Many (носії інформації, що допускають одноразовий запис та багаторазове читання).

WPAN – Wireless Personal Area Network (персональна бездротова мережа).

WSSRA – Windows Server System Reference Architecture (посібник компанії Microsoft для побудови високодоступної, безпечної, масштабованої, керованої та надійної інфраструктури підприємства).

WSUS – Windows Server Update Services (сервіс оновлень операційних систем та продуктів Microsoft).

WWAN – Wireless Wide Area Network (глобальна бездротова мережа).

WWW – World Wide Web (система, що надає доступ до пов'язаних документів на різних комп'ютерах, підключених до Інтернету).

XMPP – eXtensible Messaging and Presence Protocol (протокол обміну повідомленнями та інформацією про присутність).

ZTP – Zero Touch Provisioning (технологія спрощення розгортання нових точок).

БД – база даних.

БпЛА – Безпілотний Літальний Апарат.

БС – базова станція.

ВМ – віртуальна машина.

ВОЛЗ – волоконно-оптичні лінії зв'язку.

ВР – вимоги до розвідки.

ВЦ – обчислювальний центр.

ДМЗ – демілітаризована зона локальної мережі.

ДЦ – диспетчерський центр.

ЗМІ – засоби масової інформації.

ІКС – інформаційно-комунікаційних систем.

ІР – інформаційні ресурси.

ІТ – інформаційні технології.

КІС – корпоративна інформаційна система.

КУ – клієнтський пристрій.

МСЕ – міжмережеві екрани.

ОІ – об’єкти інтересу.

ОІ – об’єктивна інформація.

ОС – операційна система.

ПЗ – програмне забезпечення.

СІ – суб’єктивна інформація

СКС – структурована кабельна система.

СРК – система резервного копіювання.

СУ – система управління.
СУБД - система управління базою даних.
СЗД – система зберігання даних.
ТДШ – теорія Демпстера-Шейфера.
ТДС – теорія Дезерта-Смарандаке.
ТЗ – технічне завдання.
ТСДШ – теорія свідчень Демпстера-Шейфера.
ТфЗК – телефонна мережа загального користування.
УАТС – установча автоматична телефонна станція.
УЗ – управління збором.
ФАР – фазована антенна решітка.
ЦОД – центр обробки даних.
ШБД – бездротовий широкосмуговий доступ.
ШІ – штучний інтелект.

# ВСТУП

Законодавча база України визначає сфери діяльності державних органів України, що дозволяє визначити перелік об'єктів і процесів, які є предметом постійного або ситуативного інтересу та вивчення і у сукупності складають інформаційне поле фахової діяльності. Звичайно система захисту об'єкта інтересу застосовує всі можливості закрити свої відомості від інформаційного розкриття, задіюючи для цього доступні йому засоби та заходи (маскування, завади, різноманітні хитрощі тощо).

Щоб подолати такий захист і отримати необхідні відомості, державні органи залучають для виконання поставлених завдань різні засоби спостереження. Безумовно, вибір виду і конкретного типу засобу визначається характером завдання, властивостями об'єкта вивчення, рівнем його захисту тощо. Однак повсякденна практика свідчить, що дуже часто одне джерело не здатне зняти невизначеність ситуації з об'єктом вивчення та навколо нього. У подібних випадках для роботи по об'єкту рекомендується застосовувати разом кілька різних джерел.

Необхідно відзначити, що на даний час відомі певні підходи та методи щодо комбінування доцільних наборів засобів в залежності від завдання, а для проведення необхідних розрахунків існують спеціальні комп'ютерні програми. У такому наборі кожен засіб спостереження (джерело даних), в залежності від його тактико-технічних характеристик (у випадку технічного засобу) або знань і досвіду (якщо завдання вирішує людина) надає (формує) свій унікальний інформаційний портрет об'єкта інтересу, причому портрети відрізняються один від одного точністю, детальністю, повнотою і т. д.

Затребуваний рівень вивчення об'єкта і, при необхідності, підготовка різних сценаріїв розвитку обстановки або певних процесів досягаються шляхом аналізу всій сукупності інформаційних портретів об'єкта, отриманих від задіяних джерел. Такий аналіз потребує системного підходу і залучення відповідного математичного апарату.

Вище наведене дозволяє стверджувати, що методологічна основа системного зведеного аналізу інформації від різнотипних джерел має базуватися на математичному інструментарію теорії свідчень Демпстера-Шейфера (ТСДШ). Перетворення первинних даних і робота з гіпотезами за допомогою методів ТСДШ надають всі можливості забезпечити споживача обґрунтованими матеріалами для прийняття рішень.

Однак для впровадження в практику повсякденної діяльності державних органів, а також інших силових відомств нової методологічної схеми системного зведеного аналізу інформації від

різнотипних джерел необхідно вирішити цілу низку наукових та науково-технічних питань. Тому в монографії розлядаються питання формування і дослідження гіпотез на базі soft data & hard data, а також правила для зведеного аналізу даних. Запропоновані архітектура та технології забезпечення системного зведеного аналізу інформації. Розглянуто питання отримання оцінок ефективності застосування системного зведеного аналізу інформації від різнотипних джерел при вирішенні фахових завдань.

В роботі ретельно досліджені інформаційно-коммунікаційні технології зберігання та управління даними, передачі даних, віртуалізації, хмарні, Інтернету речей, а також системи підтримки операційних процесів та моніторингу.

Запропоновано технологія аналітичної обробки різнотипної інформації та інструментальний засіб її автоматизації, який дає можливість значно збільшити обсяг оброблюваної інформації, ефективність аналізу, що покращить якість аналітичної обробки та як наслідок підвищить достовірність її результатів.

Розроблено оригінальний алгоритм аналізу та пошуку кореневої аварії для підвищення ефективності діагностики мережі. А також інструментальній засіб моніторингу та автоматизації обробки інциндентів в ІТ-інфраструктурі, який дозволяє значно прискорити пошук кореневої аварії за допомогою розробленого алгоритму та суттєво підвищити ефективність роботи системи моніторингу.

Таким чином в монографії послідовно викладені теоретичні і практичні питання застосування інформаційно-телекомунікаційних технологій для розв’язання задач системного зведеного аналізу інформації від різнотипних джерел на основі сучасного математичного апарату.

Автори висловлюють подяку рецензентам: докторам наук Бідюку П.І., Циганку В.В., Мосову С.П. за зауваження та рекомендації; кандидату наук Старовойтенку О.О. за допомогу в підготовці монографії до друку та оформленні графічного матеріалу.

# РОЗДІЛ 1. СИСТЕМНИЙ ЗВЕДЕНИЙ АНАЛІЗ ІНФОРМАЦІЇ ВІД РІЗНОТИПНИХ ДЖЕРЕЛ ЯК СИСТЕМА ТА ТЕХНОЛОГІЯ

## 1.1. Основні терміни та визначення в системному зведеному аналізі інформації від різнотипних джерел

*Процеси об'єднаної розвідки за стандартами НАТО.* Одним з основних завдань воєнної політики нашої держави на даний час є реформування Збройних Сил України з метою досягнення оперативної і технічної сумісності з об'єднаними збройними силами НАТО, запровадження прийнятих у них процедур (стандартів) щодо діяльності і розподілу функцій та основних завдань між органами управління розвідки різних рівнів [1,2]. Шляхи її реалізації викладені в Державній програмі розвитку Збройних Сил України. Згідно з вимогами Програми стоїть завдання щодо розробки керівних документів JP-2.0 «Об'єднана розвідка» та JP-2.1 «Процедури розвідки» на основі Об'єднаної спільної доктрини з питань розвідки AJP-2.0 та аналогічних стандартів країн Альянсу.

Підходи до розроблення таких документів мають базуватися на процесах організації та ведення розвідки в умовах, де можуть виникнути конфлікти між державами, а операції будуть проводитись нетрадиційними прийомами та методами за умов поліпшеного технічного забезпечення.

*Об'єднана розвідка* – відповідна організація роботи органу розвідки, штабу та невоєнних організацій для підготовки і ведення операції із застосуванням сил і засобів розвідки, в якій беруть участь представники щонайменше двох видів збройних сил однієї або декількох країн-членів НАТО під час створення об'єднаного угруповання військ (сил).

В основних документах, які застосовують країни-члени НАТО, основним завданням об'єднаної розвідки є надання інформації та оцінок в інтересах забезпечення успішного проведення операції.

Реалізація цього завдання досягається шляхом *виконання визначених обов'язків*, якими керуються основні та допоміжні підрозділи: інформувати командира; описувати оперативну обстановку; розробляти, визначати та розподіляти завдання; забезпечувати планування та проведення операції; не допускати введення в оману своїх сил та протидіяти неочікуваним крокам противника; підтримувати зусилля своїх сил із введенням противника в оману; оцінювати ефективність операцій.

У вимогах до сучасного оперативного (стратегічного) середовища діяльність розвідки залежить від низки факторів, які будуть впливати на способи їхніх дій. Командири мають враховувати ці фактори, створюючи комплексну систему розвідки, і акцентувати увагу підлеглого особового складу на цей вплив.

Можна виділити, щонайменше, три головні напрями впливу:

- *складність операцій* – впливатиме на способи дій розвідки, тому що в сучасній оперативній обстановці природа агресора може суттєво відрізнятися. Противник може не мати постійної структури, матеріальних військових ресурсів або взагалі діяти тільки в кіберпросторі. У такому разі способи ведення розвідки потрібно змінювати у напрямі забезпечення більшої доступності до даних, оволодіння новітніми способами добування інформації, ефективного використання своїх професійних навичок;
- *перенасиченість інформацією* – великий обсяг інформації, що циркулює в сучасному інформаційному просторі, обмежує можливість використання наявних ресурсів для своєчасного фокусування їх у відповідних галузях. Тому здатність розвідувального співтовариства до пошуку й швидкого використання відповідної інформації є критично важливою і потребує комплексного підходу, який має бути ефективним і динамічно адаптивним. Командирам усіх рівнів потрібно бути впевненими, що вони мають відповідні структури (підрозділи), які відповідають таким вимогам, щоб пом'якшити (зменшити) інформаційну насиченість;
- *нівелювання традиційних меж* – у сучасних операціях традиційні межі між рівнями ведення бойових дій (стратегічним, оперативним і тактичним) мають все менше значення по відношенню до розвідки. Розширення можливостей засобів зв'язку (комунікацій) дало змогу командирам тактичного рівня миттєвого доступу до стратегічної розвідувальної інформації, тоді як від тактичної розвідки іноді залежить вирішення стратегічних завдань.

Базовими термінами розвідки у країнах-членах НАТО є «розвідувальні дані». Це продукт цілеспрямованого збору та обробки інформації (відомостей) про оперативну обстановку, можливості та наміри противника з метою виявлення загроз, який надається посадовим особам, які приймають рішення.

Складність сучасних операцій вимагає застосування всіх видів розвідки, використання широкого діапазону засобів і способів добування розвідувальної інформації, глибокого розуміння оперативної обстановки. Це пов'язано з обробкою геопросторових даних, їх сутністю та логічною побудовою, подальшою обробкою інформації та доведенням до споживачів. Тому нагальною є потреба в комплексній розвідці, яка полягає у використанні широкого спектра джерел добування розвідувальної інформації на основі всебічного розуміння оперативної (стратегічної) обстановки.

*Основними вимогами* до розвідки в умовах проведення сучасних операцій є: доступність; обмін; швидкість реакції; гнучкість; оперативна сумісність; всеосяжність.

*Принципами* ведення об'єднаної розвідки на всіх етапах війни під час проведення операцій є: сприйняття; узгодженість; об'єктивність; єдність зусиль; пріоритетність; досконаліть; прогностичність; гнучкість; узагальнення.

Розвідувальна інформація добувається за допомогою засобів та систем,

які можуть спостерігати, записувати та передавати інформацію щодо умов, ситуацій, загроз і подій.

Розвідка поділяється на такі *види*: акустична розвідка (Acoustic intelligence – ACINT); агентурна розвідка (Human intelligence – HUMINT); видова розвідка ( Image intelligence – IMINT); параметрична та сигнатурна розвідка (Measurement and signature intelligence – MASINT); розвідка з відкритих джерел (Open source intelligence – OSINT); радіорозвідка (Signals Intelligence – SIGINT) (електронна розвідка (Electronic intelligence – ELINT); розвідка комунікацій (Communications intelligence – COMINT); розвідка збройних сил; хімічна, біологічна, радіологічна та ядерна розвідка; біометрична розвідка, медична розвідка; науково-технічна розвідка, технічна розвідка**.**

Основу розвідки складає *розвідувальний цикл.* Це певна послідовність дій, коли інформація, що отримана в необробленому вигляді, аналізується та обробляється в розвідувальний інформаційний продукт, доступний для споживачів. У загальному вигляді *розвідувальний цикл* являє собою комплекс заходів, що складається з етапів, які виконуються на різних рівнях із різною швидкістю. Ці *етапи* передбачають виконання дій, які, фактично, визначають суть розвідки: націлювання, планування; добування; обробку; доведення. Деякі заходи перекривають один одного і часто проводяться одночасно, а не послідовно.

Етапами розвідувального циклу є націлювання, добування, обробка, доведення:

а) *націлювання* – передбачає встановлення вимог до розвідувальних даних, планування зусиль щодо збору інформації та постановку завдань добувним підрозділам;

б) *добування* – процес виконання заходів та дій, спрямованих на отримання розвідувальної інформації шляхом виявлення об’єктів противника. Активні дії щодо добування інформації ведуться за допомогою спостереження і рекогносцировки, що становить основну частину зібраної інформації;

в) *обробка* – перетворення добутої розвідувальної інформації в розвідувальні відомості шляхом аналізу, оцінювання надійності та достовірності, інтерпретації розвідувальних відомостей в дані. У результаті обробки інформації можуть з’явитися додаткові вимоги до збору та передачі розвідувальних даних;

г) *доведення* – завершальний етап розвідувального циклу, суть якого полягає у вчасному наданні розвідувальної оцінки в потрібній формі відповідними засобами споживачам у найбільш зручний для них спосіб.

У країнах-членах НАТО використовуються такі *стандартні формати звітів та повідомлень* розвідувальних даних, щоб гарантувати співпрацю з країнами-партнерами, у всіх можливих випадках, де письмові повідомлення та інформація веб-розвідки повинні відповідати форматам. Прикладами таких повідомлень є: розвідувальні повідомлення (Intelligence Report –

INTREP), короткі розвідувальні звіти (Intelligence Summaries – INTSUM), додаткова доповідь з розвідки (Supplementary Intelligence Reports – SUPINTREP), тематичні звіти (Thematic Reports).

Принципи деяких доктрин розвідки НАТО, які займають в архітектурі спільних доктрин порядок, наведений на рис. 1.1.

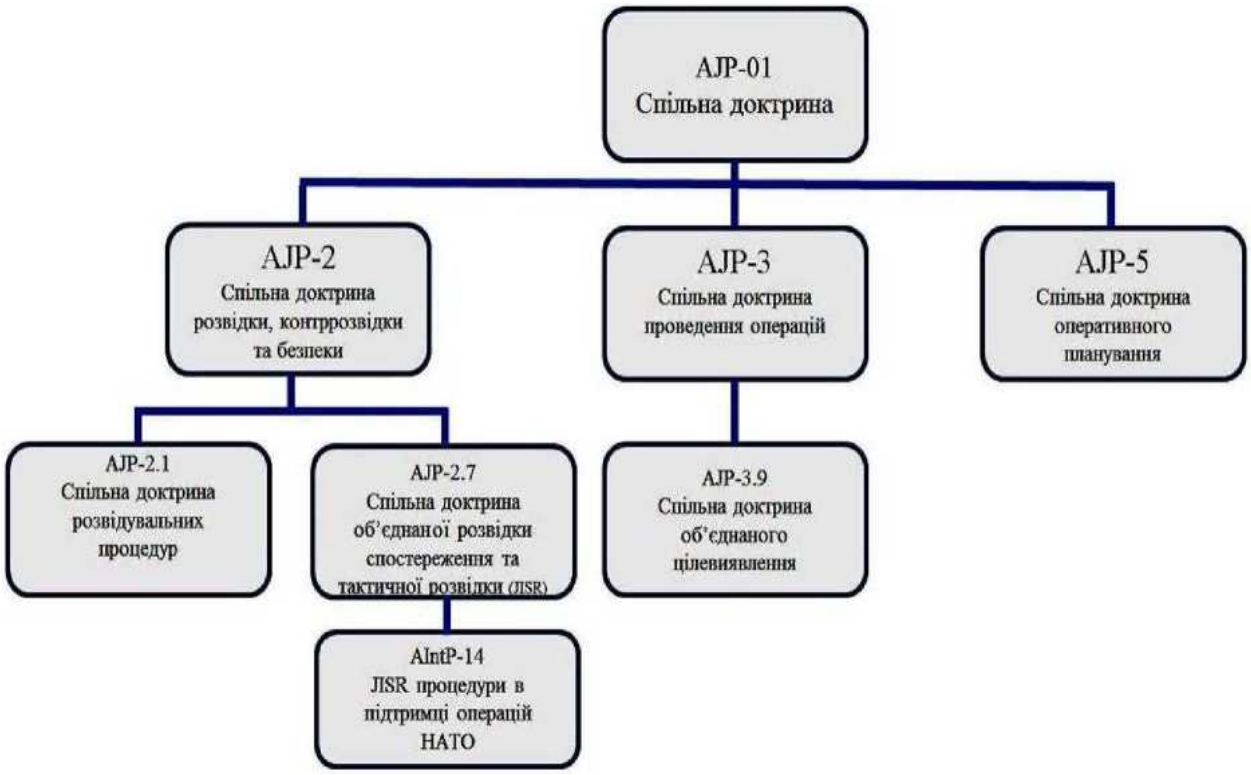



Рис. 1.1. Порядок доктрин розвідки й операцій в архітектурі спільних доктрин НАТО

Доктрини описують фундаментальні принципи, практики і процедури, якими керуються збройні сили для досягнення цілей Об'єднаних операцій. Основним принципом розвідувальних процедур є використання розвідувального циклу – послідовності дій, за допомогою яких інформація отримується, зводиться, перетворюється на розвідувальну інформацію і стає доступною для користувачів. Ці дії характеризуються цілеспрямованістю чотирьох базових етапів розвідки: *управління, збирання, оброблення і поширення* (рис. 1.2.).

Незважаючи на цикл розвідки, який зовні виглядає як простий процес, насправді – це комплекс заходів, що складається з багатьох циклів, які діють на різних рівнях і швидкостях. Кілька циклів можуть відбуватися одночасно. Деякі завдання циклу перекривають одне одного, збігаються і часто проводяться одночасно, а не послідовно.

Утім оновлення принципів у доктринах стосується *управління вимогами до розвідки* (Intelligence Requirements Management – IRM) та *управління збором* (Collection Management – CM), які регулюють функції комплексного

управління особовим складом при виконанні розвідувального циклу [3]. Управління вимогами до розвідки та управління збором є сукупністю процесів управління, спрямованих на оптимальне використання спроможностей збору. Відповідальним за проведення цих процедур є особовий склад секцій розвідки штабів, без яких цикл розвідки стане перенавантаженим.


Рис. 1.2. Розвідувальний цикл

*Управління вимогами до розвідки* (ВР) – це сукупність інтегрованих служб та процесів управління, які розробляють, затверджують, визначають пріоритети вимог до розвідки, ініціюють збір пов'язаної інформації; здійснюють контроль якості оброблених даних і нагляд за поширенням (доведенням) результатів розвідки.

*Управління збором* (УЗ) – це процес перетворення вимог до розвідки на вимоги щодо збору інформації, постановки задач та координації застосування конкретних інструментів збору, моніторингу та повторних постановок задач, що сприяє оптимальному застосуванню спроможностей збору.

Іншою провідною темою оновлених розвідувальних доктрин є поліпшення взаємодії з операційними процесами, для чого ініційовано *JISR-процес*, який дає змогу персоналу розвідувальних та операційних секцій штабів координувати, синхронізувати, деконфліктувати багатоджерельні засоби збору з усіма пов'язаними спроможностями обробки і використовувати їх ефективно і своєчасно [3]. JISR-процес сприяє досягненню зазначеними секціями штабів поставлених командиром цілей і забезпечує швидке прийняття обґрунтованого військового рішення.

*JISR* (*Joint Intelligence, Surveillance and Reconnaissance*) – «Об'єднані Розвідка, Спостереження й Тактична розвідка» – це набір розвідувальних та операційних спроможностей, поєднаних в єдину архітектуру для планування

і досягнення вимог командира. Термін «об'єднані» (J) застосовується для дій, до яких залучені два і більше учасників, що оперують в єдиному середовищі.

*JISR*-процес виконується в п'ять послідовних кроків: вимоги (*task*), збір (*collect*), обробка (*process*), використання (*exploit*) і поширення (*disseminate*), які мають абревіатуру *TCPED* (рис. 1.3).


Рис. 1.3. *JISR*-процес (кроки *TCPED*)

На *JISR*-процес покладається місія забезпечити командира всіма специфічними даними, інформацією і ситуаційною обізнаністю, що стосується збору інформації в процесі проведення операції. Така архітектура процесу дає змогу інтегрувати наявні розвідувальні спроможності в загальну схему маневру операції.

*Перший крок JISR-процесу* – це надання «вимог» (tasking), що полягає в чітких вимогах до збору у вигляді інструкцій і наказів для координації та контролю *JISR*-засобів. На цьому кроці задіються функції персоналу штабу з управління вимогами до розвідки (*IRM*) та визначають оптимальні джерела розвідки з огляду на операційну необхідність, ризики застосування, обмежену наявність інструментів.

Малоймовірно, що особовий склад розвідки колись матиме достатню кількість людей або ресурсів, аби задовольнити всім запитам. Ведення розвідки має бути заздалегідь сплановано й організовано настільки надійно, наскільки це можливо в межах наявних обмежень. Для її успішного ведення мають бути визначені пріоритети процесу розвідки, враховуючи, що вимоги не завжди відповідають наявним спроможностям.

*Другий крок JISR-процесу* – «збір» (*collect*) полягає в безпосередньому зборі даних в операційному просторі. *JISR*-засоби збирають дані, визначені вимогами, і передають їх для подальшої обробки.

*Третій крок* – «обробка» (*process*) полягає в конвертації зібраних даних у встановлені, зручні формати, які дозволяють візуалізацію, подальше використання, зберігання і поширення оброблених даних.

Головною вимогою виконання цього кроку є побудова єдиної інформаційної мережі, завдяки якій добиваються ефекту синергії, коли ефективність від сумісної дії об'єднаних у мережу сил за сукупним результатом перевищує сумарну ефективність від застосування тих же сил та засобів окремо.

Поширення оброблених даних в єдиній мережі є важливим для обробки даних з інших джерел розвідки, які в цей же час задіяні в цій або суміжній зоні відповідальності. Горизонтальні зв'язки сприяють поширенню розуміння, що є істотним для оптимізації застосування різних джерел

розвідки. Кожне джерело у співпраці з іншими може відкоригувати власний збір даних і поліпшити якість інформації в результаті їх обробки.

*Четвертий крок JISR-процесу* – «використання» (*exploit*). На цьому кроці приймається рішення як саме використати зібрану й оброблену інформацію, яка оцінюється на предмет відповідності вимогам до розвідки і, залежно від відповідності, або негайно поширюється авторизованим запитувачам, або спрямовується на дорозвідку із застосуванням функції управління збором (*УЗ*). На цьому кроці персонал приймає складні рішення, які є результатом оцінювання інформації та обстановки, що склалася за критеріями: «кількість-якість», «обґрунтованість-нагальність», «поширення-секретність» тощо. Залежно від ситуації негайне поширення інформації, яка на 80 % відповідає вимогам, може бути пріоритетним порівняно з поширенням обґрунтованої на 100 %, але з втратою часу, і навпаки.

*П'ятий крок JISR-процесу* – «поширення» (*dissemination*) включає своєчасне постачання *JISR*-результатів авторизованим запитувачам в необхідному форматі обумовленими каналами комунікації. Важливо, щоб поширювана ситуаційна обізнаність була стислою і наочною для уникнення переобтяження командира.

Кроки *TCPED* є необхідними для отримання ситуаційної обізнаності та сприяння прийняттю військового рішення. Нехтування хоча б одним кроком веде до втрати важливих даних із бойового простору – слабкість однієї ланки послаблює весь ланцюг. В операціях НАТО процедури *TCPED* застосовуються на будь-якому рівні операції від окремої одиниці, тактичного підрозділу, Об'єднаних сил до багатонаціональних операцій.

Обробка даних (хоч здебільшого й автоматизована) обов'язково вимагає певних навиків і критичного мислення, тому має виконуватися командирами груп (відділень/взводів) на тактичному рівні або командирами певних модулів, якщо джерела різних видів розвідки об'єднані в систему STAR (surveillance, target acquisition, reconnaissance) [3]. Процес обробки даних включає співставлення**,** порівняння з даними з інших джерел, оцінювання джерел на надійність (від повністю надійних до повністю ненадійних).

Результатом обробки даних стає локалізація змін в оперативному просторі, що дає можливість досягти економії обмежених спроможностей після визначення найменованих зон інтересу розвідки (Named Area of Interest – NAI) – обмеженої території, де відбувається цілеспрямований збір специфічних даних.

Рішення «як використати інформацію» приймається секцією розвідки S2/G2 на кроці «використання» за результатами проведення таких процедур: аналіз та інтерпретація.

У процесі аналізу оброблена інформація перевіряється на важливість у конкретній ситуації, можливість зробити прогноз майбутніх дій противника. Надалі вона підлягає інтерпретації, за якої оцінюється на правдоподібність з огляду на обстановку, військовий досвід, ситуаційну обізнаність (від високоймовірної до неймовірної).

Після аналізу та інтерпретації, персонал, відповідальний за процедури кроку «використання», приймає рішення про негайне «поширення» отриманої ситуаційної обізнаності в мережі або проведення дорозвідки. При рішенні на користь дорозвідки формулюють специфічні, уточнені вимоги у вигляді першочергових вимог до розвідки (*Piority Intelligence Requirements – PIR*) – вимог, у яких передбачається результат або ставляться пріоритети.

Без визначення пріоритетів можлива втрата ефективність високоточних інструментів розвідки таких, як контрбатарейні радари і БПЛА. Для запобігання цьому і використанню максимальної ефективності новітніх засобів розвідки у 2005 році було впроваджено «Архітектуру взаємодії розвідки, спостереження і тактичної розвідки НАТО» (*NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture – NIIA*).

Надавши чіткі специфічні вимоги для тактичної розвідки, зберігши можливість використовувати дані з інших сенсорів і застосувавши техніку *перехресного спрямування* (Cross-cueing) можна розраховувати на підтвердження передбачуваної ситуаційної обізнаності або спростування прогнозу. Техніка перехресного спрямування координує багатоджерельні *JISR* спроможності, використовуючи інформацію з одних джерел, для того, щоб дати напрям іншому інструменту розвідки для отримання більш детальних або пов'язаних даних.

Архітектура взаємодії розвідки, спостереження і тактичної розвідки дає змогу досягти найефективнішого результату через оптимальне застосування новітніх засобів розвідки у взаємодії з давно існуючими засобами.

*Інтеграція розвідувального і операційного циклів. JISR*-процес не підміняє розвідувальний цикл, скоріше він є частиною процесу інтеграції розвідки в операції. Через синхронізацію та інтеграцію розвідувальних і операційних процесів командири та їх штаби мають змогу визначати пріоритети, надавати вимоги та розподіляти наявні засоби в кожній конкретній операції.

Місце *JISR*-процесу в синхронізації та інтеграції розвідувального й операційного циклів наведено на рис. 1.4. Як видно, дані, які могли бути втрачені через незначущість, отримали сенс завдяки застосуванню процедур співставлення, оцінювання, аналізу, інтерпретації та цілеспрямованого залучення точніших інструментів розвідки.

Здатність перетворити інформацію в звіт розвідки, на основі якого приймається військове рішення – вирішальна спроможність. В умовах залучення великої кількості сенсорів задіяних в операції відбиття збройної агресії, та для ефективного їх застосування підрозділам операції необхідно дотримуватись єдиних розвідувальних процедур з управління вимогами до розвідки, збором даних, обробкою та поширенням інформації про зміни в операційному просторі.

Ключовим принципом розвідувальних процесів у доктринах НАТО є «централізоване планування – децентралізоване виконання» [3]. Цей принцип потребує імплементації як на оперативному, так і на тактичному рівнях процедур і технік об'єднаної розвідки, спостереження, тактичної

розвідки (JISR) та цілевиявлення, що дасть змогу гармонізувати розвідувальні й операційні функції.

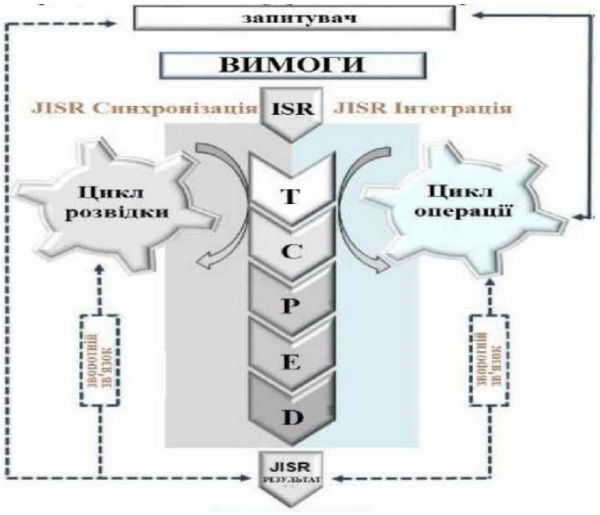



Рис. 1.4. Місце *JISR* процесу відносно розвідувального й операційного циклів

*Термінологія в галузі інформаційних технологій щодо добуванню, обробки та аналізу даних. Інтеграція інформації (Data integration)* – діяльність, що має на меті оптимальну організацію різнорідних даних у вигляді бази даних (схеми даних), при якій реалізовано всі необхідні взаємозв'язки між елементами даних, але база даних (БД) не містить повторів і зайвих елементів (так як по мірі використання бази даних вона має тенденцію роззосереджуватись). Включає об'єднання даних, що знаходяться в різних джерелах, і надання даних користувачам в уніфікованому вигляді.

*Консолідація.* У разі консолідації дані витягуються з джерел, і поміщаються в сховище даних. Процес заповнення Сховища складається з трьох фаз – витяг, перетворення, завантаження (*Extract, Transformation, Loading – ETL*). У багатьох випадках саме *ETL* розуміють під терміном «інтеграція даних». Ще одна поширена технологія консолідації даних – управління змістом інформації в організації (*Enterprise content management – ECM*). Більшість рішень *ECM* спрямовані на консолідацію і управління неструктурованими даними, такими як документи, звіти і веб-сторінки. Консолідація – односпрямований процес, тобто дані з декількох джерел зливаються в сховище, але не поширюються з нього назад в розподілену систему. Часто консолідовані дані є основою для додатків бізнес-аналітики (*Business Intelligence – BI*), *OLAP*-додатків. При використанні цього методу зазвичай існує деяка затримка між моментом оновлення інформації в первинних системах і часом, коли ці зміни з'являються в кінцеве місце зберігання. Кінцеві місця зберігання даних, що містять дані з великими часом відставання (наприклад, більше одного дня), створюються за допомогою пакетних додатків інтеграції даних, які витягають дані з первинних систем з певними, заздалегідь заданими інтервалами. Кінцеві місця зберігання даних з

невеликим відставанням оновлюються за допомогою оперативних додатків інтеграції даних, які постійно відстежують і передають зміни даних з первинних систем в кінцеві місця зберігання.

*Федералізація.* В федеративних БД фізичного переміщення даних не відбувається: дані залишаються у власників, доступ до них здійснюється при необхідності (при виконанні запиту). Спочатку федеративні БД припускали створення в кожному з вузлів декілька фрагментів коду, що дозволяє звертатися до будь-якого іншого вузла. При цьому федеративні БД відокремлювали від медіаторів. При використанні медіатора створюється загальне уявлення (модель) даних. Медіатор – посередник, що підтримує єдиний користувальницький інтерфейс на основі глобального представлення даних, що містяться в джерелах, а також підтримку відображення між глобальним і локальним уявленнями даних. Користувальницький запит, сформульований в термінах єдиного інтерфейсу, декомпозіруется на безліч підзапитів, адресованих до потрібних локальних джерел даних. На основі результатів їх обробки синтезується повну відповідь на запит. Використовуються два різновиди архітектури з посередником – глобальна видом і, як *Local View*. Відображення даних з джерела в загальну модель виконується при кожному запиті спеціальною оболонкою (обгортка). Для цього необхідна інтерпретація запиту до окремих джерел і подальше відображення отриманих даних в єдину модель. Зараз цей спосіб також відносять до федеративним БД. Інтеграція корпоративної інформації (Enterprise Information Integration – EII.) Це приклад технології, яка підтримує федеративний підхід до інтеграції даних. Вивчення і профілювання первинних даних, необхідні для федералізації, несильно відрізняються від аналогічних процедур, необхідних для консолідації.

*Поширення Даних.* Додатки поширення даних здійснюють копіювання даних з одного місця в інше. Ці програми зазвичай працюють в оперативному режимі і виробляють переміщення даних до місць призначення, тобто залежать від певних подій. Оновлення в первинній системі можуть передаватися в кінцеву систему синхронно або асинхронно. Синхронна передача вимагає, щоб поновлення в обох системах відбувалися під час однієї і тієї ж фізичної транзакції. Незалежно від використовуваного типу синхронізації, метод поширення гарантує доставку даних в систему призначення. Така гарантія – це ключовий відмітна ознака поширення даних. Більшість технологій синхронного поширення даних підтримують двосторонній обмін даними між первинними і кінцевими системами. Прикладами технологій, що підтримують поширення даних, є інтеграція корпоративних додатків (*Enterprise Application Integration – EAI*) і тиражування (реплікація) корпоративних даних (*Enterprise Data Replication – EDR*). Від федеративних БД цей спосіб відрізняє двостороннє поширення даних.

*Сервісний підхід.* Сервісно-орієнтована архітектура (*Service Oriented Architecture – SOA*), успішно застосовується при інтеграції додатків, може

бути застосована і при інтеграції даних. Дані також залишаються у власників і навіть місцезнаходження даних невідомо. При запиті відбувається звернення до певних сервісів, які пов'язані з джерелами, де знаходиться інформація і її конкретну адресу. Інтеграція даних об'єднує інформацію з кількох джерел таким чином, щоб її можна було показати клієнту у вигляді сервісу. Сервіс – це не запит в традиційному сенсі звернення до даних, скоріше, це витяг деякої бізнес-сутності (або сутностей), яке може бути виконане сервісом інтеграції через серію запитів і інших сервісів. *SOA*-підхід концентрується, в першу чергу, на визначенні та спільному використанні в формі сервісів щодо обмеженої кількості найважливіших бізнес-функцій в корпорації. Отже, сервіс-орієнтовані інтерфейси в досить великій мірі будуються на обмеженій кількості запитів на необхідну інформацію, яку потрібно представити споживачеві. Маючи відповідні облікові дані системи безпеки, споживач може здійснити вибірку будь-яких даних з джерела через майже необмежену кількість різних запитів *SQL*. Але для цього споживач повинен мати уявлення про модель джерела даних і способі створення результату з використанням цієї базової моделі. Чим складніше модель джерела даних, тим складнішою може виявитися ця задача.

*Потокова обробка даних.* Технологія потокової обробки змінює порядок роботи з даними: замість порядку «зберіг – обробив», з'являється послідовність «обробив – зберіг». Чим більша частка надлишкової інформації видаляється при обробці, тим менше інформації потрібно зберегти для прийняття рішень в подальшому і тим нижче вимоги до обсягів зберігання даних.

Оскільки більшість джерел працює в реальному часі, то і фільтрацію доводиться проводити в реальному часі. У підсумку, потокова обробка, знижує вимогу до пам'яті і підвищує вимоги до продуктивності обчислювальної системи при фільтрації. Оскільки джерела працюють незалежно, то при потоковій обробці можливий масовий паралелізм – тобто застосування великих ферм паралельно працюючих комп'ютерів з можливістю їх масштабування.

З технологічної точки зору, очевидно, що сучасна платформа для реалізації інформаційно-аналітичної системи повинна володіти технологіями для роботи як зі статичними даними (структурованими і неструктурованими), так і з динамічними даними (потоками даних від будь-яких типів джерел). Тому очевидно, що невід'ємним властивістю платформи має бути інструмент інтеграції всіх видів даних для подальшого комплексного аналізу і прийняття рішення.

*Системи реального часу на основі самонавчання.* Метою самонавчання є поліпшення характеристик інформованості та інтелектуальності системи. Наприклад, вже накопичені дані можуть використовуватися для фільтрації шумів в потоці даних (системи зі зворотним зв'язком). В цілому можна сказати, що підвищення ефективності виділення корисного сигналу на основі адаптивних алгоритмів, радикальним чином позначається на показниках

системи в цілому. Таким чином, знижуються вимоги до обсягу обчислень та обсягу пам'яті, які необхідні для прийняття рішення.

*Спеціалізовані прискорювачі обробки аналітичних запитів до реляційних баз даних.* Прискорювачі обробки запитів призначені для прискорення процесу аналітичної обробки накопиченої інформації з метою підготовки та оцінки наслідків різних варіантів рішень. Суть проблеми, на вирішення якої орієнтовані прискорювачі, полягає в наступному: аналітики заздалегідь не можуть визначити для себе, які саме запити вони будуть задавати в базу, більш того відомо, що наступні запити будуть напевно змінюватися залежно від відповідей на попередні запити. Спеціалізовані прискорювачі обробки непередбачених запитів призначені для вирішення цієї проблеми. Ідеї, на яких вони базуються: масовий паралелізм і адаптивна динамічна перебудова структури бази під запит.

*Використання зовнішніх джерел даних.* Традиційно використовують аналітичні системи, що базуються на внутрішній інформації. Сучасні підходи припускають залучення і зовнішніх джерел даних.

*Адаптивний пошук інформації.* Новітні технології пошуку інформації реалізуються через інструментарій пошукових платформ, що надають для аналітиків сервіси пошуку в усьому кіберпросторі. Оскільки процеси прийняття рішень зі статичних і апріорно зумовлених стають динамічними (із зворотними зв'язками), вже отримана інформація дозволяє розширювати або звужувати коло пошуку і підвищувати якість рішення в порівнянні з традиційною схемою. Для цього, сучасні пошукові платформи, наприклад, *IBM Data Explorer*, архітектурно поділяють на чотири рівні:

1) рівень доступу, що надає можливості уніфікованого доступу до різнотипних зовнішніх і внутрішніх джерел даних;

2) рівень обробки, який організує пошук джерел, нанесення знайдених джерел на карту пошуку, передачу інформації для візуалізації;

3) користувальницький рівень, який створює ситуаційний центр пошуку та візуалізації знайденої інформації;

4) рівень додатків, що дозволяє будувати власні схеми роботи з інформацією для її візуалізації та подальшого аналізу.

*Інтеграція нових і старих технологій.* Поряд з давно застосовуваними технологіями для роботи зі структурованими і неструктурованими даними всіх видів, програмами аналізу та прогнозування, використовуються новітні технології потокової обробки і сховища даних.

*Характеристики Big Data.* Як визначальних характеристик для великих даних зазначають: обсяг (англ. *Volume*) – величина фізичного обсягу, швидкість (англ. *Velocity*) – швидкість приросту і необхідність високошвидкісної обробки і отримання результатів, різноманітність (англ. *Variety*) – можливість одночасної обробки різних типів структурованих і напівструктурованих даних, достовірність джерел даних (англ. *Veracity*), мінлівість даних (англ. *Variability*), складність або різнорідність даних (англ. *Complexity*), ступінь візуалізації даних (англ. *Visualization*).

*Термінологія системного зведеного аналізу інформації від різнотипних джерел.* *Системний аналіз інформації* – це комплекс моделей, алгоритмів, методик аналізу, який використовується для розгляду та вивчення складних систем або ситуацій. Він передбачає розгляд інформації у контексті взаємозв'язків, властивостей та характеристик системи в цілому.

*Основні аспекти системного аналізу* інформації включають: ідентифікація складних систем, збір та обробка інформації, аналіз структури системи, оцінка функцій та характеристик, моделювання, прогнозування та сценарний аналіз, прийняття рішень, визначення впливу змін, контроль та моніторинг.

Системний аналіз інформації є потужним інструментом для розгляду складних ситуацій, систем та проблем, що вимагають комплексного підходу та врахування великої кількості факторів.

Також можна визначити *зведений аналіз інформації* – це процес об'єднання та інтеграції різних джерел інформації для отримання комплексного та об'єктивного уявлення про певну ситуацію, явище чи проблему. У зведеному аналізі інформації важливо враховувати різноманітність джерел та їхніх характеристик.

*Основні кроки зведеного аналізу* можуть включати: збір інформації, обробка та стандартизація, інтеграція, визначення надійності джерел, врахування невизначеності та ризиків, синтез та аналіз, врахування контексту та взаємозв'язків, прийняття рішення.

Зведений аналіз інформації дозволяє здійснити об'єктивний та комплексний огляд ситуації чи проблеми, що є важливим для прийняття обґрунтованих рішень.

Зведений аналіз інформації та комплексування інформації є схожими, але вони мають деякі *відмінності* у підході та меті. Зведений аналіз інформації передбачає об'єднання та інтеграцію різних джерел інформації для отримання комплексного та об'єктивного уявлення про певну ситуацію, явище чи проблему. *Комплексування інформації* означає об'єднання та систематизацію різних даних, щоб забезпечити їхню структурованість та організованість.

Отже, основна різниця полягає в тому, що зведений аналіз інформації спрямований на аналіз та прийняття рішень на основі зібраної інформації, тоді як комплексування інформації спрямоване на створення організованої та структурованої бази даних для зручного користування.

*Системний зведений аналіз інформації від різнотипних джерел* – це комплексний підхід до обробки та аналізу даних, що надходять з різних джерел з метою отримання повнішого та об'єктивнішого уявлення про ситуацію чи проблему.

*Основні кроки системного зведеного аналізу* можуть включати: збір інформації, обробка та перевірка, інтеграція, стандартизація, аналіз надійності та точності джерел, обробка невизначеності, синтез та агрегація, визначення альтернативних сценаріїв, врахування контексту та зв'язків, прийняття рішення.

Системний зведений аналіз інформації забезпечує комплексний та об'єктивний підхід до розгляду складних ситуацій та проблем, дозволяючи приймати обґрунтовані рішення на основі повного уявлення про ситуацію.

## 1.2. Проблеми системного зведеного аналізу інформації від різнотипних джерел

*Проблеми зведеного аналізу інформації.* На багатьох етапах проведення аналітичної роботи виникають проблеми пов’язані з постійним розвитком та трансформацією об’єктів інтересу, обмеженістю можливостей кожного з видів добування інформації, великим обсягом завдань, обмеженим ресурсом, зростаючими вимогами до форм подання інформації, зростаючими вимогами до достовірності та повноти інформації [1–5].

*На етапах постановки завдання та планування* постають проблеми з визначенням основних об’єктів, суміжних з ними об’єктів та об’єктів, які їх забезпечують, з визначенням переліку характеристик об’єктів, розрахунком сил та засобів спостереження. Це пов’язано з браком наявної інформації про попередні стани об’єкта (прийняття рішень в умовах невизначеності) або не точним знанням ймовірностей станів (прийняття рішень в умовах ризику). Інакше кажучи, є інформація про стан об’єкта, але ця інформація неточна й неповна.

*На етапі добування інформації* постають проблеми під час безпосереднього виконання завдань силами та засобами добування щодо добування та первинної обробки інформації. Проблеми пов’язані з обмеженістю можливостей кожного з видів спостереження, обсягами завдань, обмеженим ресурсом на їх виконання та вимогами до уніфікації форм подання інформації.

*На етапі аналітичної обробки інформації та підготовки рішення* постають проблеми аналітичної обробки інформації за результатами добування різними силами та засобами, узагальнення різнорідних даних, отриманих з багатьох джерел та підготовка інтегрального (узагальненого) рішення щодо характеристик об’єкта.

*Основною проблемою зведеного аналізу інформації є гетерогенність (різнорідність) джерел даних*. Наприклад, якщо йдеться про геопросторові дані, то їх різнорідність проявляється в кількох вимірах: простір, час, масштаб, зв’язки та атрибути. Під час інтеграції різнорідної інформації необхідно компенсувати різнорідність за вказаними вимірами, використовуючи сервіси перетворення даних [6,7]. Очевидно, що система інтеграції має включати в себе такі сервіси і забезпечувати користувачам доступ до них. Для вирішення більшості завдань інтеграції інформації перш за все необхідно визначити базиси інтеграції, стає визначення базисів інтеграції, тобто певні інформаційні характеристики або властивості, які є загальними для всіх даних, що

інтегруються.

*У загальному випадку процесу інтеграції перешкоджає неоднорідність джерел даних відносно рівня інтеграції*. Так, під час інтеграції на фізичному рівні в джерелах даних можуть використовуватися різні формати файлів. На логічному рівні інтеграції може мати місце неоднорідність моделей даних для різних джерел або розрізненість схем даних у разі використання однієї й тієї ж моделі даних. На семантичному рівні інтеграції різні джерела інформації можуть відповідати різним онтологіям. Виділяють такі основні види інтеграції даних: синтаксичну, структурну, семантичну. Для семантичної інтеграції інформації можна використовувати підхід на основі онтологій, який передбачає створення спільного та узгодженого розподіленого словникового ресурсу. На практиці для семантичної інтеграції інформації використовують такі технології, як XML, RDF та OWL.

Окрім різноманітних даних, існують і різноманітні інформаційні системи (ІС), які містять і обробляють ці дані, а саме апаратного та програмного забезпечення (на рівні інтерфейсів, прикладних програм, операційних систем). Звичайно, це створює проблеми інтеграції даних, технологій і ІС, що негативно впливає на ефективність вирішення завдань.

Зрозуміло, що в переважній більшості випадків неможливо створити ізольований інформаційний ресурс. Так чи інакше будь-який інформаційний ресурс має взаємодіяти з іншими ресурсами. Існує три рівні інтеграції інформаційних ресурсів: рівень файлів, рівень операційного середовища та рівень інформаційно-комунікаційних систем (ІКС). Вибір рівня інтеграції визначається єдиними стандартами, наприклад, OSI (Open Systems Interconnection).

*Проблема інтеграції військових та цивільних організаційних структур* (створення з’єднань, злиття напрямів діяльності тощо) для вирішення складних міжвідомчих завдань полягає в розпорошеності та неповноті технологічних рішень і стандартів формування ІС. Ця проблема стосується і сучасних технологічних підходів, і майбутніх, залежно від принципів відкритості архітектури та розподіленого функціонування. Також залишаються невирішеними проблеми стандартизації порядку надання інформації в системах міжорганізаційного обміну, стандартизації форматів повідомлень між програмними рішеннями учасників відповідної діяльності, регулюючих державних структур, інформаційних агенцій, проблеми розробки та узгодження протоколів взаємодії, обміну та захисту інформації на всіх етапах виконання того чи іншого завдання.

Вирішення згаданих проблем лежить у площині побудови спільного інформаційного простору, який має поєднати в міжорганізаційних процесах наявні електронні інформаційні ресурси (ІР) різного відомчого

підпорядкування. Загальне завдання складатиметься з таких етапів:

- об’єднання даних з IP наявних систем (інтеграція даних) у рамках новостворюваного спільного інформаційного простору;
- забезпечення спільної роботи апаратно-програмних рішень, що зазвичай для цього не призначені;
- розробка спільного плану забезпечення наскрізної інформаційної безпеки;
- швидка адаптація створеного спільного інформаційного простору до змін у цільовому призначенні та складі взаємодіючих організаційних структур;
- створення нових функціональних можливостей на основі наявних рішень із мінімальними витратами.

*Ще однією проблемою інтеграції є складність обробки великих обсягів даних* [6]. Так, серед проблем комплексного управління даними в єдиному інформаційному просторі слід відзначити неможливість або економічну недоцільність зберігання та реєстрації всього обсягу потоків даних, низьку інформативну ємність окремих потоків даних, складність зберігання великої кількості недостатньо структурованих даних, неможливість довготривалого зберігання, проблеми пошуку, розповсюдження, передачі та візуалізації даних. За допомогою традиційних технологій обробки та управління базами даних вирішити ці проблеми сьогодні не можливо. Процес обробки даних пов'язаний з такими показниками: обсяг даних; швидкість зростання обсягів даних; різноманітність даних (структурованих, напівструктурованих, неструктурованих); достовірність; мінливість; складність; ступінь візуалізації.

Для спрощення обробки даних пропонується використовувати гібридний підхід на основі технологій розподілених обчислень *Grid*, *Cloud*, *SN*-архітектури (*Shared Nothing Architecture – SNA*), що забезпечує масивно-паралельну обробку даних, а також технологій зберігання даних *NoSQL*, програмного інтерфейсу *MapReduce*, платформи *Hadoop* та технологій потокової обробки даних типу *IBM Streams* [7].

*Важливою проблемою інтеграції інформації є складність управління* процесами розподіленого замовлення, первинної обробки, доставки, зберігання, аналітичної обробки та подання результатів споживачам. Різнорідність завдань координації, збільшення розмірності завдань (кількості параметрів, що узгоджуються), невизначеність в оцінюванні стану процесів зумовлюють необхідність розроблення алгоритмів розподіленої ієрархічної координації процесів інтеграції. Очевидною стає потреба координації зусиль усіх елементів системи, гармонізація їх діяльності.

Вирішуючи задачу управління процесом інтеграції інформації, необхідно враховувати невизначеність ситуації довкола об’єктів

інтересу та складність визначення параметрів елементів системи управління [5,8]. Для декомпозиції загальної задачі пропонується використовувати теорію багаторівневих ієрархічних систем, а для вирішення задачі оптимального управління процесом інтеграції – ітеративні та неітеративні алгоритми координації.

Протягом тривалого часу *основним математичним апаратом* для аналізу невизначеності була теорія ймовірностей, при цьому передбачалося, що внутрішню природу подій точно визначено [9]. Однак у реальних завданнях підмножини випадкових подій пов'язані з результуючою, таким чином залежності ймовірностей окремих подій мають більш складний характер. Це спричиняє потребу використання інших концептуальних підходів до вирішення завдань із таким комбінованим незнанням. Такими підходами сьогодні є теорія Демпстера-Шейфера (ТДШ) і теорія Дезерта-Смарандаке (ТДС) [9–12].

ТДШ припускає випадок, коли призначення ступенів упевненості виконують кілька незалежних експертів, при цьому постає завдання комбінування цих значень на основі правил комбінування. У деяких ситуаціях досягти взаємного виключення елементів основи аналізу не вдається, з такого роду проблемами ТДШ принципово не може впоратися.

Тому в такому випадку доцільно використовувати більш широку ТДС та теорію обчислень в інтервальній формі [13]. У цій теорії комбінування здійснюється на основі процедури розрахунку узагальнених комбінованих мас упевненості для всіх можливих перетинань вихідних фокальних елементів з подальшим підсумком цих мас для однакових комбінованих фокальних елементів. Також використовуються гібридні моделі для розрахунку.

*Отже, аналіз наявних методологічних платформ свідчить про таке:*

- теорія ймовірностей має обмежені можливості застосування, оскільки події та факти про об'єкт інтересу не завжди відповідають вимогам до обсягів статистичних даних та вибірок, статистичні методи не дають можливості обробляти незнання, існують певні труднощі з обробленням даних від корельованих джерел;
- в теорії нечітких множин простежується суб'єктивний фактор у разі використання функції належності, що потребує експертних оцінок; найбільш узагальненою методологічною платформою сьогодні є теорія свідоцтв Демпстера-Шейфера, яка узагальнює статистичні теорії і позбавлена зазначених вище недоліків.

*Проблему зведеного аналізу різнотипних даних можна вирішити у двох напрямах*: збільшення сил та засобів спостереження (шлях інтенсифікації) та раціональне комплексування (інтеграція) наявних сил та засобів. Саме усунення протиріч шляхом зведення потребує методологічної платформи. Такою платформою можуть бути методи

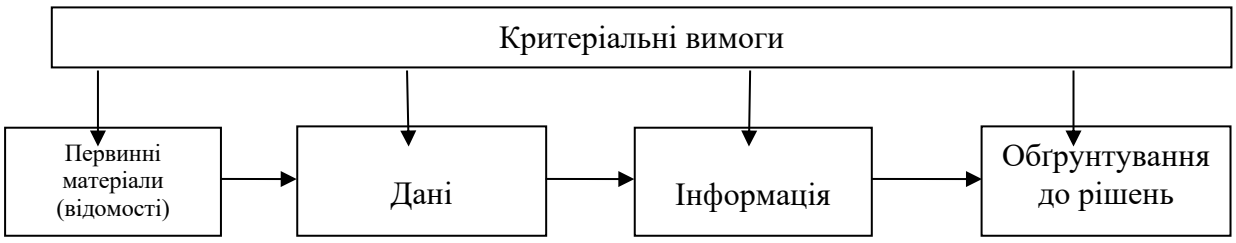
теорії ймовірностей, теорії нечітких множин, теорії свідчень та інші.

- Реалізація методології системного зведеного аналізу інформації від різних джерел дасть можливість ефективно вирішувати такі задачі:
- раціонально будувати та розвивати єдину систему збору та аналізу інформації;
- постійно розширювати коло джерел інформації, постійно вдосконалювати систему перевірки надійності та достовірності джерел інформації;
- створювати структуровані масиви даних (БД) інтегрованого банку даних;
- розробляти програми автоматизації інформаційної роботи;
- запроваджувати єдині форми інформування про розвиток ситуації в різних сферах національної безпеки, єдині штабні процедури, стандарти та форми документів;
- впроваджувати єдиний механізм аналізу і контролю виконання завдань на всіх рівнях з метою підвищення ефективності діяльності та визначення пріоритетів ресурсного забезпечення;
- автоматизувати основні процеси обміну інформацією про стан та можливості сил і засобів з використанням інформаційних технологій;
- уніфікувати засоби управління силами та засобами для досягнення повної сумісності в частині застосування програмних та апаратних засобів.

### 1.3. Технологія *Hard and Soft Data Fusion* як основа системного зведеного аналізу інформації різнотипних джерел

Будь-яка аналітична система працює з даними (збирає відомості, обробляє та аналізує їх і т.д.), а метою здійснення сукупності таких перетворень є отримання і надання споживачу інформації, необхідної для прийняття бойових, інформаційних, управлінських або інших рішень [2–4]. Загальна схема перетворень первинних матеріалів – відомостей в рішення показана на рис.1.5.

Засоби добування забезпечують отримання первинних матеріалів у вигляді певних відомостей. Якщо подібні матеріали збирає людина, то вона зазвичай документує їх. Однак робота з неформалізованими текстовими документами є дуже складною, тому далі, по можливості, текст обробляється таким чином, щоб можна було імплементувати його в комп’ютерні процедури аналізу.



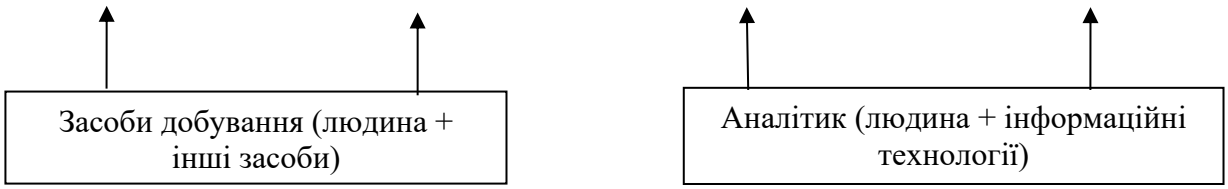



Рис. 1.5. Схема перетворень первинних матеріалів в рішення

Якщо по заданому об'єкту працює засіб технічного спостереження, то отримані ним матеріали (сукупність сигналів) також перетворюються в один з визначених форматів.

Процедури виокремлення з отриманих первинних матеріалів, перетворених у дані визначених форматів, контенту і підготовка пропозицій щодо можливих рішень виконуються Аналітиком за допомогою сучасних інформаційних технологій.

Процес перетворення первинних матеріалів – відомостей в рішення, буде досягати своєї мети, якщо дані та інформація задовольняють певним вимогам щодо їх якості. Основні, найбільш важливі параметри якості відомостей, даних та інформації наведено в табл. 1.1.

В нормативних документах НАТО [3], відзначається, що першим і найважливішим критерієм якості інформації є її достовірність. В стандарті НАТО *STANAG 2022 «Intelligence Reports»* прямо вказується, що при складанні звіту на основі здобутої інформації має наводитись рівень достовірності цієї інформації (*Credibility of Information*). У додатку до цього стандарту запропонована номінальна шкала для оцінювання достовірності, за якою рівень достовірності визначається шляхом порівняння контенту даної інформації з контентом, отриманим незалежно від референсних джерел.

Таблиця 1.1. Параметри якості відомостей, даних та інформації

| **Первинні відомості** | **Дані** | **Інформація** |
|---|---|---|
| Актуальність (відповідність потребам споживача) | Точність / детальність передавання первинних відомостей про об'єкти інтересу. | Цінність / значимість (необхідність споживачу для прийняття обґрунтованого рішення) |
| Здатність забезпечити максимум інформаційного контенту | Інтероперабельність | Достовірність |
| Надійність (відповідність оцінок об'єктивній реальності) | Захист від несанкціонованого доступу | Повнота (достатність для прийняття споживачем обґрунтованого рішення) |
| Оперативність (рівень відставання змісту надісланих відомостей від динаміки об'єкта) | Стійкість до зовнішнього впливу | Своєчасність |

Нажаль, як справедливо відзначається, такий шлях визначення достовірності інформації зустрічає серйозні труднощі, оскільки, по-перше,

Аналітику далеко не завжди доступна референсна інформація, і, по-друге, якщо референсні джерела, що залучаються, відрізняються між собою за своєю надійністю, то результати порівняння не можуть вважатися коректними. Тому актуальною задачею є пошук інших підходів до оцінювання якості інформації, її здатності задовольняти вимогам осіб, що приймають на її основі рішення.

Якщо ми звернемось до робіт останнього часу, пов’язаних з вивченням критеріальних передумов прийняття рішень, наприклад, то побачимо, що зараз дуже велика увага приділяється зменшенню невизначеності в інформації і показано, що навіть невелике зменшення рівня невизначеності сприяє суттєвому підвищенню адекватності рішення.

Невизначеність, яка завжди супроводжує процеси вивчення або дослідження, обумовлюється, в основному, двома причинами. Перша причина – це наявність елементів випадковості (непередбачуваної мінливості) в явищах і процесах, що відбуваються в реальності. Друга причина – брак (неповнота) наявних знань і наближений, оціночний характер даних та відомостей щодо явищ і процесів. Невизначеність, яка обумовлена першою причиною, називають еліторною (*aleatory*) або об’єктивною невизначеністю, а невизначеність, яка обумовлена другою причиною, – епістемічною (*epistemic*) або суб’єктивною невизначеністю.

Зменшити еліторну складову невизначеності в інформації вдається, якщо є можливість оцінити типаж і характерні риси присутньої тут випадковості, наприклад, шляхом залучення повторних вибірок процесів і визначення законів розподілу відповідних величин. Всі ці заходи здійснюються шляхом організації проведення багаторазових вимірювань та їх статистичного аналізу методами теорії ймовірності.

Епістемічна невизначеність пов'язана із обсягом, достовірністю і семантичними властивостями даних, на підставі яких формується інформація. Цей тип невизначеності характеризується станом (часткової) відсутності знань щодо досліджуваного об'єкта, стосовно його передісторії, контексту тощо. Боротьба з епістемічною невизначеністю здійснюється на етапі аналізу отриманих даних.

Ефективний шлях подолання невизначеності у цілому має базуватись на залученні до виконання завдань одночасно й людини, й технічних засобів. Врахування особливостей, притаманних людині і технічним засобам (табл. 1.2), дозволяє отримувати необхідні дані, а їх комплексування забезпечить розуміння об’єктів реального світу і процесів, які у ньому відбуваються.

Таблиця 1.2. Особливості, притаманні людині і технічним засобам збору інформації

| **Людина** | **Технічні засоби добування** |
|---|---|
| Схильна орієнтуватися на якісні моделі реального світу. Краще працює в номінальній та порядковій шкалах | Працюють за принципом кількісного вимірювання параметрів фізичних полів та об’єктів |
| Здатність працювати практично по | Номенклатура об’єктів вивчення |

| Людина | Технічні засоби добування |
|---|---|
| будь-яким об’єктам (військовим, промисловим, адміністративним, організаційним та ін.) | обмежена технічними характеристиками засобу |
| Властивості враховувати передісторію об’єкта, вторинні ознаки, контекст тощо | Низька ефективність в умовах складної сигнальної обстановки (шуми, завади) |
| Гнучкість в оцінках, здатність находити рішення при наявності суперечливих даних | Однозначність і передбачуваність в оцінках і рішеннях |
| Можливість прогнозування | Відтворюваність і рішень для тотожних (подібних) об’єктів і ситуацій |
| Здатність до самоконтролю і ситуативного коригування власних планів і дій | Орієнтовані, переважно, на роботу з об’єктами тактичної та оперативно-тактичної ланки |

Однак комплексний, системний підхід до ведення аналітичної роботи потребує розроблення і наукового обґрунтування моделей складних процесів перетворення первинних даних в інформацію та оптимальні рішення на базі використання сучасних математичних методів аналізу даних. Таку можливість надає математичний інструментарій теорії свідчень Демпстера-Шейфера (ТСДШ) [9–12].

Інструментарій теорії свідчень розглядається як узагальнення методів теорії ймовірностей і забезпечує такі можливості: можливість працювати як з «чіткими» (*hard*), так й з «м'якими» (*soft*) даними; обробляти складні гіпотези; має в своєму арсеналі доволі прості процедури об'єднання свідчень від різнотипних джерел; дозволяє вводити в розрахунки надійність джерел даних (*discounting*); пропонує нетрадиційні критерії прийняття рішень.

Кембриджський словник ділової англійської мови (The Cambridge Business English Dictionary) визначає поняття Hard Data і Soft Data наступним чином: Hard Data – це інформація, така як цифри або факти, що може бути доведена; Soft Data – це інформація про речі, які важко виміряти, такі як думки або почуття людей.

Щоб пояснити поняття «чітких» і «м'яких» даних і ризницю між ними у більш предметно, звернемось до структури даних, якими описуються об’єкти інформаційного поля, наприклад, геопросторові об’єкти. Дані про будь-який геопросторовий об’єкт складаються з трьох компонентів: тематичної, просторової і часової. Тематична компонента – це атрибути об’єкта як конкретного елемента предметної області (його назва, клас, поточний стан, функціональні зв’язки з іншими об’єктами тощо). Просторова компонента визначає місце об’єкта на земній поверхні або в тривимірному просторі у заданій системі координат. Часова компонента фіксує той момент або інтервал часу, коли визначалися атрибути об’єкта і його місцеположення. Часова компонента також може показувати залежність зміни властивостей об’єкта від часу.

Деякі елементи означених компонент, наприклад, час, координати, відстані. вимірюються за допомогою різноманітних технічних засобів. Вимірювання є завжди однозначними, й тому подібні дані вважаються чіткими. Загально кажучи, до «чітких» відносять дані, які обумовлені сигналами, що утворюються різноманітними фізичними об’єктами і полями. Чіткі дані формуються, зокрема, засобами з арсеналу GEOINT, MASINT [3].

Більшість елементів тематичної компоненти даних щодо об’єктів інформаційного поля визначаються сьогодні за участю людини. В силу психофізіологічних особливостей людини (див. табл. 1.2), таким даним та інформаційному контенту, який вони несуть, притаманні певна неоднозначність, елементи припущень, прогнозування і т. п. Таке спостерігається в доповідях, описах, оглядах та ще в багатьох інших інформаційно-аналітичних продуктах, що створюються в процесі пізнавальної діяльності людини, циркулюють в комп’ютерних мережах, наводяться в засобах масової інформації тощо. Подібні дані вважають «м’якими».

Характерними прикладами «м'яких» даних є повідомлення та текстові відомості від HUMINT, матеріали OSINT, зокрема, аудіо- та відеоматеріали, зображення та ін. М'які джерела і дані принципово відрізняються тим, що їх інформаційний контент має тенденцію бути більш якісним і вимагає значного контексту для інтерпретації. «М'які» джерела інформації передбачають присутність людини у аналітичному ланцюжку. Але треба враховувати, що люди орієнтуються за своєю природою на якісні моделі для представлення реального світу і документують свої відомості з використанням контекстно-залежних мов, тому вони неминуче вводять в свої описи суб'єктивний зміст. Безумовно, інформація від людини високо цінується, особливо в складних ситуаціях, але разом з тим відзначимо, що людський елемент м'яких джерел інформації ускладнює роботу автоматизованих систем оброблення інформації [14–16].

Приклади «чітких» та «м'яких» даних та елементів інформації щодо об’єктів і процесів, які входять до сфери інтересів, наведено в табл. 1.3.

Таблиця 1.3. Приклади «чітких» і «м'яких» даних та елементів інформації

| **Дані та елементи інформації** | **Опис** | **Hard** | **Soft** |
|---|---|---|---|
| Час | Момент виникнення або виявлення, тривалість дії, період здійснення (чогось) | ▲ | |
| Місцеположення | Просторові координати, розташування об’єкта | ▲ | |
| Маршрут | Сукупність корельованих у часі–просторі послідовностей розташування об’єкта | ▲ | ▲ |
| Колір | Колориметричні властивості об’єкта | ▲ | ▲ |
| Протяжність | Об’єм або частина реального фізичного простору, що обіймає об’єкт | ▲ | ▲ |
| Атрибути | Ознаки, що відображають типологію об’єктів, | ▲ | ▲ |

| Дані та елементи інформації | Опис | Hard | Soft |
|---|---|---|---|
| | характеризують їхні унікальні властивості (вид, тип, клас, підклас тощо) | | |
| Спектральні сигнатури | Розподіл відбивальних або випромінювальних властивостей об'єкта, робочі частоти випромінювань | ▲ | |
| Асоціації | Взаємовідношення між об'єктами, процесами, явищами, стосунки між акторами (персонами розробки, установами, відомствами тощо) | ▲ | ▲ |
| Персональна інформація | Імена, прізвища, біографічні відомості, характеристики особистостей, зв'язки , інший фактографічний матеріал | | ▲ |
| Загальні оцінки | Огляди, оцінки, висновки відносно поточної ситуації та шляхів її розвитку, думки щодо перспектив | | ▲ |

В процесі розгляду та вивчення інформації Аналітик формулює гіпотези щодо визначених об'єктів інформаційного поля, й далі задача складається у тому, щоб визначити найбільш ймовірні гіпотези. Багато років і донедавна для визначення і обґрунтування таких гіпотез застосовувались переважно методи теорії ймовірності [8,12], але внаслідок того, що вимоги до вхідних даних тут доволі суворі, в останні часи інтенсивно вивчаються можливості принципово інших підходів, зокрема, теорії нечітких множин, ТСДШ [9–11] та ін.

Одна з важливих особливостей ТСДШ у тому, що, на відміну від теорії ймовірності, тут можуть розглядатись так звані складні гіпотези. Складною є гіпотеза, елементами якої є кілька інших гіпотез. Припустимо, θ – основа аналізу, Θ={a, b, c, d, e}, де a-e – п'ять різних гіпотез, кожна з яких має свою ймовірність підтвердження в реальному світі. Тоді, наприклад, гіпотези a та d можуть бути об'єднані в одну гіпотезу f = (a, d), яка розглядається як складна і має деяку свою ймовірність. Складні гіпотези виникають, в основному, як результат багатоальтернативних оцінок, до яких схильні людина та інші джерела «м'яких» даних. Математичний апарат ТСДШ дозволяє обробляти сукупності з простих та складних гіпотез і знаходити серед них найімовірніші.

Припустимо, по визначеному об'єкту працюють одночасно людина і деякий технічний засіб. Кожний з них надає незалежно від іншого свою інформацію, на базі якої формується відповідна основа аналізу з певних гіпотез. Позначимо ті основи аналізу як $\theta_1$ і $\theta_2$. У загальному випадку обидві основи аналізу можуть: 1) складатись з одних і тих гіпотез: $\theta_1 = \theta_2$; 2) містити обмежену кількість однакових гіпотез: $\theta_1 \neq \theta_2$; $\theta_1 \cap \theta_2 \neq \emptyset$; 3) складатись із зовсім різних гіпотез: $\theta_1 \neq \theta_2$; $\theta_1 \cap \theta_2 = \emptyset$.

Названі ситуації графічно відображені на рис. 1.6.

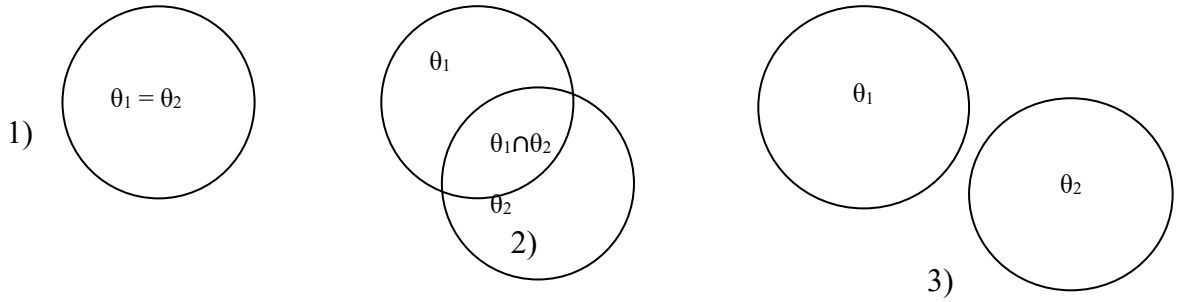



Рис. 1.6. Варіанти взаємовідношень між основами аналізу, які формуються різними джерелами

На випадок, коли основи аналізу всіх інформаційних джерел співпадають, в ТСДШ розроблено просте правило (так зване комбінаційне правило Демпстера), яке дозволяє об'єднати і звести всі існуючі сукупності гіпотез до однієї підсумкової сукупності гіпотез і обчислити ймовірність кожної з них. Однак досвід застосування правила Демпстера в розрахунках показує, що воно може приводити до невірних результатів, коли деякі дві гіпотези суперечать одна одній, а також тоді, коли хоча б одне джерело присвоює якійсь гіпотезі нульову ймовірність. Удосконалені формули для комбінування гіпотез від різних джерел, які допомагають вирішувати зазначені проблеми, а також враховують корельованість джерел.

Вище, в таблиці 1.1, серед параметрів якості первинних відомостей було вказано їх надійність, тобто відповідність оцінок, які даються джерелом, об'єктивній реальності. Різні джерела можуть мати неоднакову надійність і, безумовно, цей чинник бажано враховувати в процесі роботи з інформацією. Відзначимо, що в інструментарії ТСДШ є спеціальна процедура (discounting), яка дозволяє вводити в розрахунки надійність джерел даних.

Математичний апарат ТСДШ дозволяє розширити, у порівнянні з теорією ймовірності, набір параметрів, якими оцінюються властивості інформації. Так, в ТСДШ точкова оцінка ймовірності гіпотези доповнюється функціями довіри і правдоподібності. Використовуючи ці функції, можна конструювати нові, нетрадиційні критерії прийняття рішень. Одним з таких критеріїв є пігністична ймовірність.

*Класифікація джерел інформації.* Розглянуті вище джерела інформації зумовлюють використання різних технічних і людських ресурсів, а тому бувають об'єктивними чи суб'єктивними. Проаналізуємо їх більш докладніше.

Об'єктивні джерела добувають інформацію в результаті вимірювання та кількісного оцінювання фізичних властивостей об'єктів інтересу (ОІ) з певними помилками і відхиленнями. Такі дані достатньо формалізовані і можуть застосовуватися в математичному апараті для здійснення розрахунків, а надалі ефективно використовуватися в напівавтоматичних або автоматичних системах оброблення інформації.

Прикладами технічних об'єктивних джерел інформації є дані, добуті за допомогою з фото-, відео-, радіо-, аудіо-, інфрачервоних засобів, це дані геопросторових джерел, сигнали датчиків і інших вимірювальних пристроїв.

Особи також можуть бути оснащеними засобами для глобального позиціонування, наприклад, GPS-приймачами (рис. 1.7).

Суб'єктивні джерела принципово відрізняються тим, що надана ними інформація в більшості випадків має якісний, а не кількісний характер і для інтерпретації потребує від аналітика розуміння ситуації довкола ОІ. Джерела суб'єктивної інформації, за визначенням, передбачають етап спостереження та оцінювання людиною певних процесів або явищ. Оскільки оцінка людини є по суті є якісним показником, то для її формального опису слід використовувати відповідні моделі з використанням контекстно-залежних мов (наприклад, мови ділового спілкування, протоколу складання листів, міміка та емоції в спілкуванні, мова тіла тощо). Це зумовлює введення суб'єктивності в опис ОІ. Серед джерел інформації слід назвати тексти сайтів, блогів, соціальних мереж, БД та ін.

| Інформація від людей | Інформація з відкритих джерел | Інформація технічних видів спостереження | Інформація засобів видового спостереження | Інформація інших технічних видів спостереження |
|---|---|---|---|---|
| - записи;<br>- інформаційні звіти;<br>- звіти патрульних служб;<br>- використання інформації про зв'язки та взаємовідносини осіб;<br>- координати об'єктів | - оцінювання політичної ситуації та менталітету населення;<br>- аналіз трансляцій по радіо та ТБ, сайтів;<br>- координати об'єктів | - перехоплення розмов, фото-, відеоматеріалів;<br>- частоти та потужність сигналів;<br>- координати джерел розповсюдження сигналів | - зйомка БПЛА;<br>- фото-, відео- та аерозйомка;<br>- космічна зйомка;<br>- інформація про розмі-щення техніч-них засобів та будівель | - сейсмічна, хімічна, бактеріологічна тощо |

Об'єктивна інформація

Суб'єктивна інформація

Рис.1.7. Розподіл інформації на об'єктивну та суб'єктивну за видами джерел

Жодне з джерел інформації не може забезпечити повний та об'єктивний контроль за об'єктом, ситуацією або явищем протягом тривалого часу. Тому поєднання й сумісне використання суб'єктивної і об'єктивної інформації може бути дуже корисним (рис. 1.8) [4,5]. Збір, накопичення та інтеграція таких даних є ключем до підвищення ступеня обізнаності споживачів про ситуацію на ОІ.

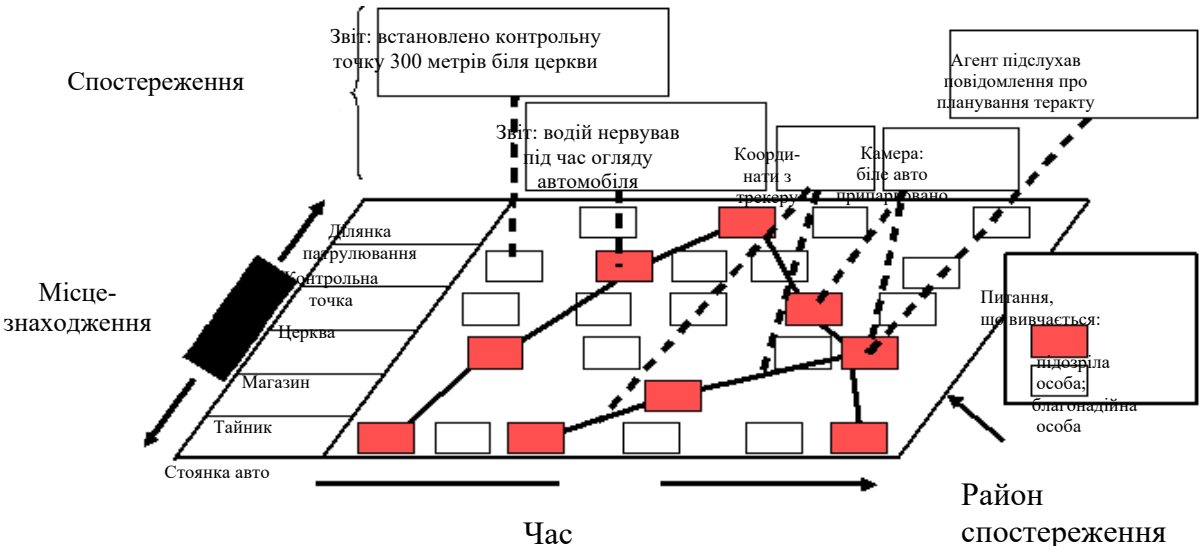



Рис. 1.8. Приклад аналізу ситуації з використанням різнотипної інформації

Наприклад, у польовому статуті США FM 3–24 (*https://fas.org/irp/doddir/army/fm3-24.pdf*) щодо заколотів та протидії ним, визначається, що необхідною умовою успішного здійснення антиповстанських операцій є відстеження діяльності сотні або тисячі осіб, зважаючи на локальність та динамічність розвитку подій.

У польовому статуті США FM 2-0 (*https://fas.org/irp/doddir/army/fm2-0.pdf*) щодо ведення розвідки визначається необхідність комплексного застосування різних видів розвідки «all-source intelligence» для надання інформації споживачу.

## 1.4. Технології системного зведеного аналізу інформації від різнотипних джерел

Для вирішення поставлених проблем та реалізації розглянутих вище підходів щодо їх вирішення на практиці, розроблено достатньо багато апаратних та програмних рішень як на відкритій, так і на комерційній основі [6,7]. Розглянемо деякі з них докладніше.

*Рішення з відкритим кодом.* Базовою архітектурою обробки великих даних вважають в *SN*-архітектуру, яка забезпечує масивно-паралельну обробку даних, з використанням технологій зберігання даних *NoSQL*, програмного інтерфейсу *MapReduce*, платформи *Hadoop*, мови програмування *R* та ін.

Зараз все більш популярною стає модель роботи з *Big Data*, яка реалізована в проекті *Apache Software Foundation – Apache Hadoop*. *Apache Hadoop* складається з двох компонентів: це розподілена кластерна система *Hadoop Distributed File System (HDFS)* і програмний інтерфейс *Map Reduce*. В основі моделі роботи *Apache Hadoop* лежать три основних принципи. По-перше, дані рівномірно розподіляються на внутрішніх дисках безлічі серверів, об'єднаних *HDFS*. По-друге, не дані передаються програмі обробки,

а програма – до даних. Третій принцип – дані обробляються паралельно, причому ця можливість закладена архітектурно в програмному інтерфейсі *Map Reduce*.

Також існують і інші технології з відкритим вихідним кодом (*open source*), які розробляються *Apache Software Foundation* і доповнюють *Hadoop*: мова опису програм *Pig*, що аналізує великі набори даних; рішення для організації сховищ даних *Hive*; середовище зберігання даних *HBase*; служба переносу даних *Flume*; бібліотека пошукової системи *Lucene*; технологія послідовного впорядкування даних *Avro*; служба синхронізації *ZooKeeper*; система планування потокової обробки завдань *Oozie*.

*Комерційні рішення.* Існує ряд апаратно-програмних комплексів, що надають наперед налаштовані рішення для обробки великих даних: *Aster MapReduce Appliance* (корпорації *Teradata*), *Oracle Big Data Appliance*, *Greenplum Appliance*. Ці комплекси поставляються як готові до установки в телекомунікаційні шафи центрів обробки даних (ЦОД), містять кластер серверів і програмне забезпечення (ПЗ) для масово-паралельної обробки.

Апаратні рішення для аналітичної обробки в оперативній пам'яті представлені апаратно-програмними комплексами *Hana* (наперед налаштоване апаратно-програмне рішення компанії *SAP*) і *Exalytics* (комплекс компанії *Oracle* на основі реляційної системи *Timesten* і багатовимірної системи *Essbase*).

Крім того іноді до рішень для великих даних відносять і апаратно-програмні комплекси на основі традиційних реляційних систем управління базами даних (СУБД) – *Netezza, Teradata, Exadata*, як здатні ефективно обробляти терабайти і ексабайти структурованої інформації, вирішуючи завдання швидкої пошукової та аналітичної обробки величезних обсягів структурованих даних. Апаратні рішення *DAS* – систем зберігання даних (СЗД), безпосередньо приєднаних до вузлів – в умовах незалежності вузлів обробки в *SN*-архітектурі також іноді відносять до технологій великих даних.

*Виробники програмно-апаратних комплексів Big Data.* Це світові лідери в області СУБД, систем статистичного аналізу, систем зберегания і обробки даних: *Cloudera, Dell EMC, Hitachi Data Systems Corporation, Oracle, IBM, Informatica, QlikView, Teradata*.

*Oracle Corporation* – корпорація, найбільший в світі розробник ПЗ для організацій, постачальник серверного устаткування. Продукти: платформа для зберігання, обробки та інтеграції великих даних *Oracle Big Data Appliance*, платформа агрегації та аналізу даних *Oracle Exadata*, інструменти аналізу даних *Oracle Exalytics Database Machine*.

*IBM* – один з найбільших в світі виробників і постачальників апаратного і ПЗ, а також IT-сервісів і консалтингових послуг. Продукти: програмно-апаратні комплекси *IBM Netezza*, платформа *IBM Big Data*, рішення для обробки потоків даних *InfoSphere Streams*, рішення для зберігання і обробки неструктурованих даних *BigInsights*, рішення для аналізу даних *IBM Predictive Analytics*.

*Informatica* – компанія, розробник ПЗ для інтеграції даних, основні функціональні призначення продуктів компанії – це керування якістю даних, управління основними даними, управління життєвим циклом інформації. Продукти: *Informatica Big Data Edition, Big Data Parser, Vibe Data Stream for Machine Data, MDM, Data Masking, Data Archive*.

*Dell EMC* – американська мультинаціональна корпорація, яка спеціалізується на СЗД, інформаційної безпеки, віртуалізації, аналітиці, хмарних обчисленнях та інших продуктах та послугах, які дозволяють компаніям зберігати, керувати, захищати та аналізувати дані.

*Hitachi Data Systems Corporation* ‑ компанія, що пропонує інструменти для зберегання даних, управління даними, оптимізації ресурсів зберігання і продуктивності системи для середовища «великих даних» на базі продуктів *Virtual Storage Platform, Hitachi Unified Storage 100, Hitachi Unified Storage VM.* Також пропонує спеціалізовані рішення для роботи з файловими даними *HNAS*, платформи для хмарного зберігання та консолідації неструктурованих даних (зокрема, *Hitachi Content Platform* та спеціалізоване ПЗ для управління апаратними ресурсами *Hitachi Command Suite* та вирішення інших завдань (зокрема, для резервного копіювання – *Hitachi Data Protection Suite*).

*Cloudera* – компанія, розробник ПЗ, випускає комерційну версію *Apache Hadoop-Hadoop for the Enterprise*.

*Qlik Technologies* – компанія-розробник ПЗ для систем *Business Intelligence*. Основний продукт – програмна *BI*-платформа *QlikView* для асоціативного пошуку та обробки обчислень в оперативній пам'яті.

*Teradata* – корпорація, що спеціалізується на розробці та постачання апаратно-програмних комплексів для обробки та аналізу даних. Продукти для роботи з великими даними: *Teradata Database, Teradata Unified Data Architecture, Teradata Analytical Ecosystem, Teradata Active Data Warehouse Private Cloud, Teradata Data Lab, Teradata Integrated Analytics*.

Окремо серед поширених інструментів інтеграції даних слід відмітити: *Alteryx, Analytics Canvas, DataWatch, Denodo Platform, HiperFabric, Lavastorm, ParseKit, Paxata, RapidMiner Studio, Jboss, Safe FME, Azure Data Factory (ADF), SQL Server Integration Services (SSIS)* та багато інших.

Серед найбільш поширених програмних продуктів аналізу та інтеграції даних слід зазначити такі:

*CTS Sentinel Visualizer Link Analysis* – ПЗ американської компанії «FMS, Inc.». Дозволяє здійснювати аналіз та виявлення зв’язків у банку даних, соціальний мережений аналіз, візуалізацію отриманих результатів, інтеграцію геопросторової інформації.

*IBM i2 Analyst's Notebook* – ПЗ американської компанії «IBM». Продукт є візуальним аналітичним середовищем, яке дозволяє максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами. Завдяки інтуїтивно зрозумілому інтерфейсу з урахуванням контексту дозволяє аналітикам швидко співставляти, аналізувати і наочно представляти дані з різних джерел. IBM i2 Analyst's

Notebook надає актуальні і дієві аналітичні засоби, що допомагають виявляти, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність.

*HunchLab* – ПЗ американської компанії «Azavea», являє собою аналітично-прогнозний інструмент у сфері попередження та розслідування злочинності. Включає можливості аналізу географічних даних.

*Crime Tech Solutions' Case Closed Software* – ПЗ датської компанії «Crime Tech Solutions», розроблено колишніми представниками правоохоронних органів, з основною спеціалізацією аналізу та представлення даних в інтересах правоохоронної сфери.

*Wynyard Advanced Crime Analytics* – ПЗ британської компанії «Wynyard Group». Дозволяє аналізувати великі обсяги даних, виявляти інформацію необхідну для розкриття злочинів іншої протиправної діяльності. Має можливості візуалізації даних, а також можливості аналізу неструктурованих даних (текстові дані, дані засобів масової інформації (ЗМІ) тощо).

*Link Explorer* – ПЗ британської компанії «Xanalys Limited». Продукт визначається як аналітичний інструмент проведення розслідувань. Дозволяє аналізувати інформацію, встановлювати взаємозвєязки та представляти результати аналізу у вигляді візуалізованих діаграм, часових графіків, геопросторової інформації.

*AllegroGraph* – ПЗ американської компанії «Franz Inc.», що є комерційним продуктом аналізу даних. Використовується зокрема у деяких проектах Міністерства Оборони США.

*Commetrix CMX Analyzer* – ПЗ німецької компанії «Trilexis», що дозволяє здійснювати аналіз банку даних, вибудовувати логічні взаємозв'язки між об'єктами дослідження представляти наочну картину результатів роботи.

*Graph Commons* – ПЗ американської компанії «Graph Commons», яке дозволяє здійснювати аналіз та візуалізацію його результатів щодо зв'язків суб'єктів дослідження.

*Data Clarity Platform Law Enforcement* – ПЗоз американської корпорації «Raytheon». Спеціалізоване на аналізі зв'язків, геопросторових даних, темпоральному аналізі даних. Слід зазначити, що компанія «Raytheon» є одним з постачальників озброєння та військової техніки (ОВТ) для потреб збройних сил США.

*Smart Visual Analytics Tool (SVAT)* – ПЗ чеської компанії «Profinit», якій має можливості аналізу соціальних мереж, добування текстових даних, візуалізації результатів дослідження.

*The Open Graph Viz Platform* – ПЗ французької компанії «Gephi Consortium», який має можливості візуалізації даних, побудови графіків та пов'язаних мереж на основі обробки даних (функціонує на основі ОС Windows, Mac OS X та Linux).

Незважаючи на достатньо широкий перелік програмних продуктів, які представлені на ринку, вони значно різняться функціональними можливостями. Зокрема, серед найбільш важливих критерії розглядається

імпорт та експорт даних, можливість побудови мережених діаграм, можливість аналізу інформації з соціальних мереж, а також можливість інтеграції даних з системами геопросторового аналізу.

### 1.5. Моделювання системи зведеного аналізу інформації від різнотипних джерел

Для вирішення задач системного зведеного аналізу необхідно розробити загальну модель, яка б забезпечувала ефективну взаємодію різних аналітичних та добувних підсистем [5,7,8,10,13]. Комплексування різнорідної інформації у ході вирішення фахових завдань є важливим науково-практичним питанням, що потребує розробки теоретичних підходів до інтеграції даних та ефективних алгоритмів інтеграції.

Базою для створення системи зведеного аналізу інформації є комплексна оцінка потреб її користувачів, в якій має бути враховано таке [4,15,16]:

- задачі користувачів та необхідні для їх реалізації дані;
- гарантування якості інформації, що надається користувачам (стандарти);
- застосування ітеративного життєвого циклу розробки системи інтеграції, що дозволить своєчасно коригувати її архітектуру відповідно до потреб користувачів; гнучке управління змінами в системі, яких потребують користувачі; документування потреб користувачів;
- залежність структури даних, апаратно-програмного забезпечення і технологічних рішень від архітектури системи; широке використання відповідних стандартів.

Створення моделі системи має здійснюватися за такими принципами:

- базування на відкритих стандартах і специфікаціях, прозорість даних/сервісів для користувачів, можливість удосконалення ресурсів системи шляхом залучення до цього процесу всіх учасників системи;
- забезпечення своєчасного доступу до інформаційних ресурсів;
- захист інформації;
- спільне підтримання системи користувачами в робочому стані в процесі її експлуатації;
- самоорганізація користувачів для внесення інформаційного вкладу в систему;
- мінімальні витрати на централізоване управління.

Для вирішення зазначених вище проблем використання розподіленої в просторі різнорідної інформації від багатьох джерел пропонується створити систему зведеного аналізу інформації від різнотипних джерел. Модель системи побудовано на основі широко відомої архітектури SOA, орієнтованої на сервіси [7]. Відповідно до цієї моделі попередньо для

всіх даних необхідно створити бази метаданих на основі профілів відповідних стандартів. Крім того, передбачено реалізацію базових сервісів для перетворення даних, щоб компенсувати вплив різних видів даних.

Модель передбачає використання таких сервісів: перетворення форматів даних, узгодження семантики даних, узгодження зв'язку між даними, узгодження структури метаданих, генералізації, управління версіями даних, інтеграція моделей даних, кодування, перетворення систем координат та ін. (рис. 1.9).

*Система зведеного аналізу інформації працює наступним чином.* На основі баз метаданих, бібліотек алгоритмів обробки різнорідних даних, стандартів (профілів стандартів) і нормативних документів, а також власних знань і досвіду, в результаті інтерактивної взаємодії з модулем визначення алгоритму інтеграції, користувачі вибирають процедуру обробки різнорідних даних, яка найкраще відповідає характеру конкретної задачі інтеграції і типам даних.

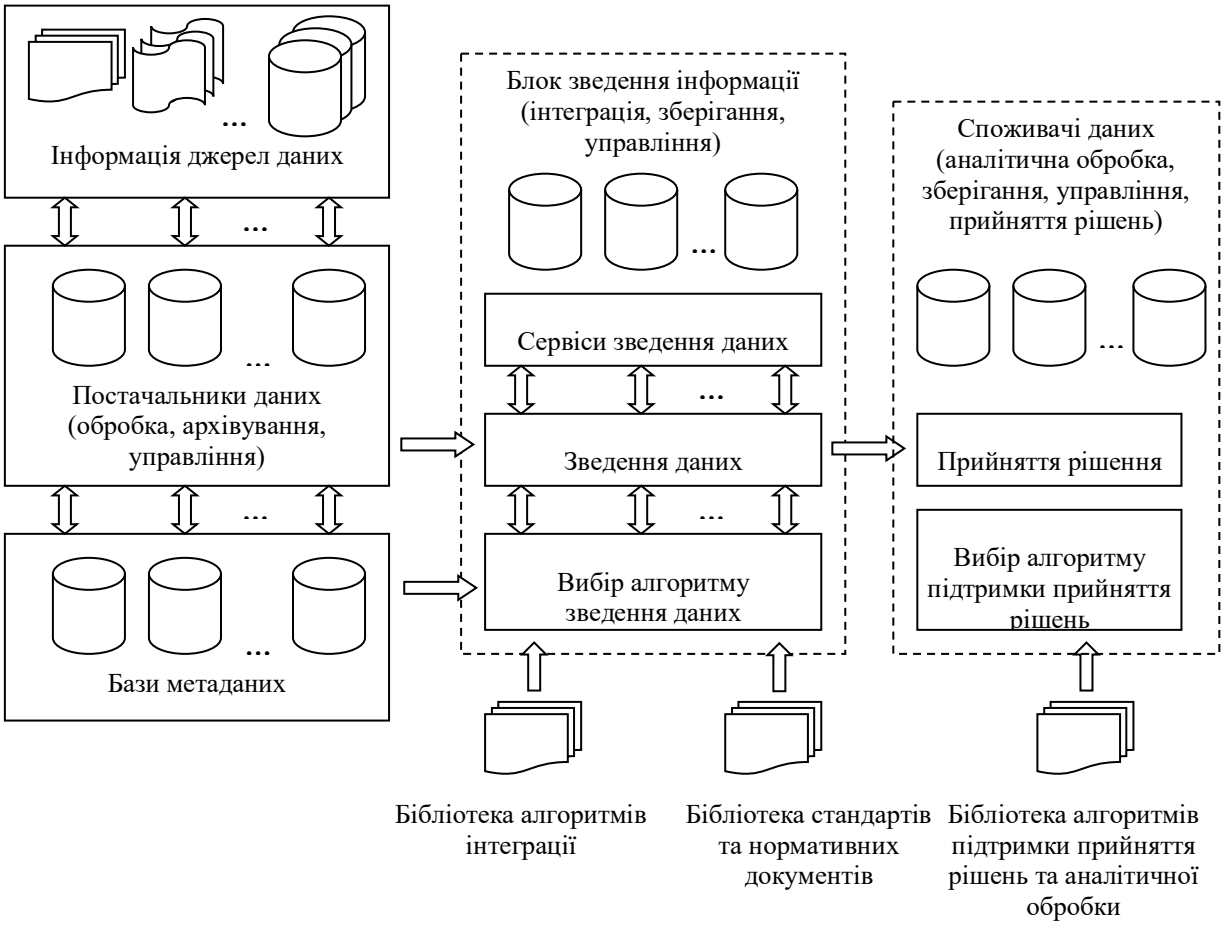



Рис. 1.9. Загальна модель системи зведеного аналізу РІ

Модуль вибору алгоритму інтеграції передає в модуль інтеграції даних обраний алгоритм, викликаються необхідні для його реалізації сервіси і виконується процедура інтеграції. Після завершення обраного

алгоритму в модулі інтеграції даних інтегровані дані стають доступними користувачам.

Для обґрунтування складу джерел інформації з урахуванням змін характеру завдань потрібно розробити відповідний науково-методичний апарат. Критерієм вибору джерел інформації може бути мінімальний ресурс на виконання задачі в певних умовах. Змістовна постановка задачі щодо визначення складу джерел полягає в пошуку мінімальної їх кількості, яка б забезпечувала вирішення задачі з необхідним рівнем ефективності.

Задача вибору джерел пов’язана зі складними математичними обчисленнями, що зумовлено недостатньою обґрунтованістю показників ефективності, необхідністю врахування великого обсягу різноманітної та суперечливої інформації.

Розробка алгоритмів зведення інформації потребує певної методологічної платформи, в якій базовими є методи теорії імовірності та Байесова модель [12], теорії нечітких множин та ТСДШ [9–11], теорія інтервальних обчислень [17–21], когнітивна теорія [15]. Оскільки процес аналітики в сучасних умовах є статистично нестійким, то для вирішення задачі вибору сил та засобів неможливо коректно використовувати методи теорії ймовірностей та математичної статистики.

Для опису процесу в різних умовах обстановки пропонуємо застосовувати теорію нечітких множин та нечіткої логіки, яка, на відміну від ймовірнісної теорії, дає змогу враховувати та математично описувати недостатньо визначені поняття, що характеризують умови обстановки та показники, оперувати ними та робити висновки, зрозумілі для сприйняття особою, що приймає рішення [22–25].

Вибір конкретної методологічної платформи залежить від обсягів статистичних даних та вибірок, необхідності обробляти неточні дані, інформацію від пов’язаних між собою джерел та експертних оцінок. За умов невизначеності ситуації навколо об’єктів інтересу пропонуємо використовувати алгоритми інтеграції на основі теорії свідчень Демпстера- Шейфера.

Точкою входу в систему є портал. Він забезпечує прозору для користувача взаємодію з ресурсами різного рівня, що дає змогу за запитом отримувати інформацію. Портал безпосередньо пов'язаний з сервісами високого рівня. Високорівневі сервіси (планування завдань, організація виконання складного потоку запитів, інтегрування даних, паралельна обробка, використання спеціалізованого програмного забезпечення), для функціонування яких потрібні великі обчислювальні ресурси, мають взаємодіяти із сервісами низького рівня. Ці сервіси призначені для планування і розподілу завдань за обчислювальними ресурсами.

Інфраструктура системи зведеного аналізу інформації має включати

в себе такі спеціалізовані компоненти, як інфраструктура безпеки, підтримання протоколу передачі даних, надання ресурсів та управління ними, система зберігання сертифікатів та управління повноваженнями, система позиціонування реплік, система організації загального доступу до даних.

В ієрархії сервісів найнижчий рівень формують сервіси спеціалізованих серверів та баз даних: віддалене сховище даних; операційне сховище даних; підсистема обчислень; сервер БД. Стандартизованість і сумісність різнорівневих компонентів дають змогу у разі потреби масштабувати систему, при цьому складність взаємодії окремих підсистем прихована від користувача.

*Багаторівнева модель зведеного аналізу інформації від різнотипних джерел на основі моделі JDL.* Інтеграція суб'єктивної (СІ) та об'єктивної інформації (ОІ) має здійснюватися в декілька етапів на різних рівнях оброблення інформації, а безпосередній процес інтеграції може бути описаним з використанням однієї з відомих моделей інтеграції, а саме: *Joint Directors of Laboratories (JDL), TRIP, Omnibus, Dasarathy, Recognition Primed Decision-Making, OODA* та ін. [26].

На рис. 1.10 зображено модель *JDL*, яку пропонується використовувати для інтеграції інформації.

Основна мета інтеграції першого рівня – відстежити й ідентифікувати окремі цілі. Спостерігаючи за станом ОР, наприклад, його положенням чи швидкістю, визначаючи зовнішні ознаки (наприклад, розмір), технічні засоби забезпечують необхідною інформацією, яка може бути пов'язана зі складанням маршруту пересування та станом інших об'єктів.

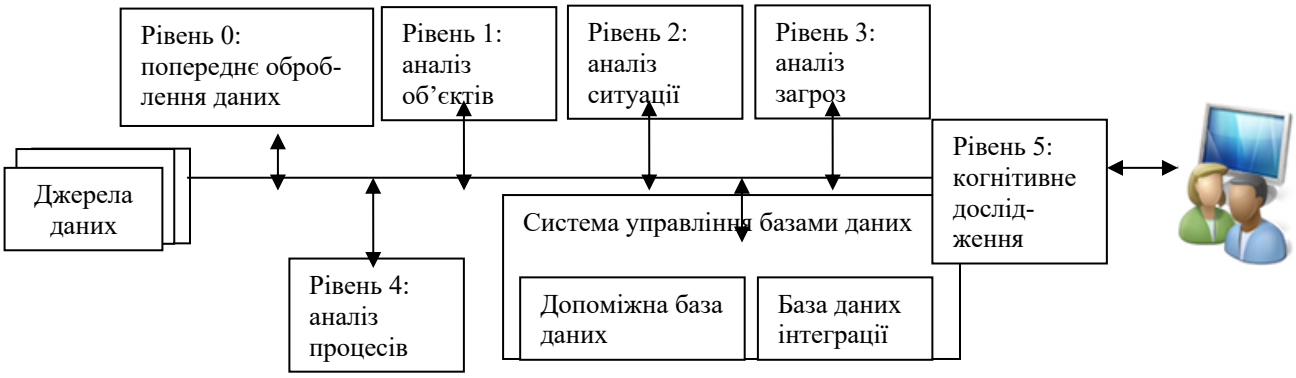



Рис. 1.10. Багаторівнева модель зведеного аналізу інформації від різнотипних джерел

Метою другого рівня інтеграції є визначення поведінки суб'єктів і відносин між ними. Оскільки поведінка і ставлення до оточення є СІ, то інтеграція другого рівня завжди передбачає поєднання різнорідної СІ. Проте об'єктивні дані також відіграють важливу роль в інтеграції даних другого рівня.

*Вимоги до процесу інтеграції РІ.* Для того щоб процес інтеграції був ефективним, алгоритми оброблення інформації мають оперувати наборами даних різнорідних джерел, крім того, результати роботи повинні у контрольних точках збігатися з еталонними значеннями та корелюватися. Після збору ОІ і СІ дані слід організувати таким чином, щоб вони були зручними для інтеграції та аналізу. У таблиці 1.4 наведено вимоги до наборів даних, необхідних для оброблення та інтеграції РІ.

Для того щоб сформувати набір реалістичних даних, визначених у контрольованому середовищі, вихідні дані слід збирати під час тренувальних вправ та навчань. Наприклад, ОІ можна отримати в результаті спостереження за виконанням вправ із використанням технічних засобів (камер спостереження, трекерів, GPS-приймачів, інфрачервоних датчиків, систем сигналізації та охорони, радіолокаторів, радіосканерів тощо). Об'єктивна інформація має бути прив'язаною до географічних координат і показників часу, для подальшого співставлення та інтеграції.

Суб'єктивна інформація може бути зібраною в результаті створення нестандартних ситуацій, залучення «незалежних» спостерігачів. Саме їм може бути поставлено завдання щодо отримання напівструктурованих даних завдяки заповнення опитувальних листів під час виконання вправ. Такий опитувальний лист може містити в собі інформацію про те, хто виконував вправу, який характер вправи, що виконується, мета виконання вправи, час її виконання, особливості місця проведення, загальної обстановки в районі проведення, яке джерело інформації (спостерігач, матеріали спостереження, звіти тощо) та інші додаткові дані.

Таблиця 1.4. Вимоги до вхідних даних

| **Вимоги** | **Стислий опис** |
|---|---|
| Інформація про ОР має бути реалістичною. | Інформація повинна стосуватися ОР. Вона може бути неповною, що цілком характерно для ситуації в місті. |
| ОР не оцінюються вийнятково одним видом інформації (об'єктивним чи суб'єктивним). | Під час інтеграції інформації мають застосовуватися різні види інформації одночасно. |
| Має існувати можливість перевірити інформацію, що надходить від різних джерел, на достовірність. | Оцінювання якості алгоритмів здійснюється тільки за умов, якщо вхідний набір даних та результати роботи можна порівняти з істинними значеннями. У реальних ситуаціях це складно зробити або взагалі неможливо. Тому як істинні значення слід використати дані, зібрані під час проведення навчальних вправ та натурних експериментів. |
| Обсяг даних для аналізу має бути достатньо повним. | Перевантаження зайвою інформацією часто спостерігається під час проведення операцій, тому в ході формування набору даних для інтеграції слід зважати на цей аспект. Додаткова та різнопланова інформація робить аналіз інформації повнішим. |

*Вимоги до алгоритмів оброблення та інтеграції РІ.* Об'єктивні методи інтеграції інформації мають містити такі чотири основні складові: методи семантичного оброблення інформації; методи отримання і представлення даних; характеристики та параметри джерел на основі їх моделей; набір алгоритмічного забезпечення для оброблення даних. Суб'єктивні методи мають схожі компоненти (рис. 1.11).

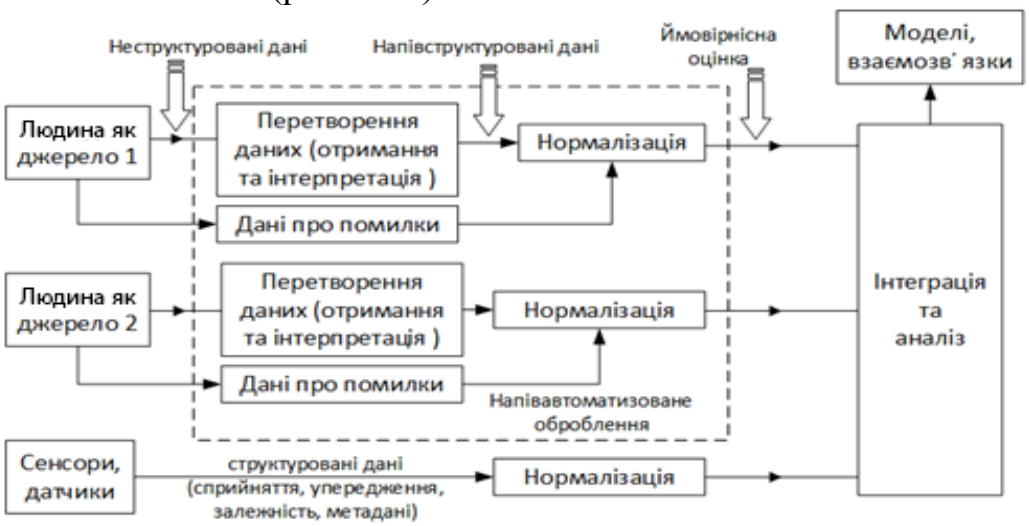
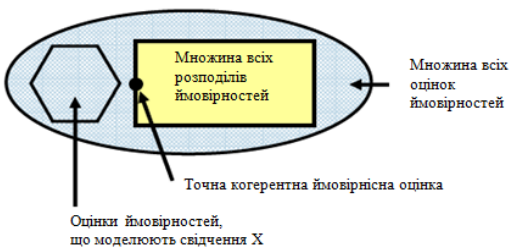



Рис. 1.11. Модель нормалізації та інтегрування різнотипної інформації

*Особливості семантичного оброблення суб'єктивної РІ.* Апарат ймовірнісної логіки може бути використаним для формалізованого опису СІ, за аналогією з моделлю інтерпретації (класифікації) фактів, отриманих з об'єктивних джерел інформації, що є умовним розподілом ймовірності у відповідному ймовірнісному просторі.

Пропонується використовувати суб'єктивну ймовірність, яка інтерпретує кожне твердження як визначення афінної множини оцінок ймовірностей. На основі цього свідчення X може представлятися у вигляді набору оцінок ймовірностей, які не є розподілом ймовірностей, як показано на рис. 1.12.а. Свідчення Y може трактуватися як порівняльна ймовірність, що є частиною бінарного відношення і визначається афінною множиною оцінок ймовірностей. На рис. 1.12б показано формалізовану модель свідчення Y. Існує і розгалуженіша теорія для оцінювання умовних ймовірностей.




*1.12а. Випадок незв'язного (некогерентного) оцінювання ймовірностей*


*12б. Випадок зв'язного (когерентного) оцінювання ймовірностей.*

Рис.1.12. Формалізований опис суб'єктивних джерел інформації

*Параметри моделі інтеграції PI.* Параметри, які використовуються для інтеграції інформації, включають у себе таке: параметри об'єктів, що змінюються в часі; взаємозв'язки між параметрами; кількісні значення параметрів, що можуть бути отримані під час спостережень. По суті, це координати об'єктів та кількість зв'язків у соціальних мережах. Узагальнений вигляд стану об'єкта можна представити як схему даних (схему бази даних), приклад якої наведено нижче.

$$\begin{Bmatrix} Об'єкт = (ID, Зв'язки, координати, ...) \\ Зв'язки = (Зв'язки, ID) \\ ... \end{Bmatrix}$$

Як і у схемі БД, будуються обмеження цілісності даних про стан об'єкта (обмеження виду, функціональні залежності, обмеження переходу тощо). Знання експертів у предметній галузі і різні методи створення моделей будуть необхідними для визначення імен, синтаксису схеми даних і обмежень цілісності, які адекватно представляють проблемну зону.

*Вимоги до алгоритмічного забезпечення інтеграції PI.* Після того як буде здійснено загальну інтерпретацію СІ та ОІ, постане проблема оброблення й інтеграції наявної інформації. Процес інтеграції СІ і ОІ може бути представлений як обчислювальна задача для сучасних і перспективних алгоритмів. Для її розв'язання слід використовувати алгоритми на основі теорії Байєса, Демпстера-Шейфера, Дезерта-Смарандаке для інтеграції PI з об'єктивних джерел, з подальшою інтеграцією з СІ когерентних джерел (рис. 1.13). Після цього доцільно обрати інтегрований розподіл ймовірностей за визначеним критерієм.

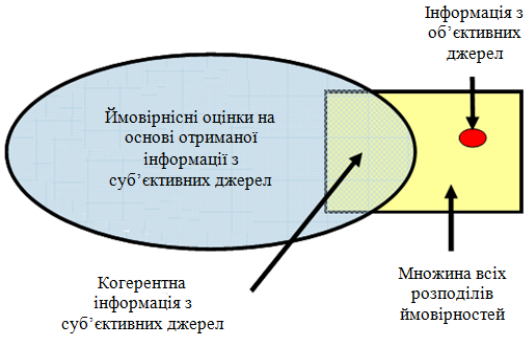



Рис. 1.13. Схема інтеграції інформації з об'єктивних та суб'єктивних джерел

Аналіз сучасного математичного апарату інтеграції інформації з різних джерел свідчить про наступне:

- теорія ймовірностей має обмежені можливості застосування оскільки події та факти про об'єкт не завжди відповідають вимогам до обсягів

статистичних даних та вибірок, статистичні методи не дозволяють обробляти незнання, існують певні труднощі з обробленням даних від корельованих джерел;

- в теорії нечітких множин простежується суб'єктивний фактор при використанні функції належності, що потребує експертних оцінок;
- найбільш узагальненою методологічною платформою на сьогодні є ТСДШ, яка є узагальненням статистичної теорії і позбавлена зазначених вище недоліків.

Теорія свідчень дозволяє обробляти неповну і неточну інформацію, а також давати оцінку джерела інформації. Однією з особливостей даної теорії є необхідність визначення коефіцієнта впевненості при комбінуванні оцінок незалежних експертів. Недосконалість правила комбінування Демпстера призвела до появи альтернативних правил, які доцільно використовувати за певних умов.

Так використання правила комбінування Демпстера при умові, що всі свідоцтва мають протиріччя, не є коректним. Також не враховується інформація, що отримана з конфліктуючих та ненадійних джерел. Проведений аналіз альтернативних правил комбінування (Сметса, Ягера, Інагакі, Жанга, Дюбуа, Прада, усереднення основних значень ймовірностей) свідчить про часткове усунення недоліків використання класичного правила комбінування Демпстера. Проте зазначені правила не дозволяють враховувати знання (метадані) про характеристики джерел: достовірність, релевантність, надійність, досконалість, чесність та інші. Дослідження показало, що врахування метаданих про джерела інформації дозволяє більш зробити оцінку та прийняти вірне рішення в складних умовах обстановки.

В основі теорії свідчень лежить поняття множини взаємно виключаючих та вичерпних елементів, однак практика використання показує, що сформувати таку множину вдається не завжди. Для вирішення даного роду проблем можливо застосувати теорію правдоподібних та парадоксальних суджень Дезера-Смарандаке. Дана теорія більш широко розглядає невизначеність та оперує такими поняттями як «вільна модель» –основою якої є множина вичерпних елементів, що можуть частково пересікатись, «основа задачі» – що є розширенням поняття «основа аналізу» теорії свідчень, «гіпермножина» – що є розширенням поняття множини елементів теорії свідчень. Серед недоліків даної теорії слід відмітити складність обчислень під час обробки незнання. Для усунення зазначеного недоліку необхідно використовувати потужні обчислювальні комплекси.

Нині всі сучасні методи інтеграції базуються на тому, що ОІ описується в результаті розподілу ймовірностей, а СІ інтерпретується як оцінка ймовірностей (у термінах ймовірнісної логіки). Проте багато видів СІ є непридатними для ймовірнісної інтерпретації. Певна інформація може бути легко представлена й інтерпретуватися логікою першого порядку, у разі, якщо джерелами СІ є БД. Методи на основі мереж Маркова та дедукції також є одним зі способів опису джерел СІ.

Інші види інформації з суб'єктивних джерел є суто якісними (експертне або нечітке оцінювання, міркування, здогадки), тому для них можуть бути застосовані методи нечіткої логіки, теорія свідчень, теорія парадоксальних суджень та інші.

*Архітектура інформаційної системи зведеного аналізу інформації від різнотипних джерел.* В якості базової архітектури для побудови системи може бути розглянута архітектура SNA, яка забезпечує масивно-паралельну обробку даних (рис. 1.14) [6,7].

Структура системи, як програмно-апаратна платформа на основі технології *Big Data* представлена на рис. 1.15. Опис системи на основі технологій *Big Data* як складної ієрархічної системи за результатами структурної декомпозиції подано на рис. 1.16.

При цьому інтеграція підсистем Big Data в єдину систему може реалізовуватися за такими двома принципами.

1. Кожна підсистема є незалежним компонентом загальної системи, при цьому оброблення даних і підготовка інформаційного продукту в основному здійснюється безпосередньо власними обчислювальними ресурсами. Такий підхід доречно використовувати, якщо немає потреби обробляти великі обсяги даних.

2. Гібридний підхід, за якого для оброблення і зберігання даних спільно використовуються ресурси інших підсистем. При цьому використовується підхід до оброблення даних на основі сервісів.

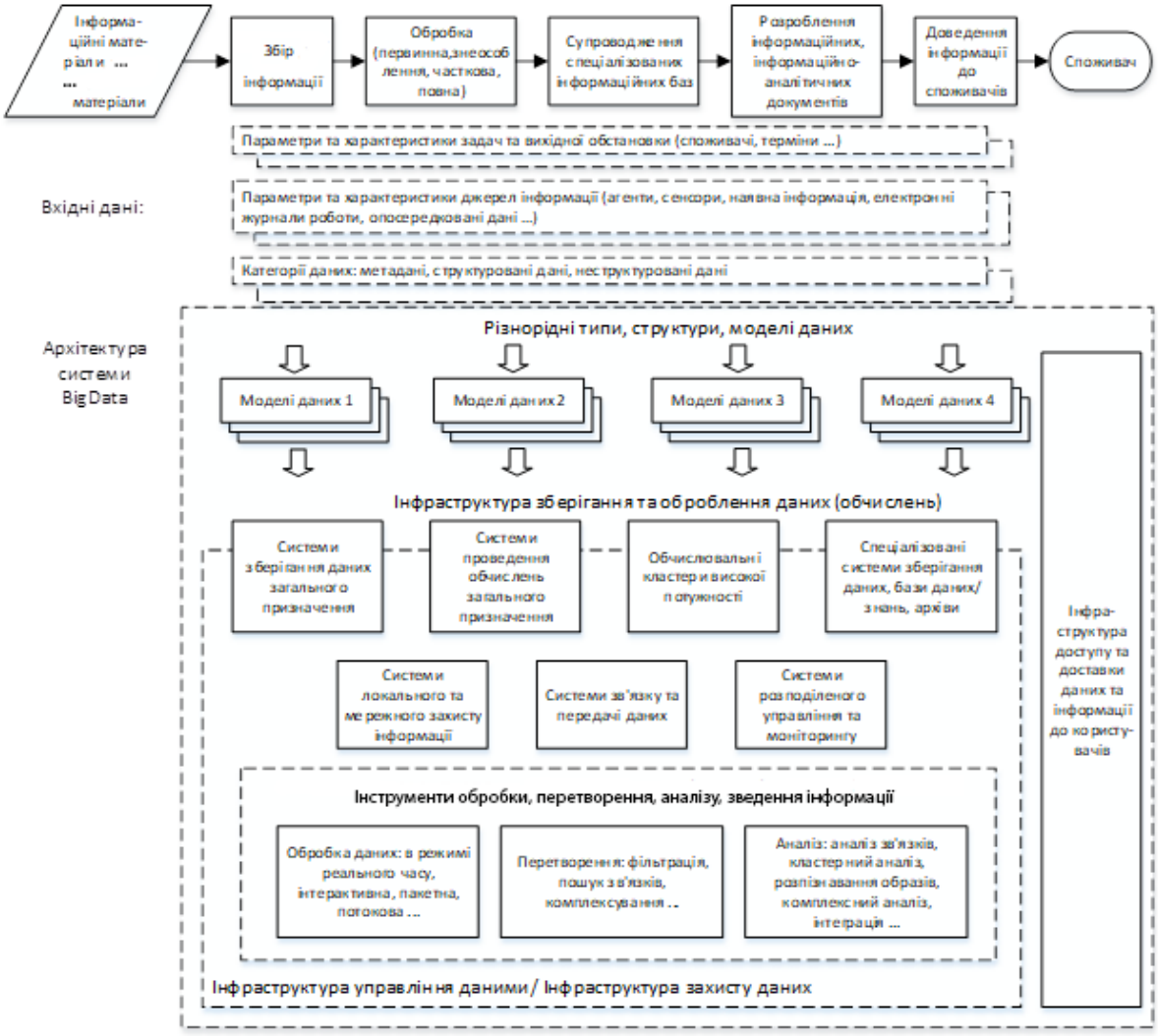



Рис. 1.14. Архітектура системи зведеного аналізу PI на основі технологій Big Data.

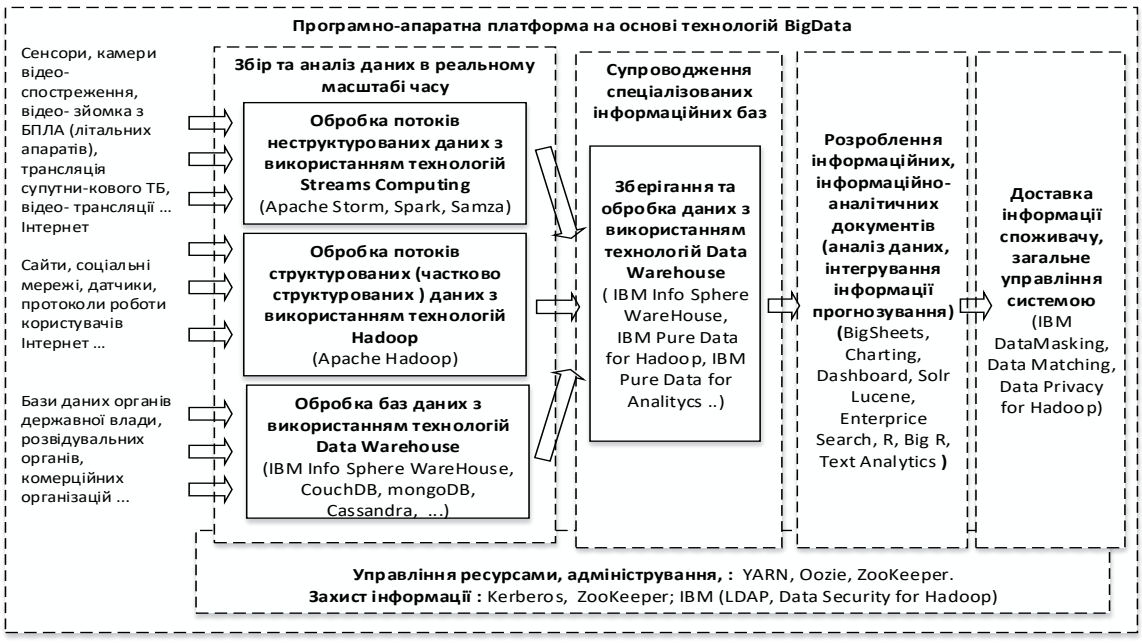



Рис. 1.15. Програмно-апаратна платформа на основі технології *Big Data.*

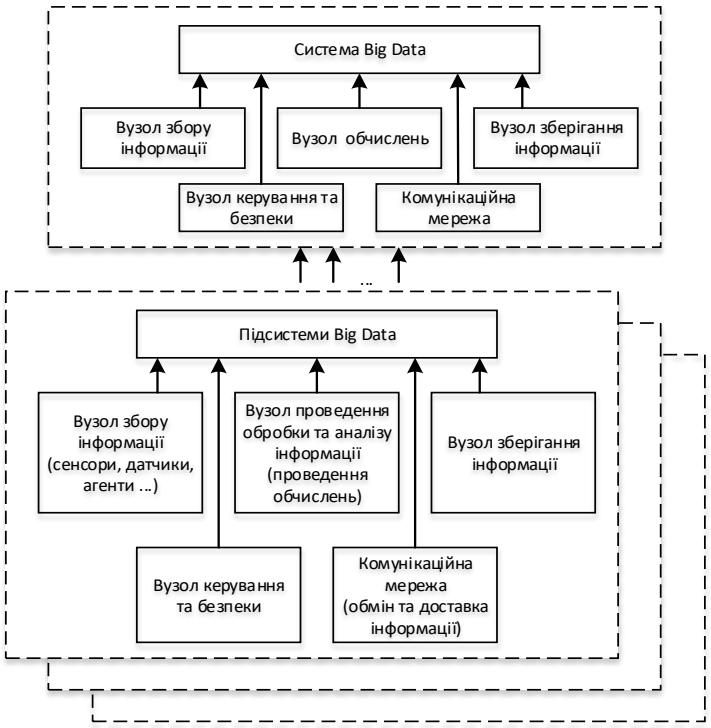



Рис. 1.16. Структурна модель системи на основі технологій *Big Data*

Такий підхід вимагає реалізації узгодженого розподіленого керування системою в цілому, з використанням механізмів балансування навантаження на компоненти системи та розподіленого управління безпекою інформації.

При цьому кожен *r*-й рівень ієрархії системи складається з $F_r$ функціональних елементів. Тоді множину всіх функціональних елементів системи можна описати таким чином:

$$L = \left\{ L_{rf} \mid r = \overline{1,R}, f = \overline{1,F_r} \right\} \tag{1.1}$$

де $R$ – загальне число рівнів ієрархії, $L_{rf}$ – *f-й* функціональний елемент *r*-ого ієрархічного рівня.

Кожний функціональний елемент $L_{rf}$ системи характеризується наступним вектором показників:

$$p_{rf} = \left\{ p_{rfj} \mid j = 1, \ldots, n_{rf} \right\}, \tag{1.2}$$

де $p_{rf}$ – кількість показників функціонального елемента $L_{rf}$, який виконує набір функцій

$$\Phi_{rf} = \left\{ u_{rfk} \mid k = 1, \ldots, m_{rf} \right\}. \tag{1.3}$$

Кожна з функцій $u_{rfk}$ у (6) залежить від значень показників вектора $p_{rf}$:

$$u_{rfk} = u_{rfk}(p_{rf}) \tag{1.4}$$

і впливає на реалізацію вимог до системи в цілому. Згідно з склад і вид функцій (1.2, 1.3) визначається в процесі системного аналізу.

Для простоти викладу відмовимося від подвійної індексації. Тоді узагальнений вектор показників можна подати у вигляді

$$\mathrm{p} = (p_1, p_2, ..., p_{N_0},)^{\mathrm{T}}, \mathrm{p} \in \mathrm{R}^{N_0}, \tag{1.5}$$

де $P = \{p_{rf}, r = 1,\ldots, R, f = 1,\ldots, F_r\}$ – множина показників функціональних елементів на всіх ієрархічних рівнях системи.

Одним із головних завдань структурно-функціонального аналізу є визначення перетворення

$$F: X \rightarrow Y, \tag{1.6}$$

з множини $X$ допустимих показників системи в простір $Y$ необхідних властивостей за набором кількісних і якісних вимог, заданих у вигляді нечітких термів.

При цьому потрібно вирішити задачу структурно-параметричної ідентифікації, що дає змогу визначити структуру ієрархічної системи в цілому, структуру функціональних елементів усіх ієрархічних рівнів, а також вид перетворення (1.6).

## 1.6. Технологія аналітичної обробки різнотипної інформації

Основною проблемою під час обробки різнотипної інформації є її неструктурованість, тобто неможливість розкласти безпосередньо первинну інформацію за окремими полями в БД та індексувати її [27]. Для обробки неструктурованої різнотипної інформації застосовують два найбільш поширені підходи:

1) залучення аналітика для аналізу неструктурованої мультимедіа інформації та виявлення закономірності та трендів з подальшою передачею результатів до стандартних систем аналізу структурованої інформації;

2) передобробка неструктурованої інформації в аналітичній системі для виявлення необхідної інформації, нормалізації та перетворення результату на структуровані дані, які обробляють відповідні аналітичні системи.

Перший підхід є класичним, його застосовують і досі через переконаність у крайній складності створення та використання алгоритмів автоматичної аналітики мультимедіа інформації та, як наслідок, безальтернативності людського мозку в завданнях аналізування об’єктів/подій та виявлення закономірностей в аудіо та візуальній інформації.

Застосування другого підходу, який використовує аналітичну систему для попередньої обробки первинної різнотипної інформації, дає можливість виконати комплексний аналіз і привести різнотипні дані до структурованого вигляду для аналізу стандартними засобами аналітики. Такий алгоритм роботи, який є аналогом роботи мозку аналітика і відповідно не може бути простим, має ґрунтуватися на використанні систем штучного інтелекту (ШІ).

Однак до останнього часу не з'явилося практичного інструментарментарію, що дозволяє автоматизувати цей досить трудомісткий процес та ефективно здійснювати аналітичну обробку різнотипної інформації.

В якості такого інструментарментарія пропонується використовувати систему аналітичної обробки різнотипної інформації, за допомогою якої можна здійснювати передобробку та нормалізацію неструктурованої

інформації, перетворити мультимедіа на числа та факти для подальшої обробки в системах аналізу структурованої інформації [28]. Причому первинна неструктурована інформація має зберігатися, щоб можна було проаналізувати вихідні мультимедіа дані за іншими критеріями, а також задати інші критерії для передобробки і отримати на вхід системи аналізу структурованої інформації інший цільовий набір структурованих результатів.

Щоб проаналізувати інформацію, необхідно попередньо визначити джерела отримання та зібрати її, для чого створюється репозиторій інформації або посилань на неї, доступну в інших БД та/або в інтернеті. Цей репозиторій може бути наповнено з таких джерел: записи ТБ програм, зокрема новини й аналітика; відео та аудіо з Youtube, інші аналогічні сервіси; пости в соціальних мережах, зокрема у Facebook, Instagram, Twitter тощо; записи з камер відеоспостереження; сайти у WEB; інші тексти, фото, відео, а також може бути використано будь-яке інше джерело. Залежно від розв'язуваних завдань та можливостей до переліку крім відкритих джерел інформації може бути включено й закриті – БД та DarkNet.

Технологія проведення аналічної обробки різнотипної інформації може бути алгоритмізована, і алгоритм матиме такі кроки:

***Крок 1.*** Отримання вихідних даних у режимі «real time»: пости та фото із соціальних мереж; новини (текст та фото); інша текстова інформація; фотографії (зокрема, із супутників та дронів); цифрові таблиці та інша цифрова аналітика.

***Крок 2.*** *RealTime InMemory* збереження «сирих» даних у разі потреби обробки *Realtime Data*.

***Крок 3.*** Передобробка: виділення з текстів, що цікавлять, словоформ і поєднань; розпізнавання в зображеннях заданих патернів; індексація таблиць та БД.

***Крок 4.*** Збереження сирих та передопрацьованих даних у БД аналітичної системи для можливості передобробки та виділення інших патернів та проведення аналізу за іншими словосполученнями.

***Крок 5.*** Проведення аналізу щодо появи заданих подій, виявлення трендів.

***Крок 6.*** Подання результатів аналітичної обробки у зручному графічному вигляді з можливістю візуалізації.

Автоматизована аналітична обробка різнотипної інформації з використанням ШІ відбувається за допомогою розроблених алгоритмів декомпозиції, розпізнавання, порівняння та аналізу вихідної неструктурованої інформації (відео, аудіо, текст тощо), кількість якої досягає 90 % від загального обсягу всієї сучасної інформації. Пошук та аналіз інформації проводиться за всіма джерелами з наведеного списку, до яких ця аналітична система має доступ.

Аналітична обробка різнотипної інформації може відбуватися такими способами:

• знаходження всіх матеріалів у всіх БД та джерелах (соцмережі, інтернет-сайти, новини, телепередачі, радіопередачі, переговори, зокрема, файловий архів тощо) за заданими критеріями пошуку: проміжок часу, місцевість/задана територія, емоційне тло, задані джерела даних, зазначені мови, які згадуються в матеріалі, люди/країни тощо, підмножина даних за будь-яким більш «суворим» критерієм;

• розпізнавання осіб і пошук у БД появи особи на відео чи фото, зокрема у своїй основі збережених файлів, на камерах відеоспостереження, у матеріалах з мережі Інернет, випусках новин, соцмережах, відеопорталах тощо. Ця дуже потужна функціональність дає можливість знайти конкретну людину за заданими умовами, джерелами, часовим діапазоном, географічними координатами, у матеріалах на вказану тему чи певного емоційного забарвлення тощо;

• розпізнавання номерів автомобіля на фото та відеоматеріалах і пошук у доступних джерелах автомобіля із цим номером, розпізнавання кольору та марки автомобіля в кожному фрагменті;

• розпізнавання заданого об’єкта на відео/фото та знаходження матеріалів, де цей об’єкт представлено. Для розпізнавання об’єкта його мають або попередньо внести до БД об’єктів аналітичної системи, або ввести в базу об’єктів за чинною процедурою;

• розпізнавання заданого зразка звуку в зазначених джерелах даних з урахуванням обмежень за місцем, часом, тематикою тощо та пошук матеріалів, в яких цей зразок аудіо було знайдено;

• розпізнавання мови та переведення її у текстовий вигляд «синхронно», окреме розпізнання діалогу, його емоційного забарвлення, визначення статі мовця. Можливість подальшого перекладу розпізнаного тексту іншими мовами. Крім того, ця функціональність дає змогу пов’язати набір характеристик цього зразка голосу з конкретною людиною та виконати пошук фрагментів мови конкретної людини в доступних базах, таким способом уже на основі аудіоінформації доповнити архів даних про людину додатковою інформацією про місце та час розмови, співрозмовника, а також іншими параметрами. Очевидно, що ця функціональність залежить від мови, яка розпізнається, доповнення системи новою мовою можливе, але потребує певної лінгвістичного опрацювання;

• побудова графа зв’язків конкретної людини та аналіз взаємозв’язків групи людей, взявши до уваги задані параметри;

• інші методи аналізу.

У результаті виконання згаданих аналітичних дій з різнотипної інформацією, аналітик отримує структуровану інформацію, яку можна використати для подальшого аналізу.

Система аналітичнної обробки різнотипної інформації складається із системи аналітичнної обробки неструктурованої інформації та системи аналітичнної обробки структурованої інформації. Це можуть бути різні модулі однієї системи або кілька систем, що взаємодіють між собою.

Система аналітичнної обробки структурованої інформації за чинним і досить широким інтерфейсом API (Application programming interface) формує запит в систему аналітичнної обробки різнотипної інформації, зокрема мультимедіа та отримує числовий або текстовий результат, наприклад, кількість певних заданих об'єктів, координати об'єкта, час/дата появи якогось об'єкта на певній місцевості тощо. Це дає змогу перейти від розпізнавання якісної інформації (відео, аудіо, текст тощо) до мови цифр для подальшого використання в аналізі звичних числових потоків даних, якими звикли оперувати аналітики.

Проте водночас залишається можливість звернутися до першоджерела (відео, фото, сайт, запис мови, пост у соцмережі тощо) та додатково проаналізувати конкретні медіадані як основу для висновків системи аналітичнної обробки різнотипної інформації. Крім того, аналітик може застосувати систему аналізу мультимедіа інформації, щоб створити запит безпосередньо в цій системі та паралельно самостійно проаналізувати вихідний мультимедіа контент. Це дає можливість використовувати весь потенціал систем аналітичнної обробки неструктурованої інформації безпосередньо у вікні системи, що в цьому разі дасть змогу отримати на робочій станції аналітика та вивчити матеріали з тематики, що цікавить (беручи до уваги позначки або теги), аналізувати аудіо/відео з прив'язкою до місцевості у заданому проміжку часу з позитивним чи негативним забарвленням, вивчати графи ланцюжків взаємозв'язків людей чи подій.

Зважаючи на викладене, можна сформулювати технічні вимоги до системи аналітичної обробки різнотипної інформації.

*1. Вимоги до вбудованого пошукового функціоналу системи розпізнавання та аналітики:*

- забезпечувати повнотекстову функцію пошуку. Це стосується вмісту кожного файлу, в якому є текстові елементи, навіть якщо їх стиснуто в архівний файл або прикріплено до електронного листа;
- забезпечувати розширену функцію пошуку, яка дає можливість користувачам проводити пошук у кожному полі метаданих;
- забезпечувати пошук об'єктів на основі концепцій, ключових слів та метаданих, включно з аналізом відео та аудіо, як перетворення тексту в текст, розпізнавання обличчя, розпізнавання символів на екрані та логотипу; повний текст у документі або поєднання критеріїв;
- результати пошуку має бути впорядковано за релевантністю (сортування за замовчуванням) та датою (як за зростанням, так і за спаданням хронологічно). Упорядкування результатів за іменами файлів (в алфавітному порядку в обох напрямках) є вагомою перевагою;
- результати пошуку має бути згруповано відповідно до метаданих документів, визначених за допомогою розпізнавання іменованих сутностей;
- давати можливість зі списку результатів отримувати для кожного з них подібні документи щодо шаблонів документів та/або назв файлів та шляху UNC та/або URL-адреси;

- уможливлювати використання аргументів (І; АБО; НЕ), наближення (“”) та операторів усічення (?; *);
- надавати можливість користувачам зберігати попередні критерії пошуку або списки результатів;
- мати можливість розглядати ланцюжки різних символів як еквівалентні ключові слова або вирази відповідно, з одного боку, до управління багатомовністю, а з іншого – до реалізації заздалегідь визначеного словника синонімів. Наявність додаткового словника синонімів у системі є вагомою перевагою;
- уміти ідентифікувати різні мови під час процесу індексації та обов’язково підтримувати українську, російську та англійську;
- забезпечити автоматичне керівництво запитом у вікні пошуку, поки користувачі вводять текст;
- розпізнавати неправильно написані пошукові терміни та пропонувати виправлення.

2. *Вимоги до функціоналу індексації та зберігання системи розпізнавання та аналітики:*

- текстові елементи у вмісті файлів, імена файлів, оригінальні метадані та шлях UNC та/або URL-адреса, за якою можна знайти документи, мають бути індексованими елементами, що уможливить як пошук, так і розпізнавання іменованої сутності;
- мати можливість вилучати з індексації конкретні місця даних у джерелах даних (наприклад, конкретні сховища документів);
- перелік вилучених місць даних має бути відомим, і їх повторне введення в індекс також має бути можливим;
- давати можливість адміністраторам виключати певні документи зі свого індексу (перелік вилучених документів має бути відомим, і їх повторне внесення в індекс також – можливим);
- користувачі мають можливість вручну змінювати метадані, прикріплені до документів, вибираючи іншу властивість заздалегідь визначених категорій. Здатність системи «вчитися» на цьому процесі та динамічно адаптувати свій процес індексації також є вагомою перевагою;
- мати можливість призначати документам як дату останньої модифікації, так і дату періоду, охопленого темою документа (наприклад, документ, що описує ситуацію у 2008 році, може бути відредаговано згодом);
- має бути можливість точно налаштувати модель пошуку системи, щоб покращити релевантність пошуку документів щодо конкретних потреб користувачів. Можливість динамічно обробляти ці функції щодо профілів користувачів та метаданих документів є суттєвою перевагою;
- уможливлювати експорт метаданих, визначених за допомогою розпізнавання іменованих сутностей у файлах xml;

- уможливлювати класифікацію відомих категорій за допомогою алгоритмів штучного інтелекту за зразками статей та концептуальними визначеннями пошуку;
- уможливлювати вилучення відомих сутностей за допомогою алгоритмів машинного навчання.

*3. Вимоги до функціоналу інтеграції системи розпізнавання та аналітики з іншими системами:*

- можливість інтегрувати змішані програми із такими системами відображення, як Google Maps, Google Earth або OpenStreetMap та керувати геопросторовими даними. Функціонал, який має бути принаймні реалізовано, – це давати можливість користувачам відображати та переглядати документи своїх списків результатів на карті. Під час індексації до документів слід додавати координати GPS;
- можливість відкривати розташування файлів з інтерфейсу користувачам. Це принаймні стосується файлових серверів та вебсерверів. Шлях UNC та/або URL-адреса кожного документа мають відображатися в результатах пошуку;
- можливість організувати документи та результати пошуку в колекції. Ці колекції можуть базуватися на типології індексованих джерел даних. Колекції може бути обрано в будь-який час і переведено на динамічно широкий та вузький обсяг досліджень;
- бути високо масштабованою щодо збільшення кількості користувачів, доданих/індексованих документів та джерел даних;
- дублікати одного документа не мають відображатися у списках результатів;
- можливість виявляти дублікати за контрольною сумою і або уникати їх під час індексації джерел даних, або видаляти їх з індексу згодом під час запиту;
- можливість інтегрувати систему в інші програми за допомогою API;
- можливість керувати великою кількістю неструктурованих даних, що швидко зростають, особливо якщо підключено соціальні медіаджерела.

*4. Вимоги до керування користувачами системи розпізнавання та аналітики:*

- надавати можливість застосовувати правила доступу/обмеження безпеки як на рівні групи, так і на рівні користувачів. Захист на рівні групи має застосовуватися до всіх користувачів у межах визначеної групи, тоді як захист на рівні користувача має передбачати додаткові обмеження або можливості для вказаних користувачів. Ці правила безпеки мають відповідати оригінальному Рольовому контролю доступу для кожного з різних джерел даних. Документи з обмеженим доступом не мають відображатися у списку результатів;
- надавати можливість застосовувати правила доступу/обмеження безпеки на рівнях документів та колекцій. Можливість визначати правила

безпеки на основі метаданих документів відповідно до профілів користувачів також є вагомою перевагою;

- працювати повністю автономно без застосування хмарних потужностей або потужностей виробника.

5. *Вимоги до функціоналу аналітики та звітності системи:*

- надавати статистичні звіти про використання системи, включно з кількістю з'єднань, більшістю введених запитів та найбільш перевіреними документами. Подальший аналіз поведінки користувачів, наприклад, щодо часу пошуку та відмови від пошуку;
- надавати особисті та/або загальні попередження користувачам про нові документи, проіндексовані в системі;
- надавати користувачам можливість «виділяти» або «позначати» документи з результатів пошуку, наприклад, «посилання» або «великий інтерес». Виділені таким способом документи мають піддаватися зважуванню критеріїв пошуку, щоб вони відображались у найкращих результатах. Також має бути можливість здійснювати пошук або фільтрувати лише документи, позначені таким способом;
- підтримувати розпізнавання номерних знаків, виявлення облич, розпізнавання облич;
- надавати користувачам можливість експортувати свої списки результатів у файл електронних таблиць.

Отже, запропонований функціонал системи аналітичної обробки різнотипної інформації є потужним додатковим інструментарієм аналітика, оскільки його інтуїція та досвід сприятимуть отриманню синергетичного ефекту.

З урахуванням вищевикладенного архітектуру системи аналітичної обробки різнотипної інформації представлено на рис. 1.17.

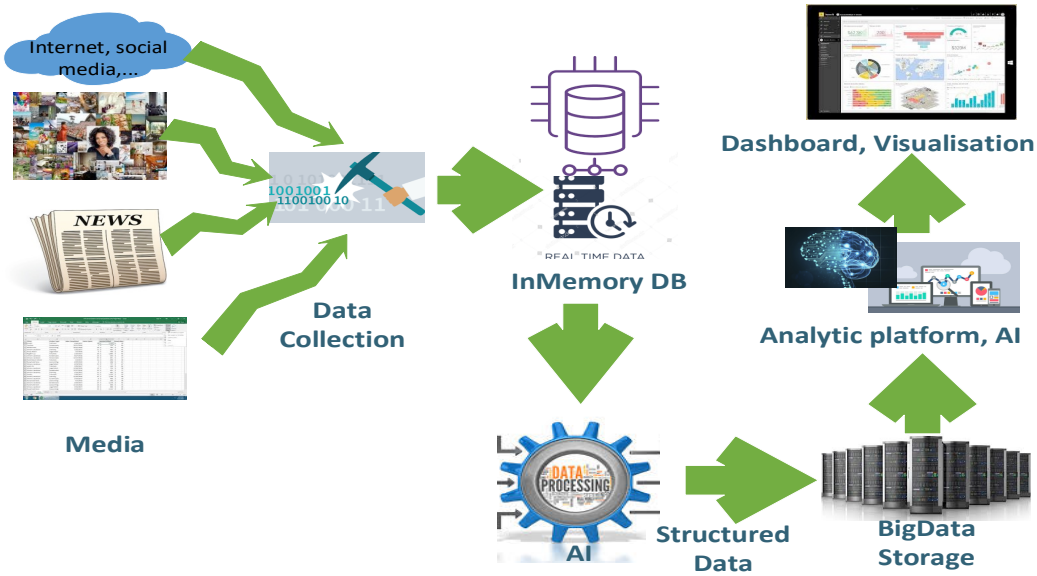



Рис. 1.17. Архітектура системи аналітичної обробки різнотипної інформації

Підсумовуючи, хотілось б відзначити, що запропоновані технологія аналітичної обробки різнотипної інформації та інструментальний засіб її автоматизації, дають можливість значно збільшити обсяг оброблюваної інформації, суттєво підвіщити ефективність аналізу, що покращить якість аналітичної обробки та як наслідок підвищить достовірність її результатів.

### 1.7. Підходи до оцінки ефективності в системному зведеному аналізі інформації від різнотипних джерел

Сучасне прискорення змін інформаційного середовища, швидкий розвиток технологій Internet/Intranet, глобалізація інформаційного простору, яка постійно розширюється, підтверджують, що роль інформації в фаховій діяльності дуже швидко росте. У цей час ефективне існування будь-якого інформаційно-аналітичного підрозділу залежить від того, наскільки докладно, вчасно і якісно вдається відслідковувати інформацію про об’єкти, явища та події у визначених законодавством сферах, наскільки якісно й адекватно виконується аналіз інформації з метою досягнення цілей. У рішенні цих питань величезну роль грають засоби автоматизації обробки інформації, тобто інформаційні системи й технології, які пропонують виробники IT-інструментів [1–3,10–12].

Сучасні технології дозволили суттєво спростити розробку й експлуатацію інформаційних систем і стало можливим створення складних розподілених в просторі інформаційних систем, у т.ч. розподілених по усьому світі. Але з іншої сторони на інформаційному ринку існує величезна пропозиція IT-засобів для інформаційно-аналітичних підрозділів. На сьогодні процес впровадження й використання інформаційних систем і технологій практично всіма учасниками ринку є закономірним, обґрунтованим і об'єктивно необхідним, оскільки серйозну конкурентну перевагу на цьому ринку одержують саме ті організації, які здатні ефективно управляти інформацією.

Очевидно, що основної метою впровадження й використання інформаційних систем і технологій в підрозділах є наступні основні кількісні показники діяльності: продуктивність, витрати, якість і множина якісних показників, як, наприклад: забезпечення потужним апаратом відстеження й аналізу ситуації; підвищення задоволеності споживачів при використанні вдосконалених процедур обслуговування й обміну і т.д.

Можна сказати, що сьогодні ІС й технології – це один з інструментів для досягнення цілей, для ефективного використання яких необхідно вирішувати, у тому числі, і проблеми, пов'язані з використанням методів і стандартів оцінки якості інформаційних систем технологій.

У процесі впровадження, експлуатації й супроводу ІС, а також при її модернізації виникає необхідність оцінки якості цієї системи. Актуальність і практична значимість цього завдання підтверджується тим, що до теперішнього часу з'явилася велика кількість організацій, основним видом

діяльності яких є аудит ІС. Однієї з найважливіших завдань аудита ІС є формалізація показників якості й методології їхнього розрахунку, на основі яких повинна бути отримана оцінка стану ІС у цілому й окремих її компонентах. Існують різні методологічні підходи й стандарти оцінки якості ІС. Їхній аналіз показує, що актуальної є завдання розробки системи критеріїв і показників, що дозволяють оцінити якість ІС. Така система показників повинна базуватися на загальноприйнятих стандартах якості ІС і комплексної оцінки моделі ІС. що відбиває всі елементи її архітектури.

Ефективне функціонування ІС значною мірою визначається якістю її компонентів: технічної, математичної, програмної, інформаційної, правовий і інших.

Аналіз публікацій, що стосується якості ІС, показав, що основними складовими й елементами якості інформаційної системи є наступні [16–23]:

- якість інфраструктури (infrastructure quality), тобто якість апаратного й підтримуючого програмного забезпечення (наприклад, якість операційних систем, комп'ютерних мереж і т.п.);
- якість програмного забезпечення (software quality), тобто якість програмного забезпечення інформаційної системи;
- якість програмного забезпечення (software quality), тобто якість програмного забезпечення інформаційної системи:
- якість даних (data quality), тобто якість даних, що використовуються інформаційною системою на вході;
- якість інформації (information quality), тобто якість інформації, зроблена інформаційною системою;
- якість управління (administrative quality), тобто якість адміністрування, включаючи якість фінансування, планування й календарного контролю;
- якість сервісу (service quality), тобто якість навчання, системної підтримки і т.і..

Крім перерахованих складових якості повинне бути прийняте в увагу якість самого процесу, який автоматизується.

У загальному випадку – до основних споживчих якостей будь-якої інформаційної системи відносяться такі, як:

- функціональна повнота;
- швидкодія;
- рівень вимог до комплексу технічних засобів;
- ступінь і простота настроювання технічного середовища;
- вартість;
- можливість перенастроювання на нові умови застосування; можливість роботи в мережі;
- якість допомоги користувачеві в процесі роботи;
- якість користувацького інтерфейсу й ін.

Для оцінки якості ІС у першу чергу необхідно визначити склад і модель інформаційної системи. Під ІС розуміється сукупність апаратно-програмних

засобів, призначених для автоматизації інформаційно-аналітичних процесів організації. Відповідно до сучасних концепцій проектуванні й розробки автоматизованих систем обробки інформації архітектура (склад) ІС представляється у вигляді наступної схеми (рис. 1.18).

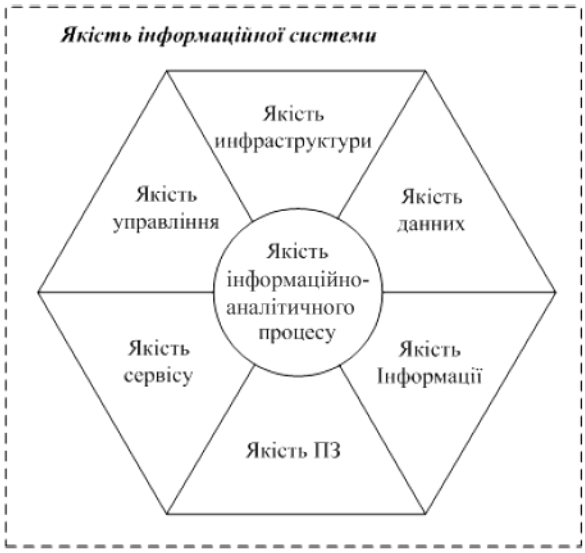



Рис. 1.18. Архітектура ІС для визначення якості

Визначивши якість кожної складової архітектури, можна говорити про якість ІС у цілому.

У результаті можна побудувати наступну модель класифікації критеріїв якості ІС (рис. 1.19.).

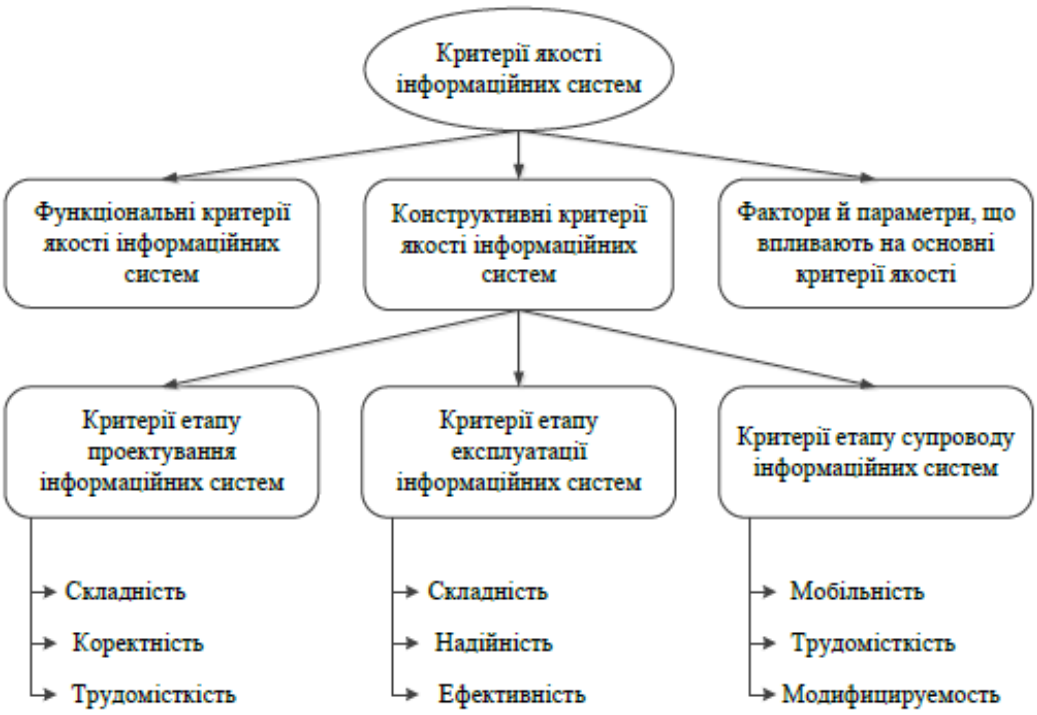


Рис. 1.19. Класифікація критеріїв якості ІС

На сьогоднішній день існує дві головні цілі проведення робіт з оцінки ІС.

Перша мета – це підтвердження того, що ІС, її функціонування й обслуговування відповідають формальним вимогам, закладеним при первісному проектуванні системи.

Друга мета – вивчення стану ІС, пов'язане з наступною її експлуатацією для досягнення цілей замовника й модернізацією, а також для виявлення неполадок і причин цих неполадок.

Деякі випадки, при яких потрібне проведення оцінки для наступної зміни ІС наступні:

- розширення спектра послуг із впровадження ІС;
- ухвалення рішення про впровадження ІС;
- реструктуризація ІТ-підрозділу;
- організація розробки або супроводу ПЗ силами ІТ-підрозділу;
- вибір стратегічних партнерів-постачальників програмних, програмно-технічних засобів і рішень;
- потреба в ефективному й обгрунтованому розподілі ресурсів між множиною нових впроваджуваних інформаційних систем і технологій.

Проведення оцінки ІС дозволяє одержати й систематизувати знання про наявну ІС, оцінити поточну ефективність і безпеку функціонування ІС, оцінити ризики, прогнозувати й управляти їхнім впливом на інформаційні процеси підрозділу, коректно й обґрунтовано підійти до питання модернізації й забезпечення безпеки інформаційних масивів організації.

Аналіз публікацій, що стосується якості інформаційних систем показав, що існуючі в цей час методи оцінки можна розділити на дві великі категорії – це методи комплексної оцінки й методи оцінки інформаційної системи за заданим критерієм, або ряду критеріїв.

Основними методологічними підходами в рішенні питань комплексної оцінки якості ІС є наступні стандарти:

1. COSO (Committee of Sponsoring Organizations) – назва цього методу звучить як: Internal Control – Integrated Framework, що переводиться як Внутрішній контроль – Єдина Структура й призначена для забезпечення управління критичними аспектами організаційного управління, ділової етики, внутрішнього контролю, управління ризиками, фінансової звітності. Рік початку публікації методу –1992.

2. GoCo – назва цього методу звучить як Guidance on Control, що переводиться як Посібник з контролю й призначена для внутрішнього аудита. Рік публікації методу – 1995.

3. Cadbury – назва цього методу звучить як Опис фінансів і внутрішнього обліку (Internal Control over Financial Reporting). Рік публікації методу –1994.

4. COBIT (Control Objectives for Information and Related Technology) – назва цього методу звучить як Контрольні Об'єкти для Інформаційної й суміжної Технологій. Роки публікації методу –1996,1998, 2000, 2006, 2008.

5. SAC&eSAC – назва цей звіт одержала від перших букв сполучення Systems Auditability and Control (SAC), що переводиться як Система Аудитоспособности й Контролю. Рік публікації методу – 2001.

6. SASs 55/78/94 назва цього методу звучить як Офіційний Звід Стандартів Аудита (Statement's on Auditing Standards). Роки публікації методу – 1990, 1997, 2001.

Огляд методів комплексної оцінки показав, що для проведення реальних оцінних робіт власними силами в організації можливо лише із застосуванням методу COBIT, тому що, по-перше, COBIT поєднує матеріали першоджерел COSO і SAC, по-друге, COBIT заснований винятково на засобах контролю інформаційної технології в підтримку цілей підрозділу і, по-третє, лише по методу COBIT є вичерпна доступна й відкрита інформація, здатна допомогти в проведенні оцінних робіт.

Для перспективних і існуючих ІС є наступні методи, у яких сформульовані критерії оцінки якості:

1. Оцінка якості у відповідності зі стандартом ДСТУ 9001:2009 України.
2. Оцінка по методології Benchmarking.
3. Оцінка по методології міжнародного стандарту керування якістю інформаційних систем і технологій COBIT.
4. Система збалансованих показників (Balanced Scorecard – BSC).
5. Інформаційна економіка (Information Economics – EE).
6. Прикладна інформаційна економіка (Applied Information Economics – AIE) .
7. Система показників ИТ (IT Scorecard).

Таким чином, слід відмітити, що найбільш зацікавленим у програмному комплексі для інформаційної системи є споживач, тобто користувач програмного продукту. Для того, щоб вибрати програмну систему, що автоматизує рішення його завдань, потенційний споживач намагається заздалегідь оцінити якість ІС, представлених і доступних на ринку. При цьому необхідно враховувати, що збитки від помилок при проектуванні й виборі ІС можуть бути досить великими.

У той же час у технічній документації більшості програмних засобів, пропонованих у цей час на ринку, відсутня інформація, що дозволяє оцінити вхідні характеристики програми і їхню динаміку при зміні обсягу вхідної інформації. Без такої інформації складно оцінити якість ІС. її економічну ефективність.

*Моделювання процесу оцінки ефективності функціонування системи зведеного аналізу PI.* Зважаючи на велику вартість створення систем, в яких використовуються розподілені в просторі різнорідні дані та потужні обчислювальні ресурси, під час розробки та експлуатації цієї системи доцільно використовувати методи структурно-функціонального аналізу [15–17]. Змістовне формулювання задачі структурно-функціонального аналізу зводиться до такого: необхідно визначити призначення, загальні

характеристики та властивості системи, а також вимоги до структурних, функціональних, експлуатаційних та економічних показників.

Залежно від переліку завдань, що вирішуються в системі, можна визначити конкретні вимоги або властивості системи. Визначимо структуру системи на основі технологій *Big Data* як складну ієрархічну систему та обґрунтуємо вимоги до кожного елемента інфраструктури та функціональних елементів на всіх ієрархічних рівнях [14,15].

Множину вимог до системи подаємо у вигляді впорядкованої структури класів (1.7)

$$V_0 = \{V_i \mid i = 1,\ldots,k\}, \tag{1.7}$$

де $V_0$ – множина вимог до системи, $V_i$ — *i*-й клас вимог до системи, $k$ – кількість вимог. Для системи побудованої на основі технологій *Big Data* визначимо таку множину класів:

$V_1$ – клас структурних властивостей (кількісні характеристики: кількість вузлів у системі, кількість процесорів, пропускна здатність каналів зв'язку тощо).

$V_2$ – клас функціональних властивостей, що визначає перелік функцій системи і кількісні показники їх виконання: підтримка запитів користувачів на виконання завдань, доступ, передачу і реплікацію даних; їх єдина реєстрація; балансування навантаження; збір статистики, прозорість, керованість, адаптованість.

$V_3$ – клас експлуатаційних властивостей, що визначає зручність експлуатації системи та відповідність системи зовнішнім умовам: наявність певного програмного забезпечення, зручний для користувача інтерфейс, вимоги до якості роботи сервісів (доступність, надійність, оперативність).

$V_4$ – клас властивостей безпеки: конфіденційність, цілісність та доступність інформації; можливість спостерігати за роботою системи, відповідність системи визначеним рівням гарантій якості.

$V_5$ – клас економічних властивостей визначає вимоги до вартості створення та експлуатації системи: вартість обладнання, вартість експлуатації, вартість послуг, що надаються системою.

Кожна властивість $v_{ij}$ класу $V_i$ визначається набором показників:

$$W_{ij} = \{w_{ijm} \mid m = 1,\ldots,k_{ij}\}, \tag{1.8}$$

де $w_{ijm}$ – кількість показників для властивості $v_{ij}$, які можуть мати як кількісний, так і якісний вигляд. Вимоги до кількісних показників задаються за допомогою інтервальних оцінок у вигляді

$$\underline{w_{ijm}} < w_{ijm} < \overline{w_{ijm}} \tag{1.9}$$

Вимоги до якісних показників зручно задати за допомогою нечітких термів.

# РОЗДІЛ 2
# ТЕХНОЛОГІЇ ЗБЕРІГАННЯ І УПРАВЛІННЯ ДАНИМИ

Обсяг електронної інформації, що виробляється у всьому світі, щороку зростає. За оцінками компанії IDC, навіть глобальні світові кризи не позначаються на темпах цього зростання, і найближчими роками фахівці передбачають збільшення потреби в обсягах сховищ на рівні 50% на рік. У цьому реальний рівень використання існуючих в компаніях систем зберігання даних (СЗД) загалом становить лише 25–35 %.

Для оперування сучасними величезними потоками інформації їх необхідно збирати, структурувати, зберігати та аналізувати. Операції, які здійснюють над інформацією, зазвичай об'єднують у п'ять груп: збір, передача, зберігання, обробка та споживання.

Для більшості компаній характерно наявність численних розрізнених джерел даних, більшість інформації з яких залишається не затребуваною для цілей аналітики з низки технічних причин і залишається лежати «мертвим» вантажем, не приносячи фактичної користі. Підвищити віддачу від накопичених даних можливо за рахунок впровадження корпоративних СЗД, що забезпечують інтеграцію, очищення та структуроване зберігання даних для подальшого аналізу інформації [30].

## 2.1. Системи резервного копіювання

Існує досить багато визначень терміну «інформація», оскільки у поняття «інформація» вкладається різний зміст залежно від предметної області, на яку воно розглядається. Зазвичай під інформацією мають на увазі будь-які відомості (повідомлення, дані) незалежно від форми їх подання. До основних видів інформації відносяться – графічна, звукова, текстова, числова та відеоінформація, що визначаються формою її подання, а також способами кодування та зберігання. З погляду інформатики найважливішими властивостями інформації є: актуальність; цілісність; достовірність; автентичність; конфіденційність та доступність. Зі зростанням обсягів інформації, що знаходяться на різних носіях, пристроях та системах, ускладнюється завдання надійності їх зберігання, особливо у сучасних умовах вірусної активності, інформаційних загроз, кібератак. Одним із інструментів забезпечення збереження інформації є резервне копіювання та створення інформаційних архівів для швидкого доступу до даних [31]. Для цього необхідно мати механізми їхнього швидкого відновлення із резервних копій. Традиційні методи архівування та відновлення – малоефективні і не дозволяють реалізувати вимоги щодо надійної безпеки та доступності

інформації. Вирішити це можна за допомогою систем резервного копіювання (СРК) [32].

### 2.1.1. Основні системи резервного копіювання та їх особливості

На сьогоднішній день існує досить велика кількість промислових СРК з різним функціоналом. З них можна виділити основних виробників, системи яких максимально відповідають сучасним вимогам щодо зберігання інформації. Це компанії IBM з Tivoli Storage Manager, Veritas з Backup Exec і NetBackup , яка є лідером у цьому сегменті та інші.

*Tivoli Storage Manager* – це СРК рівня підприємства. Надає автоматизовані послуги управління даними на робочих станціях та серверах, що працюють на різних ОС). Для інтерактивного резервного копіювання застосовується програма-клієнт, що ініціює резервне копіювання або відновлення даних. У своєму складі має різні компоненти, які дозволяють нарощувати необхідний функціонал для різноманітних завдань. Як правило, Tivoli Storage Manager використовують у складі комплексних рішень на базі апаратного та програмного забезпечення від IBM.

*Backup Exec та NetBackup* – перша орієнтована на малі та середні підприємства, в IT-інфраструктурі яких переважають ОС на базі Windows, а друга призначена для захисту даних в enterprise -сегменті, з гетерогенною IT-інфраструктурою. Це комплексні рішення для всіх видів резервного копіювання: від окремих фізичних або віртуальних систем до відновлення додатків і БД у масштабах всього підприємства. Ці СРК працюють з урахуванням технології V-Ray.

### 2.1.2. Технологія V -Ray

Технологія V-Ray являє собою новий рівень контролю та моніторингу віртуальних та фізичних систем, що забезпечує розподіл завдань резервного копіювання та автоматичний захист нових віртуальних систем у міру їх підключення. Вона надає можливість контролювати віртуальні файлові системи та програми з подальшим виконанням прозорого резервного копіювання, застосовуючи гнучкі варіанти технології дедуплікації файлів, яка, у свою чергу, дозволяє суттєво скоротити обсяг резервної копії на СЗД. Завдяки вбудованій інтелектуальній дедуплікації з'явилася можливість підвищити ефективність зберігання даних до 98% та скоротити обсяг резервних копій VMware та Hyper-V до 95%. Технологія V-Ray суттєво економить час на резервне копіювання та відновлення у розподіленій ІТІ, а також спрощує керування цими процесами.

Для віртуального середовища технологія V-Ray дає можливість забезпечити безпеку, захист, резервне копіювання та відновлення даних у будь-який момент часу та в будь-якому місці. Завдяки цій технології стало можливим зменшити навантаження на мережу та СЗД, а також швидше

відновлювати дані без зниження продуктивності віртуального середовища, оскільки для її роботи не потрібні агенти. V-Ray дозволяє відновити потрібні дані всього за кілька хвилин за рахунок використання технології гранулярного відновлення, яка виключає необхідність тривалого пошуку архіву СЗД для виявлення потрібного файлу. Для цього реалізовано можливість прямого звернення до backup -образів систем з метою вибору та відновлення потрібної інформації. Технологія V-Ray автоматично захищає нові віртуальні машини (ВМ), які перейшли у стан online , при цьому політика резервного копіювання залишається незмінною.

### 2.1.3. Технологія дедуплікації

Дедуплікація даних – це технологія, що дозволяє усунути дублювання даних та скоротити при цьому обсяги фізичних носіїв для зберігання (рис. 2.1). До її появи кожна резервна копія могла мати однаковий набір файлів, що не змінилися з часу останньої резервної копії, що призводило до збільшення обсягів зберігання, а зі зростанням змінюваних даних збільшувало і час резервного копіювання.


Рис. 2.1. Технологія дедуплікації даних

Технологія працює на рівні блоків даних, записаних на диск, де використовуються хеш функції. Коли система дедуплікації знаходить хеш-функції, що збігаються, для різних блоків, вона пропонує зберегти блоки у вигляді єдиного екземпляра і набору посилань на нього. Ця технологія також дозволяє виробляти глобальну дедуплікацію – порівнювати блоки даних з різних комп'ютерів, що ще більше збільшує ефективність дедуплікації , так як на дисках різних комп'ютерів з однієї і тієї ж ОС може зберігатися велика кількість даних, що повторюються. У СРК компанії Veritas реалізовано три способи застосування дедуплікації :

- *дедуплікація на стороні клієнта/джерела,* при якій в СЗД передаються лише унікальні дані, при цьому сам сервер резервного копіювання в процесі не бере участі, що дозволяє звільнити його ресурси для виконання інших завдань та знизити навантаження на канали передачі;

• *дедуплікація на сервері,* при якій дані, що надходять на СРК, дедуплікуються і записуються на СЗД;

• *дедуплікація на пристрої,* при якій дані дедуплікуються безпосередньо на СЗД, з якими інтегровані СРК, що дозволяє швидко відновлювати дані у разі збою за рахунок мінімізації часу відновлення (Recovery Time Objective – RTO ) .

Особливо ефективною технологія дедуплікації показала себе у віртуальних інфраструктурах VMware та Hyper-V, де більшість таких ОС, як Windows та Linux, розгорнуті з еталонного дистрибутива, містять однаковий набір програм, компонент та бібліотек на своїх віртуальних дисках і можуть відрізнятися між собою лише файлами та папками персональних налаштувань. Кожна така ВМ займає десятки гігабайт у системі зберігання, і в цьому випадку технологія дедуплікації допомагає зменшити обсяг резервних копій та скоротити час на їх створення. Використання цих технологій дозволяє прискорити резервне копіювання до 10 разів, а обсяг резервних копій скоротити на 95%.

### 2.1.4. Система резервного копіювання Backup Exec

Найбільш поширеною СРК є Backup Exec, здатна захистити як фізичні середовища, а й віртуальні. Багатофункціональність Backup Exec дозволяє реалізувати всілякі сценарії роботи з такими об'єктами ІТТ організації, як ВМ, фізичні сервери, додатки, їх компоненти, файли, папки (рис. 2.2).

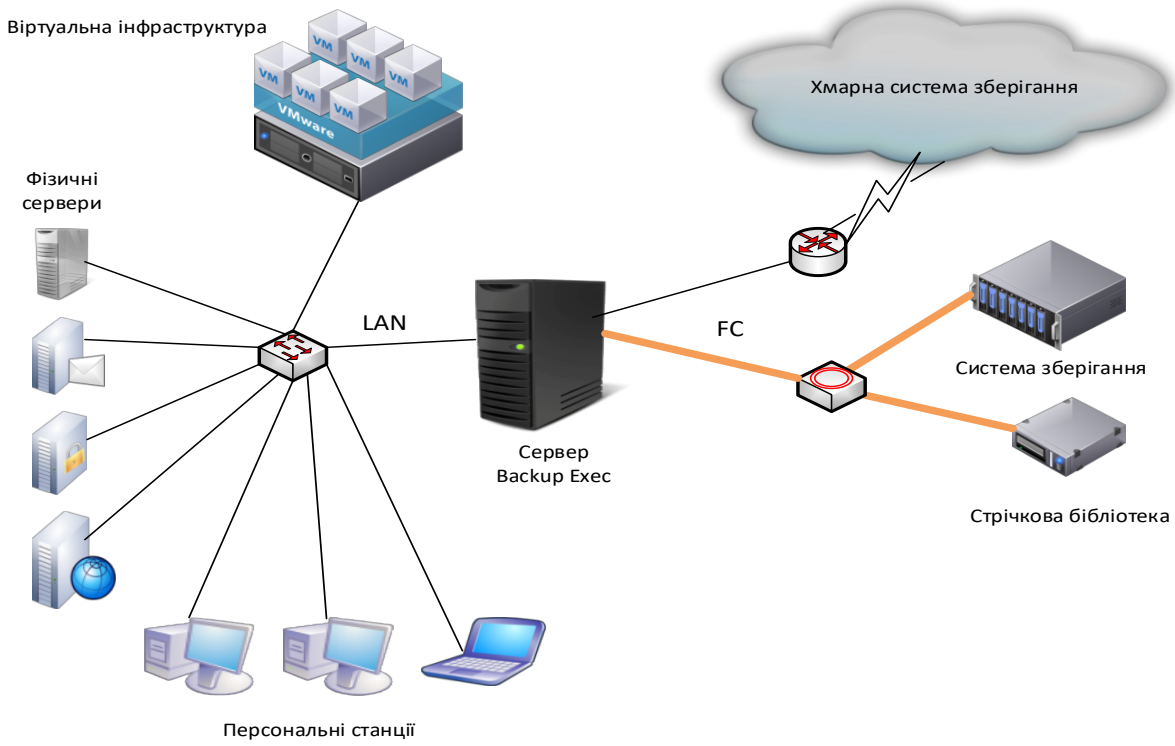



Рис. 2.2. Інтеграція Backup Exec з об'єктами ІТ-інфраструктури

Основними перевагами Backup Exec є:

- *резервне копіювання на будь-які пристрої зберігання* , такі як: жорсткий диск, стрічкові бібліотеки, сховища, доступні по Storage Area Network (SAN) або Local Area Network (LAN), хмарні сервіси Amazon S3, Google Cloud Storage та Microsoft Azure;
- *швидке створення моментальних копій ВМ* завдяки тісній інтеграції з Microsoft Volume Shadow Copy Service та VMware vStorage API для Data Protection (VADP), що дозволяє зменшити споживання ресурсів процесора, пам'яті введення-виведення на ВМ;
- *захист ВМ* с Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory, Microsoft SQL Server завдяки вбудованій функції Instant Granular Recovery Technology (GRT), яка дозволяє з резервних копій ВМ миттєво вилучати та відновлювати окремі файли, папки, SQL, сховища Exchange та елементи поштових ящиків;
- *інтегрована функція відновлення після аварії* – технологія Bare Metal Restore, вбудована в процес резервного копіювання, здатна виконати відновлення на вихідну апаратну платформу або на відмінну від неї.

### 2.1.5. Система резервного копіювання NetBackup

Це кросплатформне рішення для резервного копіювання, здатне працювати з дуже великими обсягами даних для комплексної фізичних та віртуальних систем, додатків та БД у корпоративних ЦОД. Система володіє високим рівнем продуктивності, автоматизації та масштабованості, орієнтована на організації корпоративного рівня, IT-інфраструктура яких включає тисячі як фізичних, так і віртуальних серверів (рис.2.3). До її складу входить широкий набір компонентів для оптимізації резервного копіювання та відновлення в гетерогенних середовищах, що дозволяють працювати з такими ОС, як HP-UX, HP Tru64, IBM AIX, Linux, Microsoft Windows, Novell NetWare, SGI IRIX та Sun Solaris. Для оперативного відновлення критично важливих БД та додатків NetBackup пропонує агентів для взаємодії з програмним та апаратним забезпеченням компаній IBM, Microsoft, Oracle, SAP та Sybase.

СРК NetBackup у своїй стандартній конфігурації має трирівневу архітектуру.

*Майстер-сервер* – забезпечує централізоване управління всією інфраструктурою резервного копіювання. Адміністратор може з однієї консолі управляти всіма носіями резервного копіювання, створювати політики, ставити та керувати розкладом резервного копіювання, створювати звіти за результатами операцій.

*Медіа-сервер* – відповідає за роботу зі стрічковими або дисковими СЗД, яких у інфраструктурі, як правило, кілька, і кожен може працювати як з одним, так і з декількома типами різних СЗД, що дозволяє підвищити

швидкість запису резервних копій через медіа-сервери з балансуванням між ними трафіку резервного копіювання.

*Агент* – клієнтська програма, що забезпечує читання та відправлення даних з серверів, що захищаються.

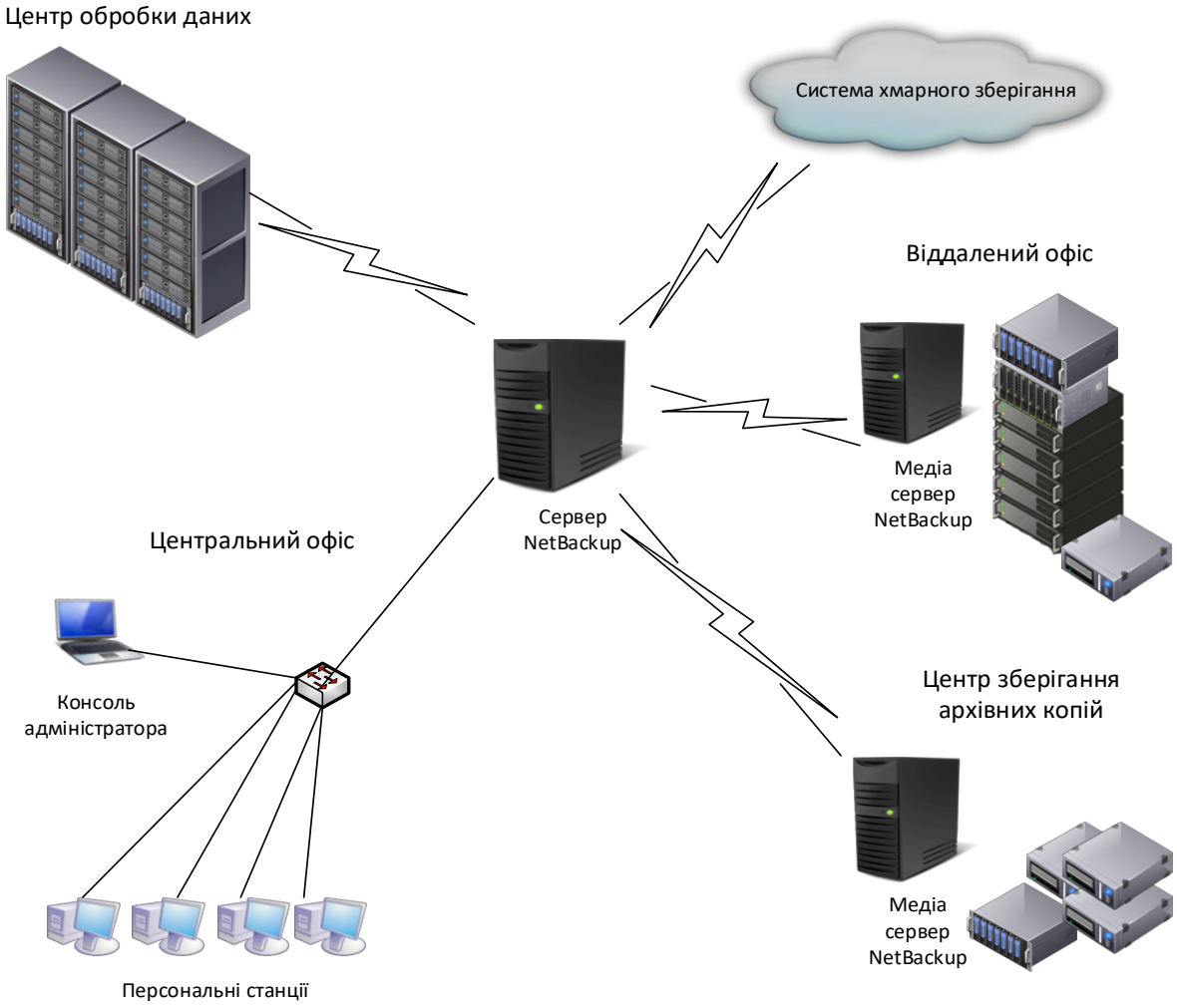



Рис. 2.3. Інтеграція NetBackup з об'єктами IT-інфраструктури

До основних переваг NetBackup відносяться:

- *централізоване управління* – керування всіма серверами NetBackup з однієї консолі керування, що дозволяє підвищити ефективність системи;
- *висока продуктивність* – використання технології синтетичного резервного копіювання дозволяє зберегти пропускну спроможність мережі та знизити рівень впливу на сервер програми завдяки тому, що резервне копіювання виконується лише один раз, а також мультиплексування до 32 різних потоків даних на один стрічковий накопичувач забезпечує максимальну пропускну спроможність апаратного забезпечення для зберігання інформації;
- *автоматизоване аварійне відновлення* – за допомогою технології Bare Metal Restore забезпечує відновлення системи та відновлення працездатності серверів у разі аварійної ситуації;

• *NetBackup Vault Option* – керування віддаленими стрічковими накопичувачами, використовується для створення та зберігання дублікатів стрічкових носіїв на резервному майданчику.

СРК NetBackup також має додатковий функціонал, який розширює її можливості.

*NetBackup Accelerator for VMware* – функція, що дозволяє скоротити час, необхідний резервного копіювання ВМ з допомогою комбінування инкрементального резервного копіювання з дедуплікацією . Після виконання повного резервного копіювання на дискову бібліотеку передаються лише змінені блоки, використовується механізм відстеження змінених блоків VMware Changed Block Tracking (CBT), а потім медіа-сервер збирає з інкрементальних резервних копій повну копію за допомогою функції синтетичного резервного копіювання Optimized Synthetics .

*NetBackup Accelerator for Microsoft Hyper-V* – функція практично аналогічна NetBackup Accelerator for VMware, але на відміну від неї резервне копіювання виконується за допомогою технології Microsoft Resilient Change Tracking (RCT), вбудованої в Windows Server 2016. Здійснюється передача тільки змінених блоків і синтез нових повних резервних копій, резервне копіювання та відновлення ВМ Hyper-V у цьому випадку можна виконувати значно менший проміжок часу.

*NetBackup for vCloud Director* – Інтеграція з Vmware vCloud Director дозволяє за допомогою цієї функції виявляти розгорнуті в публічній або приватній хмарі нові ВМ та одразу забезпечувати їх захист. Навіть якщо образи ВМ досягають обсягу 2ТБ, NetBackup має можливість їх відновлення протягом декількох хвилин.

Таким чином, СРК Backup Exec орієнтована на використання організаціями, в IT-інфраструктурі яких основні сервіси працюють під керуванням ОС Windows і резервне копіювання яких виконується на кілька пристроїв зберігання, у відведений для цього нічний час і не потребує додаткових ресурсів. Використання СРК NetBackup буде більш ефективним в організаціях корпоративного рівня з гетерогенною IT-інфраструктурою, в яких сервіси працюють під різними ОС (Unix, Linux, Windows), з великими обсягами даних та для резервного копіювання яких необхідні гнучкіші інструменти та налаштування.

Отже, СРК є критично важливим елементом IT-інфраструктури будь-якої організації та ефективним інструментом забезпечення захисту інформації.

## 2.2. Системи зберігання даних

СЗД – це комплексна програмно-апаратна платформа для організації надійного зберігання інформаційних ресурсів та надання гарантованого доступу до них. Існують такі види СЗД:

Direct-Attached Storage (DAS) – це безпосередньо підключені до обчислювальної системи диски. Зазвичай, як DAS кваліфікуються варіанти

тільки безпосереднього прямого підключення. Так, наприклад, підключення дисків СЗД по каналу FC в режимі «точка-точка» (без «мережі зберігання», порт системи зберігання в порт сервера), незважаючи на те, що формально є DAS, проте вважається приватним, «виродженим» випадком SAN.

SAN є архітектурним рішенням для підключення зовнішніх пристроїв зберігання даних, таких як дискові масиви, стрічкові бібліотеки, оптичні приводи до серверів таким чином, щоб ОС розпізнала підключені ресурси як локальні.

Network Attached Storage (NAS) – мережна СЗД, мережне сховище. По суті, це комп'ютер з деяким дисковим масивом, підключений до мережі (зазвичай локальної) і підтримує роботу з протоколів. Часто диски в NAS об'єднані в RAID-масив. Декілька таких комп'ютерів можуть бути об'єднані в одну систему.

Функціональні можливості сучасних СЗД орієнтовані на виробничі та фінансові потреби замовників. В даний час компанії, що працюють у різних галузях економіки, зацікавлені в отриманні, обробці, зберіганні та ефективному управлінні інформацією [33]. Тому традиційні рішення, які виробники інтелектуальних систем пропонували ще кілька років тому, не відповідають критеріям цільових споживачів. Необхідні нові підходи у галузі розробки СЗД:

- безперервне функціонування за необхідності відновлення БД у надзвичайних ситуаціях;
- комплексні послуги, що оптимізують витрати на зберігання та доступ до даних;
- надання мережевих сервісів, орієнтованих реалізацію конкретних галузевих завдань;
- можливості розширення для діючих програм;
- постійний моніторинг, архівування та складання звітів, іншої документації у середовищі зберігання, вільної від ризиків.

В даний час на світовому комп'ютерному ринку СЗД представлені технологіями нового покоління, одним із найперспективніших напрямків є віртуалізація систем зберігання. Її повсюдне використання значно полегшує управління різними системами, оскільки програмні частини сумісні з пристроями різних типів. СЗД може бути як частиною, і основою ЦОД.

### 2.2.1. Основні проблеми, що вирішуються СЗД

Для будь-якої організації, навіть якщо це хоча б кілька десятків комп'ютерів і кілька територіально рознесених офісів, характерні типові проблеми, пов'язані з обсягами інформації, що зростають.

Децентралізація інформації – якщо раніше всі дані могли зберігатися буквально на одному жорсткому диску, то тепер будь-яка функціональна система потребує окремого сховища – наприклад, серверів електронної

пошти, СУБД, домену та ін. Ситуація ускладнюється у разі наявності територіально-розподілених офісів (філій).

Лавиноподібне зростання інформації часто кількість жорстких дисків, які можна встановити в конкретний сервер, не може надати необхідну системі ємність. І як наслідок – неможливість повноцінно захистити дані, що зберігаються, недостатня швидкість обробки інформації, складність резервного копіювання (архівування). Дуже складно чи неможливо передбачити необхідний обсяг дискового простору при розгортанні комп'ютерної системи, внаслідок чого виникають проблеми розширення дискових ємностей та неефективної утилізації ресурсів.

Низький ступінь конфіденційності розподілених даних – неможливо проконтролювати та обмежити доступ відповідно до політики безпеки підприємства. Це стосується як доступу до даних існуючих для цього каналів (локальна мережа), так і фізичного доступу до носіїв.

Складність управління розподіленими потоками інформації – будь-які дії, створені задля зміни даних у кожному філії, містить частину розподілених даних, створює певні проблеми, починаючи з складності синхронізації різних БД, версій файлів розробників і до непотрібним дублюванням інформації.

Низький економічний ефект впровадження «класичних» рішень – у міру зростання інформаційної мережі, великих обсягів даних і все більш розподіленої структури підприємства фінансові вкладення виявляються не настільки ефективними і часто не сприяють вирішенню проблем, що виникають.

Високі витрати на підтримку працездатності усієї інформаційної системи підприємства – починаючи від необхідності утримувати великий штат кваліфікованого персоналу та закінчуючи численними дорогими апаратними рішеннями для вирішення проблеми обсягів та швидкостей доступу до інформації в сукупності з надійністю зберігання та захистом від збоїв.

У контексті перерахованих проблем, що рано чи пізно виникають у будь-якій динамічно розвивається, можна сформулювати вимоги до сучасних СЗД.

### 2.2.2. Вимоги до систем зберегання даних

Традиційний підхід до побудови сучасної архітектури зберігання даних, що вже досить давно містить концепцію багаторівневого зберігання, з різними вимогами щодо надійності, продуктивності, доступності, необхідно доопрацювати відповідно до сучасних вимог до ІТІ організацій з метою забезпечення динамічної та гнучкої ІТ-інфраструктури для віртуалізованих серверних ресурсів та швидкого розгортання або розширення програмних програм. Традиційні аспекти високої надійності, високої продуктивності та простоти управління залишаються актуальними і для нових поколінь СЗД. Але їх необхідно доповнити такими характеристиками:

- спрощене використання та початкове планування зміни;
- динамічне виділення ресурсів;

- постійна оптимізація та налаштування системи при зміні зовнішніх умов та для забезпечення найбільш ефективного зберігання інформації;
- оптимізація лише на рівні одного логічного тому;
- забезпечення безпечного доступу до даних та адміністрування системи;
- масштабована архітектура;
- розрахована на багато користувачів система зберігання;
- планова надійність системи;
- оптимальне використання ресурсів системи;
- віртуалізоване зберігання даних як лише на рівні однієї системи, і лише на рівні кількох систем.

Одне з основних завдань, яке прагнуть вирішити при розробці та побудові СЗД, – забезпечення максимальної гнучкості та масштабованості при збереженні високої ефективності використання ресурсів.

## 2.3. Програмно-визначені системи збереження данних та їх особливості

У великих організаціях СЗД становить до 25% вартості IT-інфраструктури. Ця цифра може істотно збільшитися внаслідок зростання обсягу даних і потреби в ємностях СХД. У той самий час організації мають обмежені IT-бюджети, що змушує шукати технологічні рішення, дозволяють скорочувати Витрати побудова СЗД без погіршення якості сервісу.

Одне з таких технологічних рішень – програмно-визначені СЗД (Software-Defined Storage – SDS), які дозволяють створювати сховища даних на неспеціалізованому обладнанні масового класу, як правило, групі серверних вузлів архітектури x86-64 під керуванням ОС загального призначення (Linux, Windows, FreeBSD) [34]. Основна відмінність SDS – віртуалізація функції зберігання, що відокремлює апаратне забезпечення від програмного, яке управляє інфраструктурою зберігання.

SDS входять до нових технологій, які швидко проникають в IT-інфраструктуру організацій і компаній-провайдерів хмарних сервісів. Очікується, що за п'ять років обсяг цього ринку перевищить 16 млрд доларів. Згідно з прогнозом IDC, у період з 2020 по 2025 роки. світові витрати на програмно-визначені сховища щорічно збільшуватимуться приблизно на 13,5 % на рік і становитимуть близько 16,2 млрд доларів до кінця цього тимчасового відрізка. За прогнозами Gartner, вже протягом 2024 р. 70-80% неструктурованих даних зберігатимуться на недорогих системах, керованих за допомогою SDS, а 80% існуючих масивів зберігання стануть доступними у повністю програмній версії.

SDS є ПЗ для управління послугами зберігання на основі бізнес-орієнтованих політик незалежно від обладнання. Різні визначення програмно-визначених сховищ зазвичай включають віртуалізацію сховищ для відокремлення апаратного забезпечення від програмного, яке керує

інфраструктурою зберігання. ПЗ, що включає програмно-визначуване середовище зберігання, повинно забезпечувати гнучку організацію зберігання даних, а також управління на основі політик такими функціями, як кешування, дедуплікація, реплікація, миттєві знімки , резервне копіювання, тонке резервування.

В асоціації виробників та споживачів систем зберігання (Storage Networking Industry Association, SNIA) SDS визначають, як віртуалізоване середовище зберігання даних з інтерфейсом управління сервісами, яке повинно включати:

- автоматизацію – спрощене управління, що знижує витрати на обслуговування інфраструктури зберігання даних;
- стандартні інтерфейси – API для управління, виділення та звільнення ресурсів, обслуговування сервісів та пристроїв зберігання;
- віртуалізацію шляхів доступу до даних – блоковий, об'єктний та файловий доступ відповідно до інтерфейсів додатків;
- масштабованість – зміна інфраструктури зберігання без зниження необхідного рівня доступності чи продуктивності;
- прозорість – моніторинг споживаних ресурсів зберігання, управління ними та контроль їх вартості.

На сьогоднішній день SDS пропонують багато виробників: Dell EMC (Dell Nexenta, EMC і ScaleIO), HPE (StoreVirtual VSA), IBM (Spectrum Storage), NetApp (ONTAP Select), VMware (vSAN), Red Hat (RedHat Ceph Storage та RedHat Gluster Storage), StoneFly (SCVM, SDUS), DataCore (SANsymphony), VMware (vSAN), Virtuozzo (vStorage), Microsoft Storage Spaces Direct та ін. Умовно всі SDS можна розділити на три категорії:

- класичні (CEPH, Red Hat Storage Server, EMC ScaleIO);
- на основі традиційних систем зберігання (NetApp ONTAP Select, HPE StoreVirtual VSA);
- у складі обчислювальних комплексів (VMware vSAN).

Деякі виробники пропонують як комплексні рішення, і програмну частина (Huawei, Dell EMC). Це дозволяє гнучкіше підходити до підбору продуктів і використовувати застаріле обчислювальне обладнання для вирішення менш ресурсомістких завдань зберігання даних. Ще одна особливість SDS – можливість застосування деяких класичних СЗД віртуалізації дискових масивів. Архітектурно SDS будуються за двома принципами: слабо пов'язані та розподілені (без загальних елементів).

У першому випадку відмовостійкість забезпечується за рахунок розподілених копій даних, але через надмірність комунікацій між вузлами знижується швидкість запису. Критичним елементом є мережа передачі, тому такі рішення зазвичай реалізовані на основі InfiniBand . За таким принципом побудовано SDS VMware vSAN, HPE StoreVirtual VSA, Dell EMC ScaleIO .

У системах без загальних елементів дані записуються на один вузол, а потім із заданою періодичністю копіюються на інші для забезпечення стійкості до відмови. При цьому записи не є транзакційними, тому такий

підхід є більш економічним. Найчастіше як інтерконнект у ньому використовується Ethernet. Ця архітектура також зручна з погляду масштабованості.

На сьогоднішній день SDS є дуже затребуваними на IT-ринку, оскільки їх впровадження дозволяє отримати такі переваги: абстрагування від нижнього рівня апаратної платформи, масштабованість, спрощення інфраструктури зберігання та не потребує значних фінансових витрат.

## 2.4. Центри обробки даних

ЦОД – це спеціалізоване приміщення для розміщення серверного та мережевого обладнання, а також підключення користувачів до каналів передачі інформації. Він призначений для обробки, зберігання та розповсюдження інформації корпоративних клієнтів, як правило [35].

Побудова високопродуктивних ЦОД – один із найефективніших способів консолідації обчислювальних ресурсів обробки та засобів зберігання даних [36]. Традиційною моделлю побудови ЦОД є трирівнева модель, яка включає рівні ядра, агрегації та доступу (рис. 2.7).

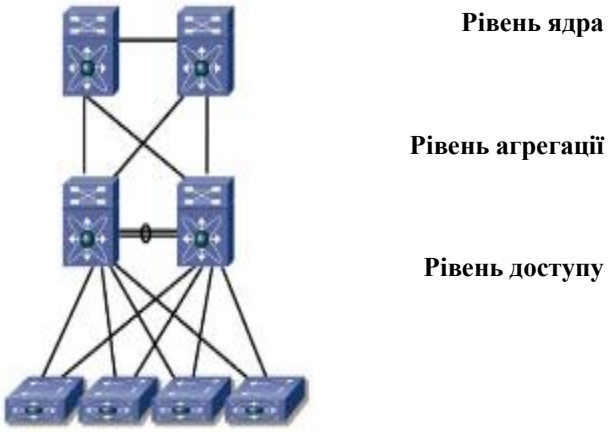



Рис. 2.7. Трирівнева модель побудови ЦОД

Ця модель сформувалася, коли потоки трафіку даних ЦОД були ще незначними [37].

Рівень ядра забезпечує швидке пересилання пакетів у напрямках від та до ЦОД. Він є точкою з'єднання всіх агрегаційних вузлів, що забезпечує маршрутизацію між ЦОД-модулем і основним ядром корпоративної мережі.

Рівень агрегації є точкою поєднання трафіку всіх серверних ресурсів, підключених до рівня доступу. Він виконує таку найважливішу функцію, як інтеграція сервісного модуля, де використовуються ключові послуги для транзитного потоку даних.

Рівень доступу є місцем фізичного підключення серверних ресурсів в ЦОД. Як правило, для побудови рівня доступу використовуються моделі Top of Rack та End of Row. У моделі Top of Rack для кожної серверної шафи ставиться невеликий комутатор доступу до фіксованої або модульної

конфігурації. При цьому сервери з'єднуються мідними кабелями з комутаторами. Комутатори доступу поєднуються оптичними каналами зв'язку з рівнем агрегації. У моделі End of Row використовуються модульні комутатори рівня доступу, які знаходяться у шафах, куди засобами структурованої кабельної системи (СКС) комутуються всі з'єднання із серверами. Між серверами та комутаторами доступу використовуються мідні з'єднання, між комутаторами доступу та комутаторами агрегації – оптичні з'єднання.

При побудові мережної інфраструктури ЦОД українських підприємств та організацій зазвичай застосовують дворівневу модель. У такій моделі як ядро мережної інфраструктури ЦОД використовується ядро корпоративної мережі. Двохрівнева модель здешевлює вартість побудови ЦОД, але при цьому обмежує можливості масштабування IT-інфраструктури у разі використання підприємством кількох ЦОД.

В останні роки спостерігається активний розвиток інноваційних технологій для ЦОД. Так, наприклад, компанія Cisco Systems випустила серію комутаторів Nexus , що дозволяють реалізувати нову модель побудови рівня доступу – Distributed Access Fabric (DAF). Основна відмінність цієї моделі полягає у побудові єдиної розподіленої фабрики комутації для рівнів доступу та агрегації. Комутатори рівня доступу виступають як модулі, керовані комутатором агрегації.

Основні переваги моделі DAF:

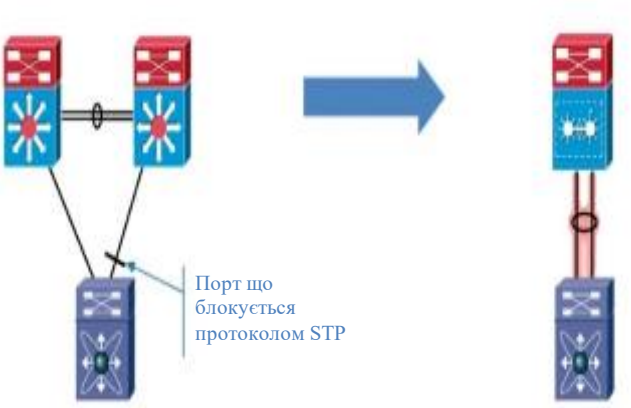
- єдина керуюча компонента для комутаторів рівня доступу та агрегації;
- єдина уніфікована комутаційна фабрика, що дозволяє передавати як IP-дані, так і Fiber Channel-дані у напрямку Storage Area Network (SAN);
- значне розширення комутаційної матриці, порівняно з моделями Cisco Catalyst 6500 серії;
- спрощення топології СКС та зменшення вартості її побудови;
- можливість вирішення проблеми поділу зон відповідальності між SAN-адміністраторами та адміністраторами IP-мережі.

Ще однією інновацією компанії Cisco Systems у галузі віртуалізації ЦОД є використання технології Virtual Switching System (VSS) на базі комутаторів Catalyst 6500. Дана технологія спільно з Spanning Tree Protocol (STP) дає можливість логічно об'єднати два шасі в одне, що дозволяє отримати загальну контрольну компоненту та загальну матрицю комутації. Схема STP із використанням VSS-технології представлена на рис. 2.8.

Такий підхід має такі переваги:

- об'єднання розподіленого L2 домену, що дозволяє будувати Etherchannel між рівнями ядра та агрегації;
- забезпечення швидкої збіжності мережі у разі виходу з експлуатації одного з шасі, модуля шасі;

- можливість побудови загальної контрольної компоненти для обох шасі, що значно полегшує адміністрування мережі.




**Вигляд логіки STP** **Мультишассійна агрегація каналів (виглід логіки STP)**

Рис. 2.8. Схема STP із використанням VSS-технології

Компанія Juniper Networks випустила серію міжмережевих екранів (MCE) SRX, які дозволяють вирішити одну з головних проблем ЦОД – збільшення продуктивності MCE. Дане сімейство MCE забезпечує продуктивність до 120 Gbps та Intrusion. Detection System до 30 Gbps . Побудова віртуального шасі на основі комутаторів Juniper EX 4200 серії дозволяє спростити топологію СКС за рахунок зменшення кількості з'єднань між рівнем доступу та рівнем агрегації, а також створити єдину комутаційну матрицю та контрольну компоненту між групою комутаторів різної конфігурації (до 10 комутаторів). Дане рішення можна використовувати як для Top of Rack, так і для End of Рівень моделей рівня доступу.

У моделі Top of Rack будується кільце між комутаторами кожної з шаф. Відстань між двома комутаторами, що з'єднуються, не повинна перевищувати 5 метрів. Для побудови Virtual chassis між кількома рядами використовують додаткові uplink-модулі або Ethernet-порти у відповідному режимі. У моделі End of Row комутатори, що утворюють Virtual chassis, розміщуються в одній шафі і з'єднуються між собою daisy-chained способом. Серверні шафи поєднуються з комутаційними шафами за допомогою СКС. Такий варіант є більш масштабованим та гнучким з точки зору нарощування продуктивності та збільшення кількості шаф у ЦОД.

Деякі виробники замість традиційної трирівневої моделі побудови ЦОД використовують власні моделі. Так, наприклад, компанія Extreme Networks пропонує Direct-Attach модель, яка дозволяє зменшити кількість рівнів за рахунок підключення blade-серверів безпосередньо до комутатора агрегації, укомплектованого модулями з великою кількістю портів. Така модель пред'являє певні вимоги до матриці комутації і Extreme Networks забезпечує їх виконання засобами комутаторів Black Diamond 8900 серії. Основна перевага застосування Direct-Attach моделі полягає у використанні модулями

в шасі комутатора MRJ21 технології, що дозволяє об'єднати 6 Ethernet-кабелів в один і тим самим спростити топологію СКС у разі відсутності Top of Rack або Blade-комутаторів.

Таким чином, розглянуто традиційну трирівневу модель побудови ЦОД, дворівневу, а також моделі DAF та Direct-Attach, компаній Cisco Systems та Extreme Networks, їх особливості, переваги та недоліки.

### 2.5. Комплексний підхід до управління даними

Організації та підприємства різних галузей щодня займаються вирішенням безлічі завдань з обробки та зберігання зростаючих обсягів даних, контролю доступу до них, дотримання нормативних вимог підтримки оперційних процесів та забезпечення їх безперервності [38]. При цьому інфраструктура зберігання даних має давати можливість раціонального використання ресурсів, бути гнучкою та сприяти мінімізації витрат на керування інформацією.

Враховуючи, що в даний час дані є одним із найбільш цінних активів будь-якої організації, необхідно більше уваги приділяти управлінню цими даними. Тому завдання такого роду дуже актуальні і вимагають якісно нових рішень, орієнтованих на комплексний підхід до управління даними та забезпечення ефективної роботи підприємств та організацій [39].

#### 2.5.1. Концепції зберігання та управління даними

Для вирішення завдань зберігання та управління даними існує кілька концепцій, що описують правила зберігання, а також розроблені відповідні технології їх реалізації.

Найбільш відомими прикладами можуть бути: концепція, запропонована компанією EMC для вирішення завдань резервного копіювання, відновлення та архівування даних – BURA (Backup, Recovery and Archive) та концепція резервного копіювання та аварійного відновлення даних (Backup&Recovery), спрямована на забезпечення безперервності функціонування організації. Вони реалізовані, як різні рішення: від традиційного бекапу окремої, критичної БД, до реалізації технології безперервного захисту даних (Continuous Data Protection – CDP) для організацій корпоративного рівня.

Досить схожою концепцією є архівування оригінальної інформації (Archive), спрямоване переміщення еталонних даних для безстрокового чи довгострокового зберігання високонадійний носій. У більшості випадків за допомогою технології одноразового запису з багаторазовим читанням (Write Once Read Many – WORM).

Ще одним прикладом є концепція управління життєвим циклом інформації (Information Lifecycle Management – ILM), яка дозволяє оптимізувати використання ресурсів зберігання та забезпечити доступ до них із мінімальними витратами. Вона передбачає переміщення даних відповідно до їх затребуваності та поточної цінності між різними рівнями зберігання, які

відрізняються вартістю самого ресурсу зберігання, включаючи показники його продуктивності та захисту від відмов.

Для невеликих підприємств та організацій реалізація будь-якої з обраних концепцій може бути здійснена як за допомогою окремих продуктів різних виробників, так і за допомогою певного набору таких продуктів. У свою чергу, для великих корпорацій саме комплексний підхід до управління даними є пріоритетним, оскільки дозволяє ефективніше вирішити основні завдання з управління даними:

- інтегрувати в єдиний репозиторій гетерогенне обладнання різних виробників, розподілене по безлічі майданчиків;
- уніфікувати захист неоднорідної інформації у складній та розподіленій IT-інфраструктурі;
- організувати контроль за безпекою конфіденційних даних на мобільних пристроях користувачів;
- забезпечити відповідність вимогам національних та міжнародних регуляторів під час проходження аудиту.

Таким чином, в даний час розроблено різні технології для реалізації концепцій резервного копіювання та аварійного відновлення, архівування та управління життєвим циклом інформації. Більшість цих технологій базується на програмних та апаратних платформах відомих галузевих лідерів і заслужено займає свою нішу на малих та середніх підприємствах. Але організаціям корпоративного рівня, для яких комплексний підхід до управління даними є більш ефективним, пропонується використовувати платформу CommVault Simpana .

### 2.5.2. Комплексне управління даними за допомогою CommVault Simpana

Компанія CommVault є одним із лідерів ринку систем резервного копіювання та управління і неодноразово включалася до Gartner квадрант «Лідери» дослідження «Enterprise backup and integrated appliance». Зі своїм флагманським продуктом Simpana вона також є лідером галузі, на думку аналітиків: A Лідер: Forrester Wave: Enterprise Backup and Recovery Software; №1 for Enterprise Backup Applications у журналі Storage Magazine у номінації якості; №23 у списку Forbes of America's 25 технологічних компаній, що найбільш швидко ростуть; названо «Champion» у ряді звітів Info-Tech Research Group (Backup Software for Heterogeneous Environments Vendor Landscape, Virtual Backup Vendor Landscape та Email Archiving Vendor Landscape).

Повністю реалізувати функціонал, аналогічний функціональним можливостям Simpana, можна лише за допомогою досить великого набору продуктів різних виробників (рис. 2.9). При цьому вони будуть з різними інтерфейсами управління, з різними ресурсами зберігання, що, у свою чергу,

призведе до ускладнення та збільшення вартості впровадження та подальшої підтримки.

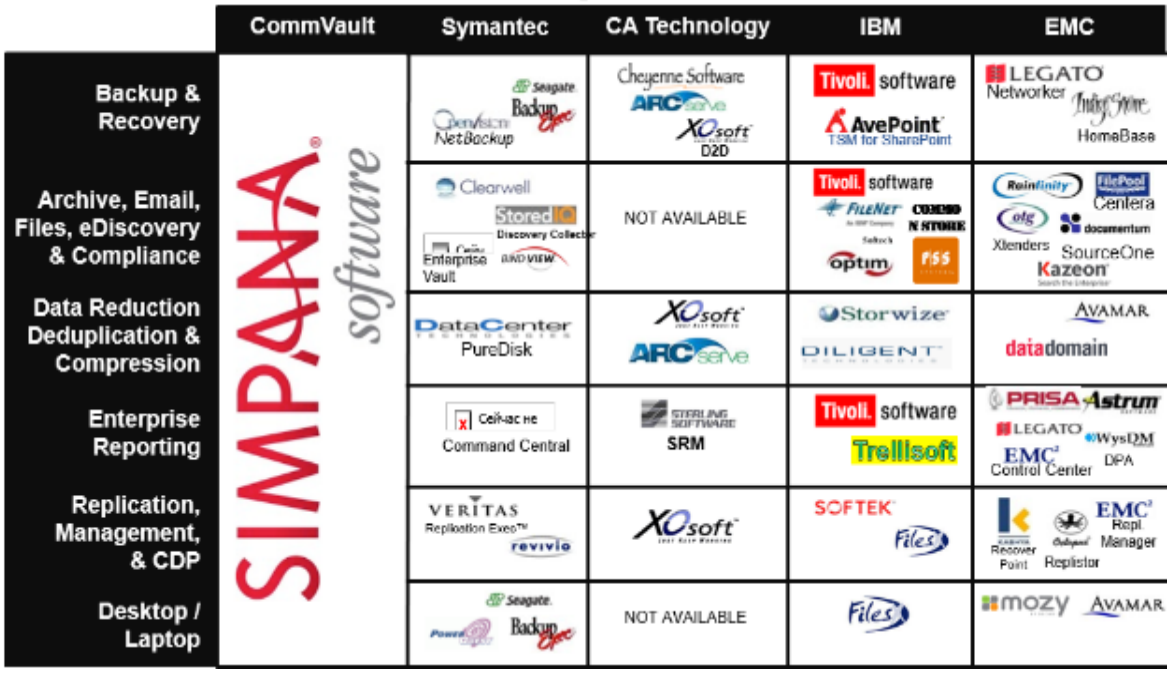



Рис. 2.9. Порівняння функціональних можливостей Simpana із продуктами інших виробників

Simpana пропонується в рамках OEM-партнерства таким лідером систем зберігання, як HDS, у редакції Hitachi Data Protection Suite (HDPS). CommVault Simpana є єдиною платформою для захисту та управління всією інформацією підприємства: від даних додатків користувача та ОС до корпоративних СЗД та ресурсів хмарних провайдерів. З її допомогою реалізуються: резервне копіювання даних, включаючи віртуальні середовища; автоматичний контроль віртуальної інфраструктури; перенесення ВМ між різними гіпервізорами; перенесення фізичних машин у віртуальне середовище; архівування електронної пошти, файлових серверів, ВМ, БД; захист даних персональних комп'ютерів із захистом від втрати ноутбука; створення індексованого сховища з повнотекстовим пошуком; контроль вмісту щодо несанкціонованого контенту; портал самообслуговування для самостійного відновлення даних користувачами; відповідність вимогам регуляторів та проведенню службових розслідувань щодо захисту даних (E-discovery, Compliance, Legal hold). Структура CommVault Simpana представлена на рис. 2.10.

Основними її компонентами є:

- CommServe – керуючий сервер Simpana ;
- ContentStore – єдиний набір ресурсів для зберігання даних. Це можуть бути СЗД (в тому числі і програмно-визначені СЗД), будь-які backup appliance, файлові сервери, стрічкові бібліотеки, хмарні сховища Amazon, Microsoft Azure та ін;

- Data Agent – агент для додатків та файлових систем. Виконує також функції компресії, дедуплікації та шифрування на джерелі (source side dedup compression);
- Media Agent – медіаагент Simpana , що приймає потік даних Data Agent, який реалізує обрану політику зберігання, записуючи дані на відповідні носії в ContentStore. Медіаагент також безпосередньо виконує процес дедуплікації даних на одержувачі (target-side dedup).

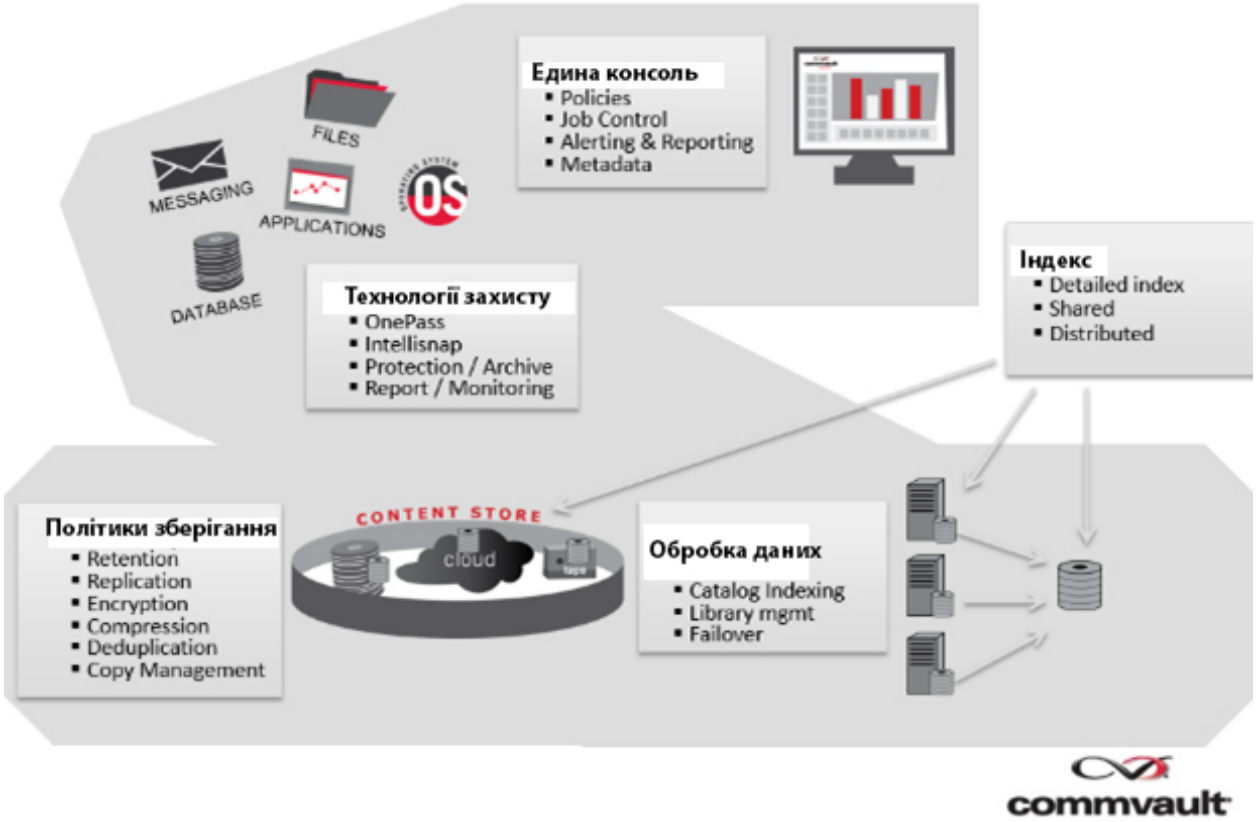



Рис. 2.10. Структура платформи CommVault Simpana

Для захисту та управління даними реалізовані такі підходи, як уніфікований процес архівування та резервного копіювання даних (OnePASS), єдиний репозиторій для зберігання, індексування та глобальної дедуплікації (ContentStore). Особливістю платформи CommVault Simpana є її горизонтально масштабована архітектура як за продуктивністю, так і за обсягом.

Якщо раніше Simpana був виключно ПЗ, яке встановлювалося на апаратне забезпечення, налаштоване залежно від потреб користувача, то з появою Storage Appliance компанії CommVault, спільно з партнерами Fujitsu і NetApp, були розроблені програмно-апаратні комплекси для зберігання архівів та резервних копій. Окрім цього, оновлення торкнулися і найбільшого OEM-постачальника CommVault – компанії Hitachi Data Systems, де пристрої зберігання HDS комплектуються ПО Simpana, в редакції HDS – HDPS і також інтегрується з пристроями зберігання єдиний програмно-апаратний комплекс.

Функціональні оновлення у версії.10 R2 Service Pack 1, окрім традиційних покращень та розширення функціональних можливостей у галузі інформаційної безпеки та моніторингу, також торкнулися віртуальної інфраструктури, публічних хмар та захисту робочих місць користувачів, включаючи мобільні пристрої. Для підтримки віртуалізації в ОС – UNIX, IBM AIX і ORACLE/SUN Solaris пропонується робота на рівні агентів Simpana, що встановлюються всередині самих розділів відповідної ОС (LPAR/WPAR або Containers). Більшість змін торкнулися традиційних платформ віртуалізації для x86 архітектури від Microsoft, XEN і VMware, причому для останньої істотно розширений спектр можливостей, включаючи підтримку vSphere 6, VSAN 2.0 і vVols.

При інтеграції приватних хмар на базі перелічених вище гіпервізорів з публічними хмарами MS Azure і Amazon, взаємодія здійснюється без встановлення будь-яких агентів, а безпосередньо через API цих хмарних інфраструктур. Завдяки такій інтеграції можна виконувати функції створення, управління життєвим циклом та автоматичного призначення політик як для локальних віртуальних середовищ на основі VMware та HyperV, так і для віддалених хмарних – Amazon та MS Azure. Така функціональна можливість, як конвертація ВМ за допомогою Virtualize me між VMware і HyperV, тепер можлива і на VMware з MS Azure , що дозволяє спростити міграцію ВМ у хмарні середовища. Для зберігання даних, крім підтримки Amazon S3/Glacier, додався і Google Cloud Platform. За аналогією з Amazon, у Google Cloud даними можна керувати на двох рівнях зберігання: оперативному та довготривалому зі зниженою доступністю (Standard/Durable Reduced Availability).

Такий широкий спектр функціональних можливостей є унікальним на ринку платформ для управління даними, що дозволяє позиціонувати CommVault Simpana, як справді «гібридне» хмарне рішення.

У оновлених версіях CommVault Simpana реалізовано функцію захисту робочих місць користувачів. Основні зміни торкнулися модулів Endpoint Data Protection (резервне копіювання робочих місць) та EDGE drive (синхронізація файлів і папок як між різними пристроями, так і з внутрішньою хмарою зберігання). Модуль Endpoint Data Protection підтримує весь функціонал резервного копіювання для нової ОС Windows 10, включаючи відновлення образу машини цілком (One Touch). У модулі EDGE drive оновилися програми для мобільних пристроїв на базі Android, iOS, Windows. Для синхронізації даних можна скористатися кількома режимами роботи з різними папками. Синхронізація папок та файлів між комп'ютерами може бути односпрямованою, якщо цільова папка знаходиться в режимі read only, або двонаправленою, якщо файли можуть бути редаговані на будь-якому пристрої. Також є можливість інтеграції з Office 2013 завдяки підключенню EDGE drive за допомогою MS Office Connected Services, що робить роботу користувачів із сховищем CommVault повністю прозорим.

Розширення можливостей Comm Vault Endpoint Data Protection Solution Set для полегшення роботи в гібридному середовищі, дає можливість IT-службі бачити дані на сервісах обміну файлами OneDrive, Dropbox і, відповідно, захищати їх відповідно до стандартів інформаційної безпеки, тим самим мінімізуючи ризики при використанні хмарних публічних сховищ. Подальший розвиток платформи Simpana спрямовано збільшення як її продуктивності, і кількості корпоративних користувачів, активну підтримку інтелектуальної системи аналітики у масштабі реального часу. Завдяки цьому значно збільшаться можливості масштабування архітектури, а нові методи індексації збільшать продуктивність. Також з'являться нові механізми оркестрації функції відновлення для роботи в Azure та Amazon, а підтримка VSA поширеться на Redhat RHEV (KVM), Nutanix Acropolis (AHV) та OpenStack платформи.

Таким чином, комплексний підхід до управління даними може бути рекомендований для застосування у всіх організаціях та підприємствах корпоративного рівня, оскільки істотно підвищує ефективність управління даними, а завдання розробки якісно нових технологій для його реалізації є дуже актуальним.

# РОЗДІЛ 3
# ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ

Метою даного розділу є огляд основних мережевих технологій, що сформували історію розвитку корпоративних мереж, а також їх еволюція від набору різних технологій до єдиної мультисервісної мережевої інфраструктури, що нерозривно пов'язана зі світовою глобальною мережею Internet, що є для більшості сучасних корпоративних мереж одночасно і сервісом, і транспортним середовищем [40].

## 3.1. Корпоративні мережі передачі даних

### 3.1.1. Корпоративна мережа та її компоненти

Визначення «корпоративна мережа» в сучасному розумінні є комплексним і традиційно має на увазі набір базових компонентів, що взаємодіють (рис. 3.1), серед яких: Main Site – мережа головного офісу; Remote Site (Branch) – мережі віддаленого офісу, Wide Area Network (WAN) – глобальна мережа, що об'єднує мережі офісів; LAN – локальна мережа; WAN Edge – точка підключення до WAN. Internet Edge – точка підключення до Internet, Data Center – корпоративний ЦОД. У деяких джерелах також розглядається Service Block – окрема частина мережі, що містить специфічні мережеві службові сервіси, такі як, наприклад, wireless-контролери, термінація ISATAP тунелів, Unified Communications services і т.д.

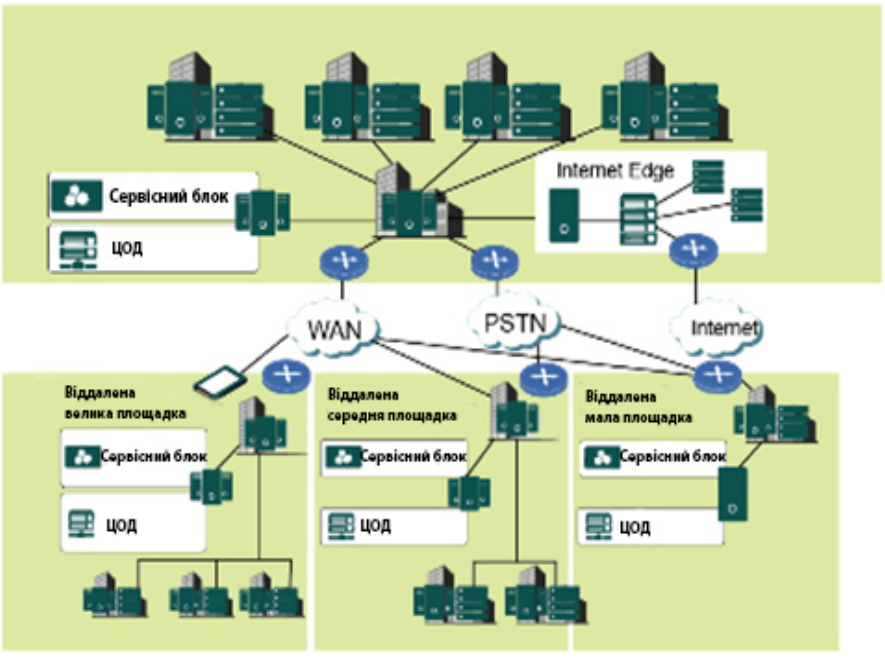



Рис. 3.1. Компоненти корпоративної мережі

Кожен компонент корпоративної мережі включає в себе власний набір технологій, кожна з яких, у свою чергу, має історію виникнення та розвитку.

### 3.1.2. Тенденції розвитку корпоративної мережної інфраструктури

Ще недавно для надання сервісів телефонії, відеозображення та передачі даних потрібно будувати майже повністю незалежні інфраструктури. Особливо це було актуально для територіально розподілених організацій корпоративного рівня. Потім з'явилися мультисервісні мережі, здатні передавати голос, відео та дані в рамках єдиної корпоративної телекомунікаційної структури. Це значно зменшило вартість володіння, дозволило підтримувати складні мультимедійні прикладні програми та розширити функціональні можливості мережного обладнання.

В останні роки спостерігалися тенденції розвитку корпоративної мережевої інфраструктури за рахунок включення до її складу: маршрутизаторів та комутаторів мережі [41]. Вони вийшли за звичні рамки апаратного забезпечення. ОС на мережевому обладнанні дозволяє реалізовувати додаткові можливості не тільки на рівнях L2–L4, але і на більш високих, згідно мережевої OSI моделі.

Компанії-виробники не зупиняються на досягнутому та надають можливість розширення програмного підходу до мережного обладнання. Відкритий програмний інтерфейс взаємодії з мережею розширює існуючі підходи до створення програмно-орієнтованих інфраструктур, дозволяючи контролювати її рівні.

Один із таких прикладів – платформа Cisco Open Network Environment (ONE). Вона реалізована на принципі «policy, one management, one network» та у формі широкого набору API-інтерфейсів для ОС Cisco IOS, IOS-XR та NX-OS. Пакет One Platform Kit (onePK) дає розробникам можливість використовувати API-інтерфейси під час створення ПЗ.

Однією зі складових частин Cisco ONE є комутатор лінійки Cisco Catalyst 3850, який інтегрований функціонал бездротового контролера Wireless LAN C ontroller (WLC). Такий підхід дозволяє нарощувати функціонал без встановлення додаткового обладнання, а також спрощує схему реалізації мережі. Розглянемо приклад реалізації цього підходу на схемі організації віддаленого офісу.

Для реалізації централізованого сервісу бездротового доступу на віддаленому сайті раніше необхідно було встановлювати окремий WLC або організовувати доступність контролера WLC у центральному офісі. Для цього також необхідно по всьому шляху між точкою доступу і контролером впровадити політики якості обслуговування – Quality of Service (QoS), які мають суттєві обмеження для тунельного трафіку. Маючи функціонал бездротового контролера WLC на комутаторі доступу, схему реалізації можна значно спростити (рис. 3.2).

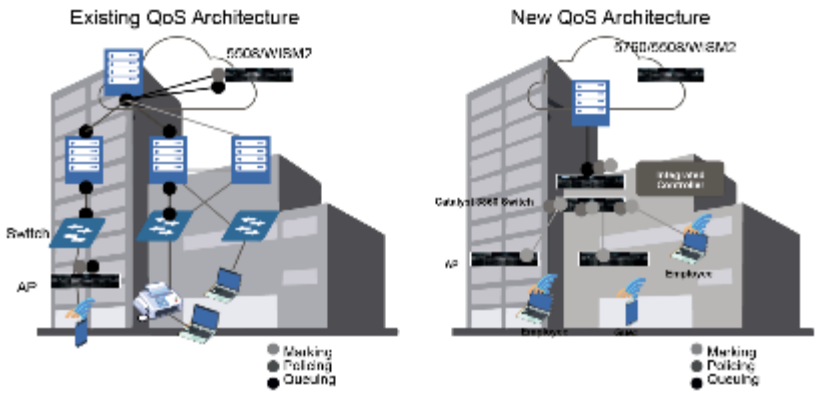



Рис. 3.2. Схема реалізації QoS при класичному та новому підходах із використанням Cisco Catalyst 3850

Такий підхід дозволяє збільшити «прозорість» усієї мережі, оскільки трафік бездротових користувачів більше не інкапсулюється в тунель, а передається як звичайний трафік даних. Іншими словами, бездротовий трафік доступний так само, як і провідний, для застосування корпоративних політик підприємства та аналізу.

Масштабування цієї схеми досягається шляхом стекування комутаторів. Це дозволяє реалізувати мережу з підтримкою до 50 точок доступу та 2000 бездротових користувачів для кожного стека без використання окремого контролера WLC .

Наступний складовий компонент Cisco ONE – розширена лінійка комутаторів Cisco Catalyst 4500E Series Switches для рівня доступу та агрегації кампусних мереж. Використання супервізора нового покоління Supervisor 8-E дозволяє на одному пристрої розширити функціонал для дротового трафіку на бездротових користувачів за аналогією з Cisco Catalyst 3850. Одна система з Supervisor 8-E підтримує до 50 точок доступу та 2000 бездротових клієнтів.

При використанні мультишасійної схеми, наприклад, VSS, максимальні показники можна збільшити до 250 точок доступу та 4000 бездротових користувачів, без використання окремого контролера WLC. Застосування такого походу краще, якщо в існуючій мережі вже використовуються комутатори серії Cisco Catalyst 4500E. Обновивши супервізор, можна отримати новий функціонал із мінімальною зміною архітектури.

Ще однією зі складових частин Cisco ONE є модуль Cisco Catalyst 6500 Series Wireless Services Module 2 (WiSM 2) або Cisco 5508 WLC, які використовуються для великих кампусних мереж і дозволяють централізовано керувати мережею з 1000 точок доступу та 15000 клієнтів. У найближчому майбутньому підтримка платформи Cisco ONE буде розширена і на інші лінійки продуктів, а також доповнена новими можливостями.

Підхід до інтеграції різного виду сервісів в одне фізичне обладнання використовують інші компанії – виробники мережного обладнання, що дозволяє консолідувати функціонал маршрутизації, комутації, безпеки та гнучких можливостей для об'єднання LAN і WAN-сегментів мережі,

використання унікальних можливостей світової мережі Internet. Такий підхід дає змогу зменшити кількість різного обладнання у віддалених офісах, що, у свою чергу, зменшує витрати на підтримку та розвиток корпоративної мережі.

Таким чином, основний напрямок розробок виробників мережного обладнання спрямований у бік уніфікації та консолідації. Відкриті програмні інтерфейси взаємодії з мережею активно розвиваються і дають можливість стороннім розробникам реалізовувати інноваційні підходи незалежно від компаній-виробників, а підходи та способи побудови корпоративної мережевої інфраструктури постійно еволюціонують через зміни потреб бізнесу та розвитку технологій.

### 3.1.3. Локальні мережі

Початок історії локальних мереж передачі даних LAN було покладено в 1973 р. інженером компанії Xerox Робертом Меткалфом (Robert Metcalfe) (рис. 3.3), який створив проект експериментальної мережі, що отримала назву Ethernet і призначена для з'єднання декількох персональних комп'ютерів (з графічним інтерфейсом) Xerox Alto, серверів, а також – лазерних принтерів (рис. 3.4).


Рис. 3.3. Роберт Меткалф

Рис. 3.4. Робоча станція Xerox Alto

Фізична швидкість у цій мережі становила 2.94 Мб/с. Дане технічне рішення було розвитком більш раннього проекту Alto Aloha Network (рис. 3.5).

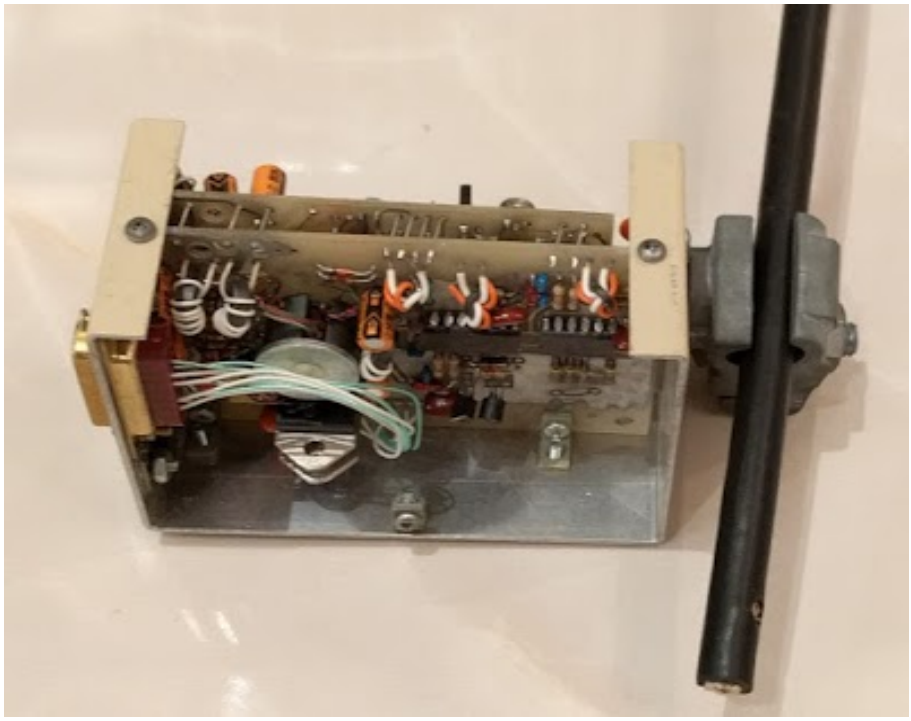


Рис. 3.5. Ethernet-трансівер для Xerox Alto

Назва Ethernet ґрунтувалася на слові «ether» (ефір), що натякало на одночасну передачу бітової інформації у фізичному середовищі всім учасникам мережі (рис. 3.6).

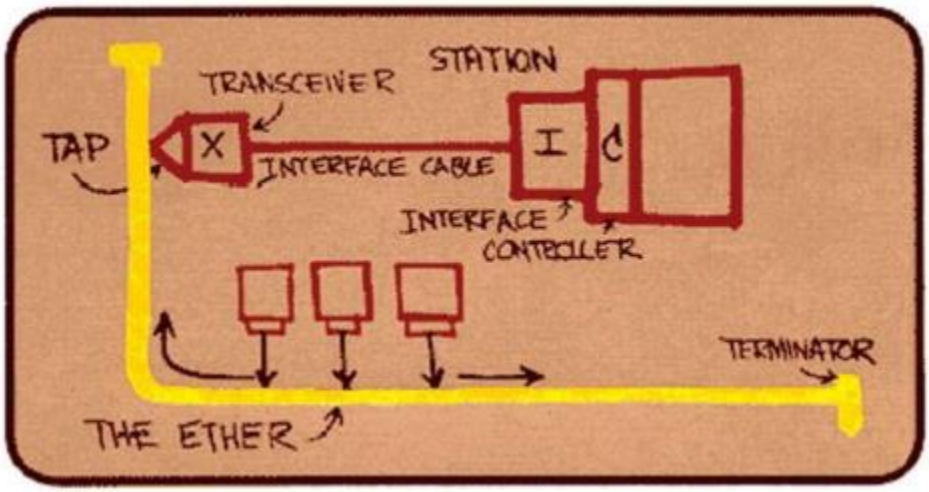



Рис. 3.6. Оригінальний авторський малюнок, який розкриває фізичний принцип Ethernet

Першу спробу стандартизувати Ethernet зробив консорціум, що включає компанії: DEC, Intel, Xerox. Стандарт отримав назву DIX (перші літери назв компаній). Останнім стандартом DIX, який побачив світ, був DIXv 2.0 (*The Ethernet, A Local Area Network: Data Link Layer and Physical Layer Специфікації*).

Технологія стала загальновизнаним стандартом у 1985 р. в результаті роботи Інституту інженерів електротехніки та електроніки – IEEE (Institute of Electrical and Electronics Engineers). Стандарт носить назва IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. IEEE, в процесі створення стандарту, дистанціювався від комерційної назви Ethernet, проте ця назва міцно закріпилася в середовищі виробників.

Далі стандарт активно розвивався шляхом переробок та внесення доповнень (supplements). Відносна простота поряд зі своєчасними поліпшеннями дозволили технології Ethernet (IEEE 802.3) проникнути майже у всі сфери застосування мереж передачі даних – від LAN до глобальних (WAN). Тому на сьогодні сучасна частина дерева стандартів IEEE 802.3 (наприклад 1000 BASE-T, 1000 BASE-LX, 1000 BASE-SX, 10G BASE-SR, 10G BASE-LR та інші) поряд з WI-FI (IEEE 802.11) лягли в основу сучасних enterprise-мереж.

Кількість доповнень стандарту яскраво ілюструє великий обсяг напрацювань, накопичений цією технологією у процесі активного розвитку (табл. 3.1). Стек протоколів TCP/IP дав можливість уніфікувати передачу даних у мережах і легко підключати локальні мережі до Інтернету.

Таблиця 3.1. Доповнення стандарту IEEE 802.3

| Доповнення стандарту IEEE 802.3 | Рік створення | Опис |
|---|---|---|
| 802.3a | 1985 | 10BASE2 thin Ethernet |
| 802.3c | | 10 Mbps repeater specifications, clause 9 |
| 802.3d | 1987 | FOIRL fiber link |
| 802.3i | 1990 | 10BASE-T twisted-pair |
| 802.3j | 1993 | 10BASE-F fiber optic |
| 802.3u | 1995 | 100BASE-T Fast Ethernet and Auto-Negotiation |
| 802.3x | 1997 | Full-Duplex standard |
| 802.3z | 1998 | 1000BASE-X Gigabit Ethernet |
| 802.3ab | 1999 | 1000BASE-T Gigabit Ethernet over twisted-pair |
| 802.3ac | 1998 | Frame size extension to 1522 bytes for VLAN tag |
| 802.3ad | 2000 | Link aggregation for parallel links |
| 802.3ae | 2002 | 10-Gigabit Ethernet |
| 802.3af | 2003 | Power over Ethernet – перший стандарт керування для цієї технології |
| 802.3ah | 2004 | Ethernet for First Mile |
| 802.3ak | 2004 | 10G-Base-CX4 10Gbps, Ethernet over twinaxial cables |
| 802.3an | 2006 | 10G-Base-T 10Gbps over unshielded twisted pair, UTP |
| 802.3ap | 2007 | Backplane Ethernet, 1 & 10 Gbps over a PCB |
| 802.3aq | 2006 | 1-G-Base-LRM 10 Gbps over multimode fibre |
| 802.3as | 2005 | Frame expansion |
| 802.3at | 2005 | Power over Ethernet Plus – навантаження на 25.5W |
| 802.3au | 2006 | Isolation requirements for Power over Ethernet |
| 802.3av | 2009 | 10 Gbps |
| 802.3ax | 2008 | Link aggregation – see IEEE 802.1ax |
| 802.3az | 2010 | Energy efficient Ethernet |
| 802.3ba | 2010 | 40Gbps & 100Gbps Ethernet |
| 802.3bc | 2009 | Update Ethernet Type, Length & Value, TLVs, що були попередньо визначені в 802.1AB to 802.3 |
| 802.3bd | 2011 | Priority based flow control |

| | | |
|---|---|---|
| 802.3bf | 2011 | Provision of accurate indication of transmission and reception initiation times of some packets to support IEEE P802.1AS |

Сучасні стандарти Ethernet практично не схожі на свою технологію. Середовищем передачі є так звана кручена пара, або оптоволокно. Швидкості передачі в цих середовищах набагато вищі. До того ж, середовище передачі давно не є роздільним – кожен кадр, згенерований хостом, не передається обов'язково всім іншим хостам. Для цього в передачі даних бере участь активне обладнання, здатне запам'ятовувати належність MAC-адрес і після навчання на основі трафіку мережі комутувати кадри Ethernet тільки для хостів, відповідних MAC-адресу одержувача. Оскільки сучасні стандарти Ethernet передбачають два незалежні канали передачі в протилежних напрямах, поняття «колізій» і «доменів колізій» втратило свою актуальність. Прямий та зворотний потоки трафіку не відчувають взаємного впливу, що на рівні комутаторів досягається за допомогою спеціальної матриці комутації.

Проте Ethernet не втратив деяких своїх рудиментарних недоліків. Одним з них є BUM (Broadcast, Unknown unicast and Multicast) трафік, марнотратно витрачає пропускну здатність мережі. Причина існування даного трафіку криється, по-перше, особливо роботи протоколу ARP, покликаного відображати Інтернет-адреси (IPv 4 адреси) одержувачів на їх адреси в рамках фізичного середовища передачі (MAC-адреси), для чого спочатку необхідно опитувати всі хости-учасники підмережі на предмет володіння шуканою IP-адресою. По-друге, комутатор, який не має у своїй таблиці комутації MAC-адреси хоста – одержувача, змушений транслювати кадр у всі свої порти (усім одержувачам).

Всі перелічені недоліки походять від спочатку простого призначення даного протоколу і, безумовно, мають велике значення у використанні Ethernet для WAN-мереж та мереж операторів зв'язку.

Зростаюча кількість користувачів, збільшення обсягів трафіку разом із вимогами надійності вплинули на дизайн локальних мереж. Ієрархічний дизайн мережі став вирішенням проблем масштабованості, розширюваності та надійності мережі. Згідно з вимогами ієрархічного дизайну мережа стала багаторівневою. Традиційно в мережі виділяють три рівні: рівень доступу (Acce ) – обладнання для підключення користувачів мережі; рівень розподілу ( Distribution ) – обладнання для об'єднання пристроїв доступу, відповідальне за найбільш інтелектуальний функціонал мережі такий, як, наприклад, VLAN-сегментація, L3-комутація, фільтрація пакетів тощо; рівень ядра (Core) – устаткування, що об'єднує пристрої рівня розподілу та відповідальне за швидку комутацію (зазвичай це L3 – комутація) трафіку. Ієрархічний дизайн локальної мережі представлено на рис. 3.7.

У подібних топологіях активно використовується резервування пристроїв та лінків між ними. Традиційно для запобігання логічних петель, за наявності надлишкових L2-лінків, та перемикання маршрутів, при відмови L3-лінків,

використовуються відповідно Spanning Tree в декількох модифікаціях та IGP-протоколи маршрутизації, такі як, наприклад, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP).

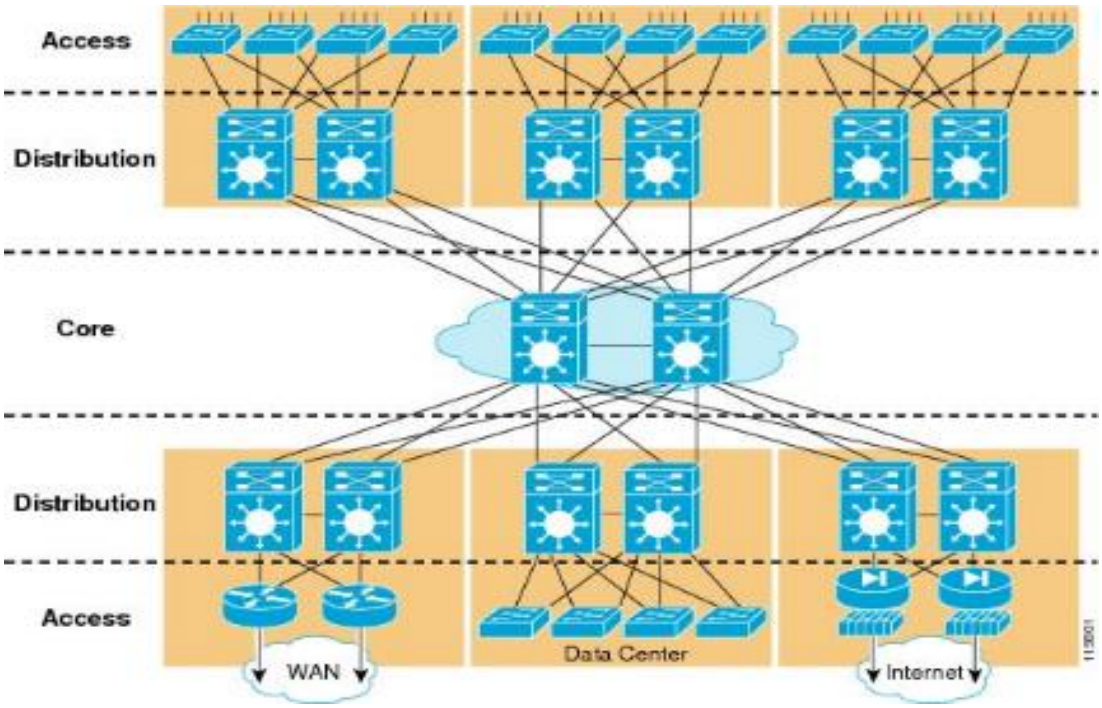



Рис. 3.7. Ієрархічний дизайн локальної мережі

З розвитком технологій кластеризації та стекування обладнання з'явилася можливість замінити Spanning Tree на EtherChannel, перетворивши незалежні лінки, що резервують один одного, в учасників одного загального EtherChannel-лінка (рис. 3.8).

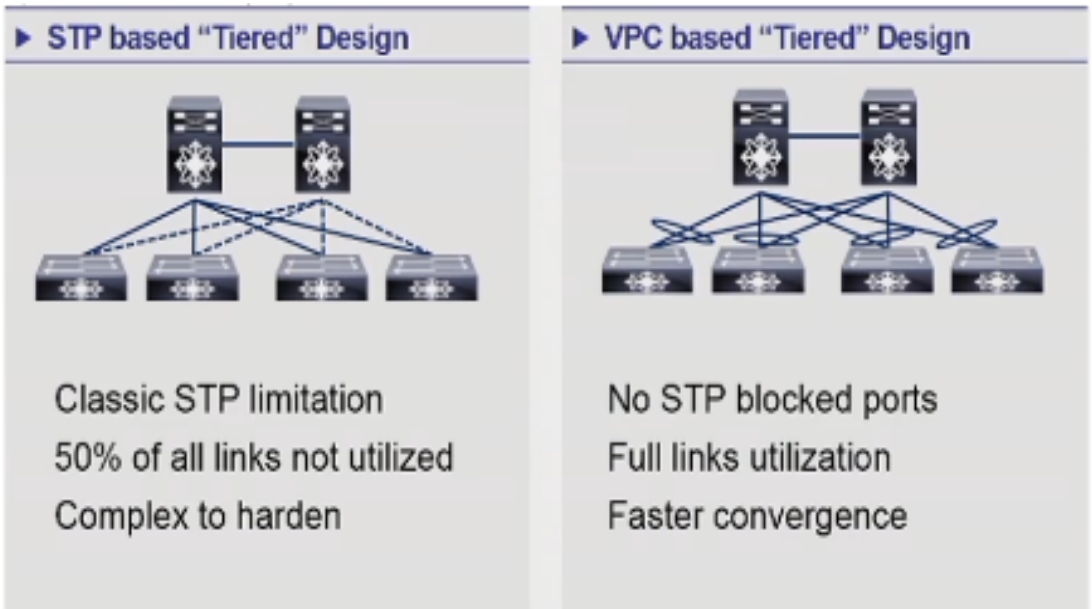



Рис.3.8. Перехід від Spanning Tree до кластеризації та EtherChannel

Кластеризовані або стековані для резервування фізичні пристрої є одним логічним. Оскільки EtherChannel завжди означає один логічний лінк між двома пристроями, то утворення логічних кілець між його фізичними лінками-учасниками неможливе. Такий підхід дозволяє легко балансувати трафік.

### 3.1.4. Глобальні мережі

На відміну від мереж LAN, покликаних пов'язувати набір офісного комп'ютерного устаткування, глобальні мережі створювалися зв'язку географічно рознесених об'єктів. Враховуючи велику довжину необхідних каналів передачі, було логічно використовувати готову інфраструктуру операторів зв'язку.

Історія WAN-мереж почалася зі стандарту X.25, розробленого комітетом ITU-T. Стандарт був реалізований і набув популярності в 70-х, 80-х рр. н. минулого сторіччя. X.25-мережа на основі комутації пакетів, що має власний стек протоколів з спеціальним комутуючим обладнанням. Першим застосуванням мереж X.25 було використання зв'язку віддалених терміналів з мейнфреймами (рис. 3.9).

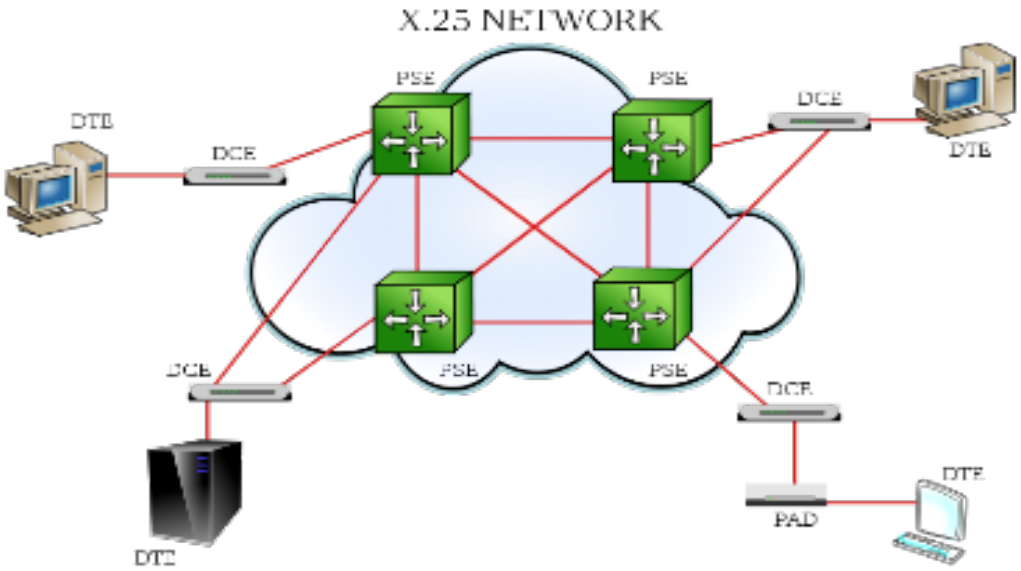



Рис. 3.9. Мережа X.25

Для об'єднання LAN у 80-ті роки. активно використовувалися цифрові виділені point-to-point канали. Це були канали DS0 (56 Kbps) або дорожчі T1/E1, T3/E3. Спочатку даний тип каналів (E1) розроблявся для передачі голосу (рис. 3.10).

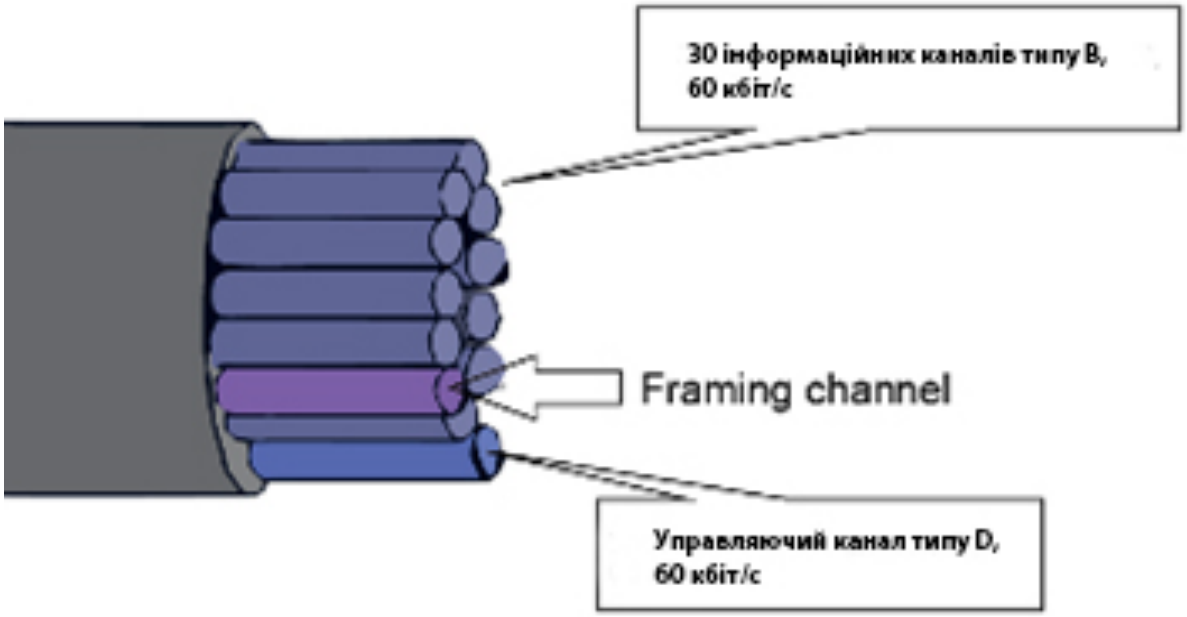



Рис. 3.10. Структура каналу E1

Канали комутуються в операторів зв'язку на постійній основі, використовуючи спеціальні комутатори потоків і мультиплексори, що поєднують канали малої пропускної спроможності більші (цифрова ієрархія). LAN сполучаються з WAN за допомогою пристроїв-шлюзів (Gateway), що є IP-маршрутизаторами, що мають на борту LAN і WAN-інтерфейси. Стек протоколів TCP/IP виступає уніфікованим інструментом передачі даних за допомогою різних базових технологій. Спосіб організації WAN на базі цифрових синхронних каналів, розроблених для передачі голосу з кінця в кінець, є дорогим та негнучким.

На початку 90-х років. почала активно впроваджуватися технологія Frame Relay. Технологія також передбачає використання каналів DS 0, T1/E1, T3/E3 між абонентським обладнанням (Data Terminal Equipment – DTE) та обладнанням оператора зв'язку (Data Communication Equipment – DCE). Дані канали не з'єднують абонентське обладнання безпосередньо, а лише транспортом для віртуальних каналів Frame Relay, які, у свою чергу, безпосередньо з'єднують між собою абонентське обладнання (маршрутизатори на майданчиках абонента) відповідно до логічної топології (рис. 3.11). Комутація відбувається на спеціальних Frame Relay-комутатори на стороні оператора зв'язку. Перевага даної технології полягає у можливості будувати гнучкі топології для об'єднання локальних мереж абонента поверх існуючих цифрових каналів без залучення додаткових виділених ліній point-to-point.

Крім того, єдина інфраструктура використовується для побудови мереж безлічі незалежних абонентів. Frame Relay дозволила драматично зменшити OpEx і CapEx для WAN-середовища, чим завоювала абсолютну популярність у операторів зв'язку. Протягом п'яти років навіть найбільш консервативні

клієнти, такі як банки, перейшли на використання Frame Relay. У 90-ті роки. також розвивалася досить складна технологія ATM, проте як WAN для корпоративних мереж вона майже не використовувалася.

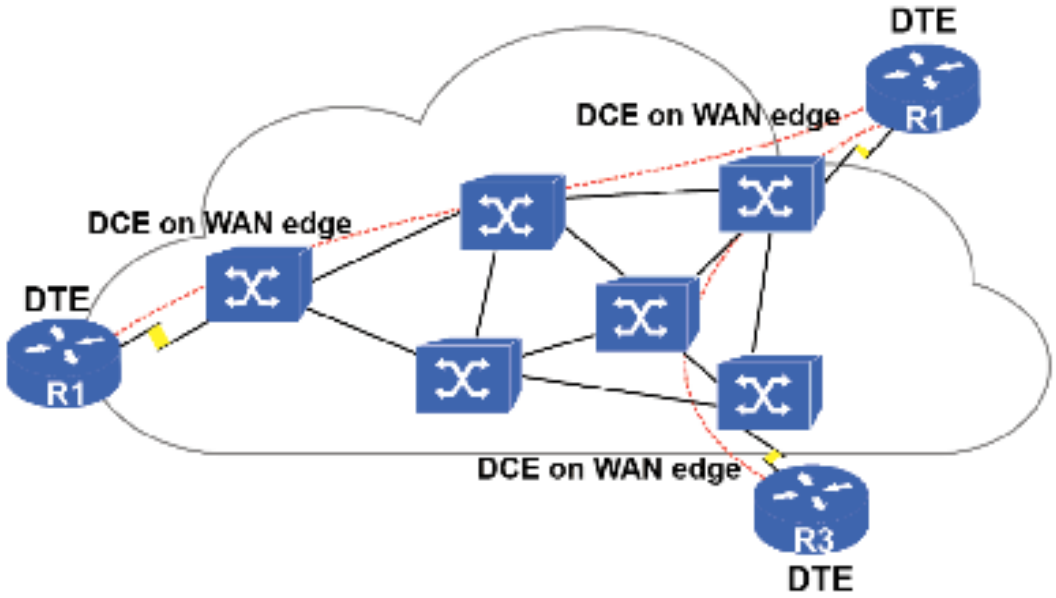



Рис. 3.11. Мережа Frame Relay

Повноправним наступником Frame Relay стала технологія Multi protocol Label Switching (MPLS). MPLS зазвичай реалізується у межах мережі оператора зв'язку (рис. 3.12).

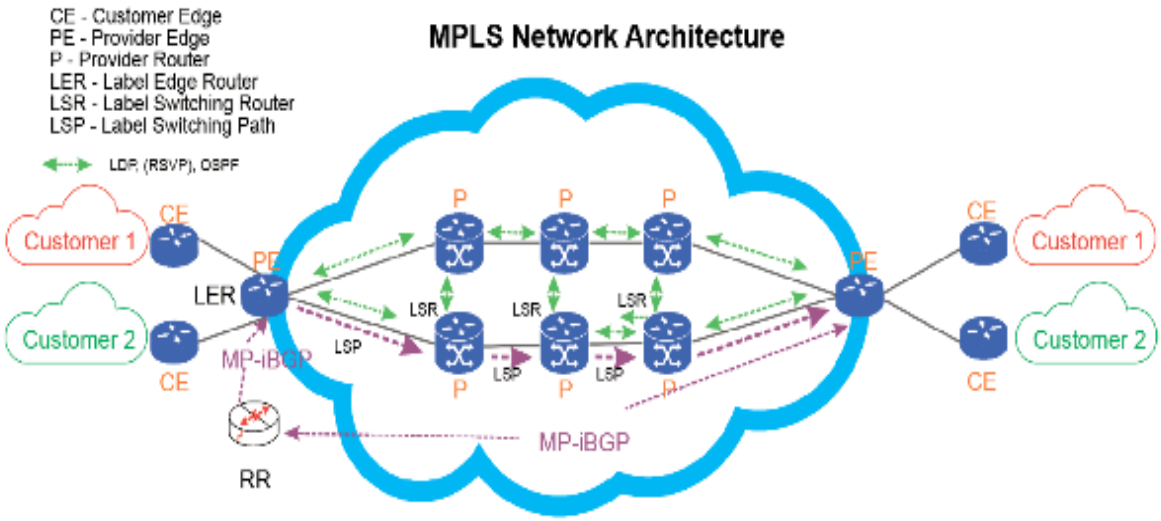



Рис. 3.12. Мережа MPLS

Технологія передбачає маршрутизацію IP-пакетів лише на межі мережі провайдера. Усередині мережі відбувається комутація за мітками. Приходячи ззовні на прикордонний маршрутизатор, пакет потрапляє у FIB (Forwarding

Information Base), де, згідно з адресою призначення, пакет інкапсулюється в спеціальний MPLS-фрейм, до одного із заголовків якого додається номер мітки – значення, взяте з FIB при маршрутизації пакета. Далі MPLS-frame інкапсулюється у кадр базового протоколу передачі. Наприклад, в Ethernet, де в заголовки кадру додаються MAC-адреси джерела та призначення.

Оскільки в рамках мережевої моделі OSI заголовки MPLS додаються між заголовками другого та третього рівнів, MPLS називають протоколом рівня «2.5». Заголовки MAC-призначення присвоюються відповідно до адреси шлюзу FIB і adjacency-таблицею. Далі шлях кадру MPLS всередині MPLS-хмари оператора зв'язку визначено відповідно до таблиць LFIB (Label Forwarding Information Base) проміжних маршрутизаторів, де кожному можливому значенню мітки кадру відповідає нове значення мітки, а також вихідний інтерфейс. Ланцюжок мінливих міток пакета на шляху з однієї крайньої точки мережі до іншої називається LSP (Label Switched Path).

Мітки можуть утворювати так званий стек – це означає, що MPLS-фрейми можуть вкладатися один в одного. На виході з MPLS-хмари IP-пакет декапсулюється з кадру MPLS і перенаправляється у вихідний інтерфейс згідно з LFIB. Інформація про IP-маршрути поширюється протоколами маршрутизації. Інформація про теги може поширюватися такими протоколами, як Label Distribution Protocol (LDP), Resource ReSerVation Protocol (RSVP), Border Gateway Protocol (BGP) або навіть OSPF . Зазвичай в MPLS-мережі використовуються одночасно два протоколи маршрутизації: IGP (зазвичай IS-IS або OSPF ) для обміну інфраструктурними маршрутами (зазвичай 32 адреси лупбеків маршрутизаторів) і MP-BGP на межі мережі для обміну клієнтськими IPv 4, 6 PE, VPNv 4, 6VPE маршрутами. Технологія спочатку створювалася як спосіб знизити навантаження на внутрішні маршрутизатори мережі оператора шляхом заміни маршрутизації IP-пакетів комутацією за мітками. Крім того, технологія MPLS на сьогодні пропонує можливість організації незалежних L2/L3 Virtual Private Network (VPN) поверх єдиної MPLS-мережі (MPLS-хмари). А протокол RSVP у поєднанні з одним з Link-State-протоколів, таких як OSPF або IS-IS, пропонує також можливість інжинірингу трафіку, що дозволяє вигідно навантажувати фізичні канали всередині операторської мережі. Таким чином, MPLS – високопродуктивна гнучка технологія зі зручними засобами віртуалізації, що дозволяє легко розгортати незалежні високошвидкісні WAN -мережі із заявленими Service Level Agreement (SLA) та QoS для багатьох клієнтів поверх провайдерської інфраструктури. Серйозним недоліком MPLS є її складність, обумовлена роботою тандему кількох протоколів сигналізації (control-plane ), таких як OSPF, LDP та/або RSVP, MP-BGP, необхідних для складних процедур побудови LSP та маршрутизації, що підвищує вимоги до кваліфікації обслуговуючих інженерів. До того ж, через розподіл control-plane складно привести мережу до єдиної точки управління. Хмара MPLS обмежується обладнанням оператора зв'язку. Як технології кінцевого доступу зазвичай виступають: Ethernet, GEPON, DSL, а також Wireless-

технології. Наразі MPLS є стандартом де-факто в операторських мережах, незважаючи на солідний вік. Однак як засіб надання WAN у корпоративних мережах дана технологія сьогодні здає позиції через свою дорожнечу, незахищеність та прив'язку WAN до одного (можливо – двох) оператора зв'язку.

Поряд із WAN-технологіями, що спираються на інфраструктуру оператора зв'язку, ближче до кінця 90-х стали набирати популярності оверлейні VPN, що дозволяють пов'язувати ділянки корпоративної мережі безпосередньо через Internet. Основною ідеєю цього класу технологій є різного виду тунелювання, що передбачає інкапсуляцію IP-пакетів або L2-фреймів корпоративного трафіку в тіло IP-пакетів (або дейтаграм транспортного рівня) Internet-трафіку. При цьому можливе використання спеціальних протоколів, що тунелюють, що несуть додаткові проміжні заголовки і, можливо, здатних шифрувати тунельований трафік. Найбільш поширеною VPN-технологією стала технологія IPSec, що підтримує тунелювання трафіку, його шифрування, перевірку збереження незмінності трафіку в дорозі, а також взаємну автентифікацію сторін, що встановлюють шифроване з'єднання (рис.3.13).

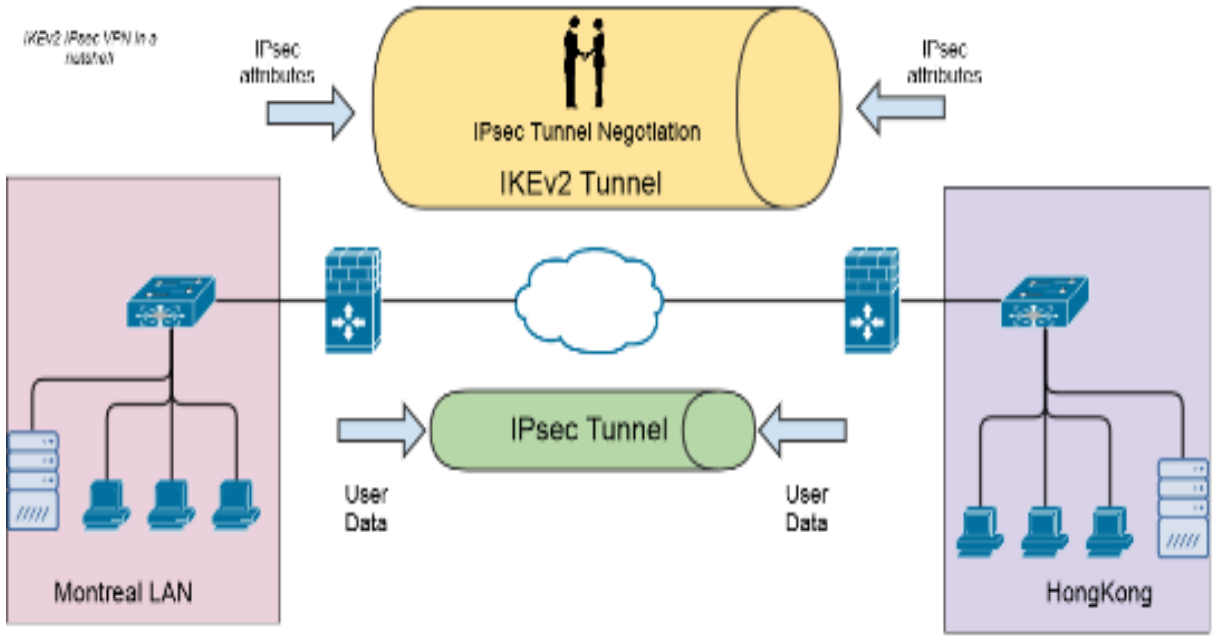



Рис. 3.13. Технологія IPSec

Основою IPSec є протоколи інкапсуляції ESP і AH, а також ISAKMP, протокол управління контекстами безпеки (Security Assotiation) та ключами. Для збільшення гнучкості шифрованих тунелів, спільно з IPSec, часто використовується розроблений свого часу компанією Cisco Systems протокол GRE (Generic Routing Encapsulation), як проміжний шар між інкапсульованим корисним трафіком та IPSec. Оверлейні VPN дозволяють безпосередньо через Internet пов'язувати тунелями прикордонні маршрутизатори локальних мереж компанії, не витрачаючись на додаткові послуги Інтернет-провайдера.

Ще однією визначальною перевагою оверлейних VPN (та IPSec зокрема) є вбудовані функції безпеки. Проте простота реалізації породжує істотний недолік як неможливості встановити SLA для тунелю у зв'язку з недостатнім рівнем надійності Internet як транспортного середовища. Другою перешкодою для організації IPSec-тунелів, на відміну від MPLS VPN можуть послужити накладні витрати на шифрування на тлі низької швидкості доступу в Internet .

Коли оверлейні VPN стали використовуватися досить широко, а пропускна спроможність зовнішніх каналів досягла прийнятних значень, дешеві VPN-канали в деяких випадках стали розглядатися поряд з WAN і врешті-решт зайняли цю роль. Класичний IPSec VPN, тим не менш, не володів необхідним функціоналом, щоб по праву зайняти нішу WAN, і розробники мережевих технологій почали створювати нове, що базується на IPSec, WAN-рішення з відповідним набором функцій. Зокрема, компанія Cisco створила рішення, що має назву iWAN (Cisco Intelligent WAN). Рішення iWAN пропонує чотири основні переваги на тлі класичних WAN-рішень:

- інваріантність по відношенню до транспорту;
- інтелектуальний контроль трафіку;
- оптимізація додатків;
- безпека з'єднань.

Незалежність від фізичного транспорту виходить з принципі оверлейной мережі. Як оверлейна технологія використовується DMVPN, що представляє собою протокол mGRE, що працює поверх IPSec. DMVPN надає досить гнучкі можливості у побудові оверлейних топологій з огляду на резервування зовнішніх фізичних каналів (рис. 3.14).

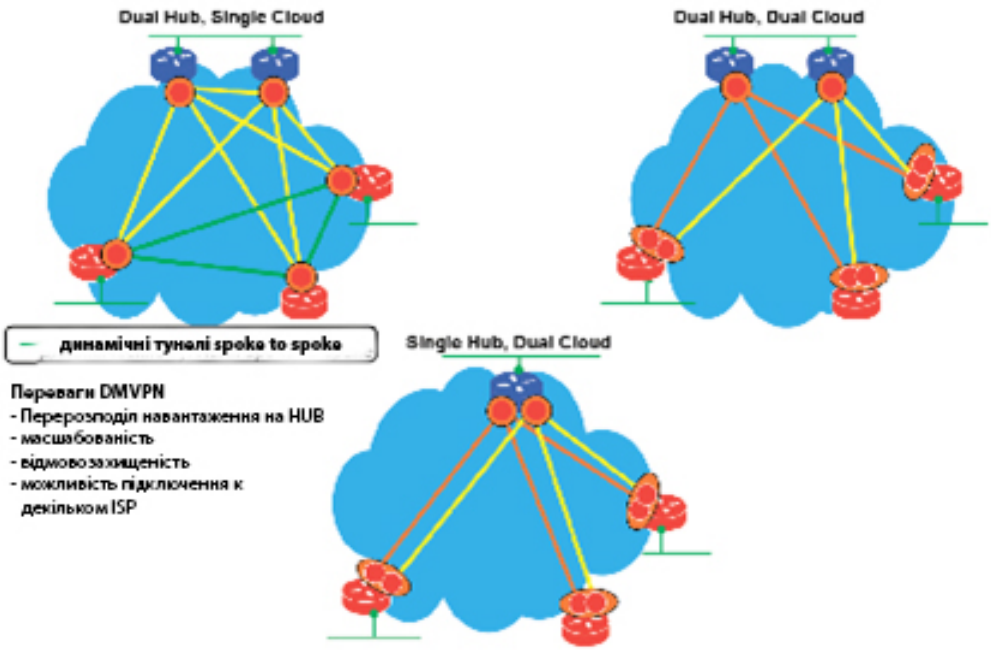



Рис. 3.14. Використані топології DMVPN

Протокол DMVPN створює оверлейну NBMA (None-Broadcast Multiple Access) середовище (hub-and-spoke або full-mesh, добудоване автоматично поверх hub-and-spoke), в якому адресами хостів служать IP-адреси тунельних інтерфейсів маршрутизаторів, а адресами канального рівня – IP-адреси зовнішніх інтерфейсів маршрутизаторів, до яких прив'язані відповідні тунельні інтерфейси (NBMA-адреси). Для дозволу тунельних адрес NBMA-адреси служить протокол NHRP, що функціонує за допомогою NHRP-сервера, що є одночасно хабом в топології DMVPN.

Інтелектуальний контроль трафіку передбачає додаткові критерії вибору маршруту, необхідних ефективної доставки додатків, балансування навантаження, збільшення доступності. Серед таких додаткових критеріїв використовуються: bandwidth, delay, jitter, loss і т.д. У складі iWAN інтелектуальний контроль трафіку базується на технології PfR (Performance Routing), яка передбачає попередній активний чи пасивний вимір параметрів продуктивності, перевірка доступності каналів поруч із класифікацією трафіку і наступним застосуванням політик маршрутизації.

Протокол PfRv 3 передбачає централізоване керування трафіком. На кожному сайті встановлено Border Controller (Hub-BR, Branch-BR), в область відповідальності яких входить локальне управління трафіком в межах сайту. У його ролі виступає один із прикордонних маршрутизаторів. MC (Master Controller) розташовується на HUB-сайті і задає політики управління трафіком для всієї мережі, взаємодіючи з Border Controllers кожного сайту. Варто зазначити, що PfRv 3 не може функціонувати самостійно і завжди працює спільно з протоколом маршрутизації, таким як, наприклад, EIGRP або BGP. Дані протоколи Cisco рекомендує як варіанти використання в мережах, що добре масштабуються, на базі і WAN (рис. 3.15).

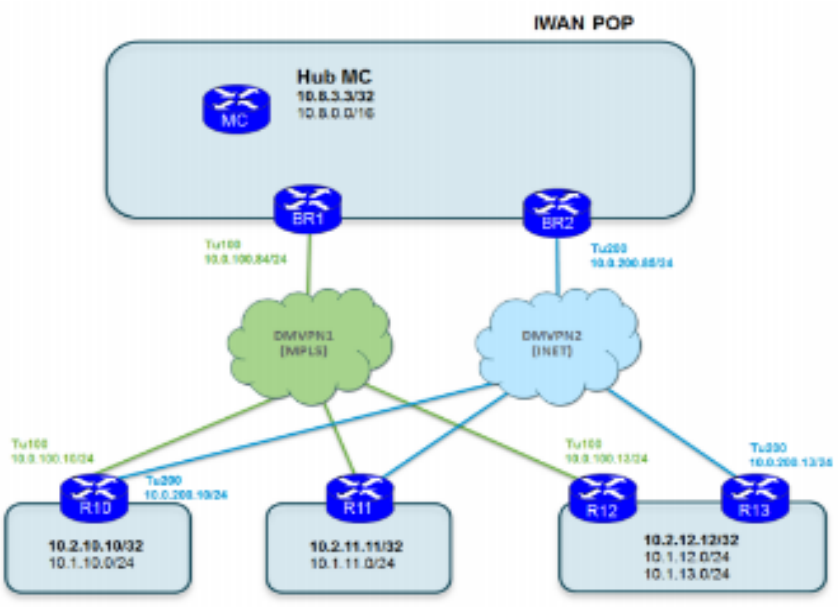



Рис. 3.15. Типова топологія та WAN

Оптимізація додатків включає оптимізацію TCP-з'єднань (Transmission Control Protocol – TCP), оптимізацію даних (кешування), компресію, оптимізацію прикладних протоколів.

### 3.1.5. Мережа Internet

Вперше ідею обміну цифровими даними між двома комп'ютерами було реалізовано дослідником лабораторії Массачусетського технологічного інституту Ларі Робертсом (рис. 3.16). Згодом ідея розвинулася в проект, в рамках якого Агенством Міністерства оборони США з перспективних досліджень у 1969 р. було побудовано мережу передачі даних ARPANet (Advanced Research Projects Agency Network), яка стала основою для розвитку досконалішої мережі NSFNet (National Science Foundation Network), а потім – і глобальної мережі Internet. Спочатку в рамках цієї мережі були з'єднані дослідницькі центри, зайняті у розробці ARPANet. Мережа розвивалася, стаючи все більш розгалуженою. Динаміка розвитку ARPANet наочно представлена на рис. 3.17–3.20. У січні 1983 р. відбулася справді знакова подія – мережа ARPANet перейшла використання стека протоколів TCP/IP замість попереднього йому NCP .

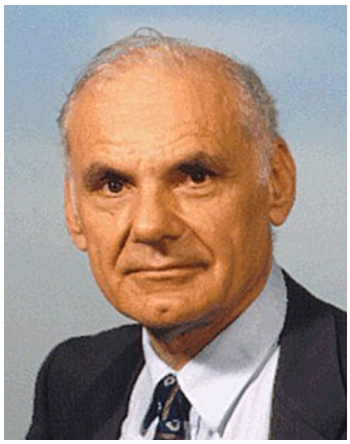


Рис. 3.16. Лари Робертс


Рис. 3.17. Схема мережі ARPANet за станом 1969 р.

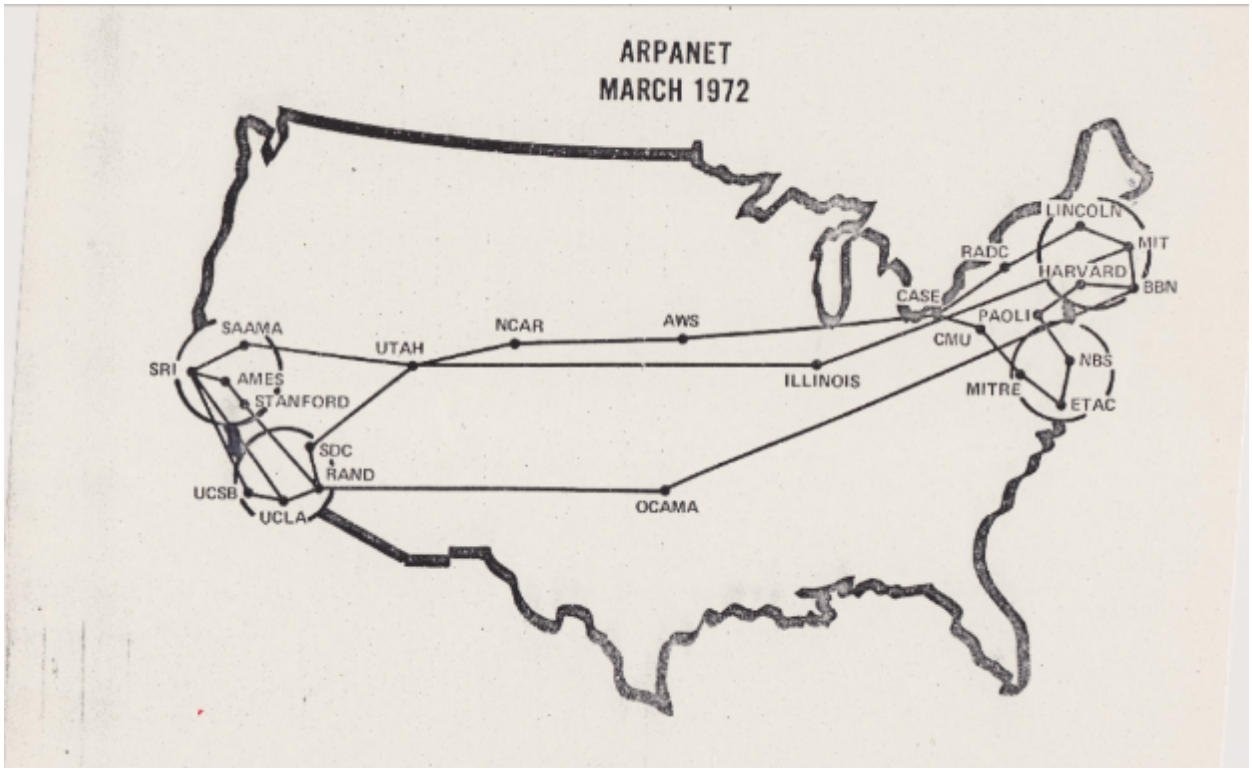



Рис. 3.18. Схема мережі ARPANet за станом 1972 р.

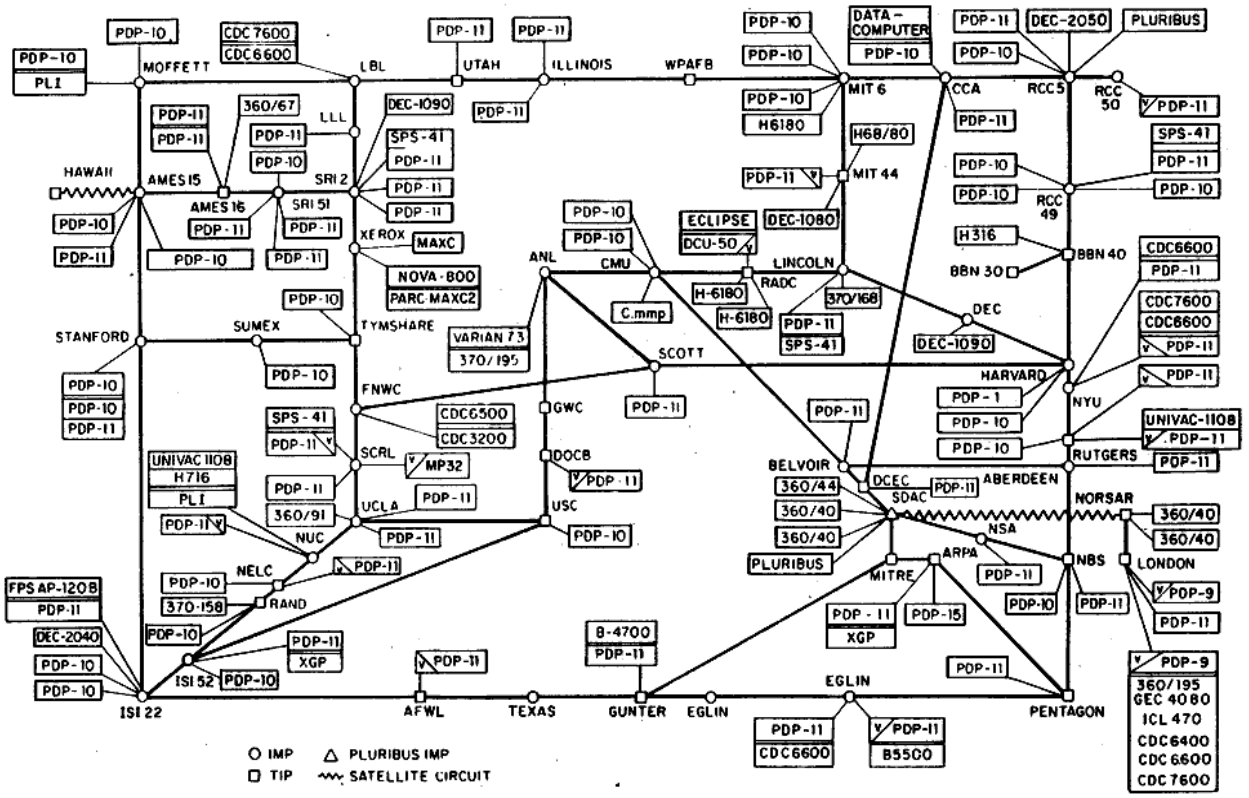



Рис. 3.19. Схема мережі ARPANet станом на 1977р.

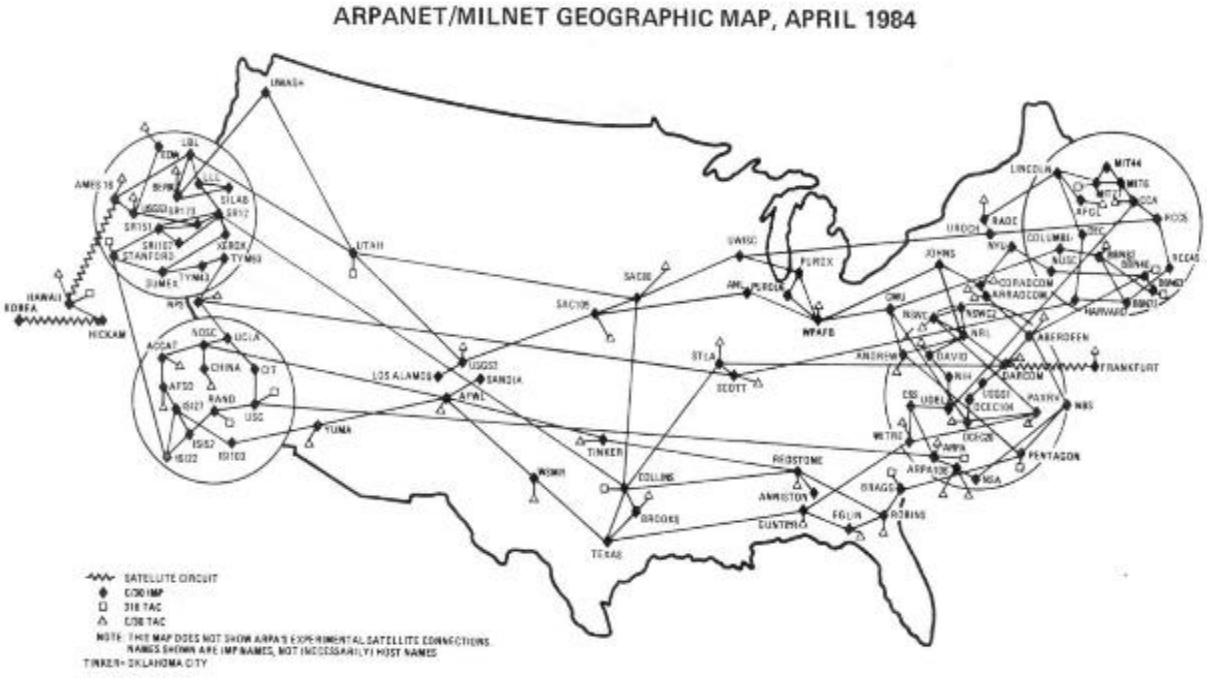



Рис. 3.20. Схема мережі ARPANet за станом 1984 р.

У 1985 р. Національним Науковим Фондом США (NSF) була створена нова мережа NSFNet (рис. 3.21), яка також використовувала TCP/IP, призначена для обміну науковими даними, яка пізніше почала використовуватися також і комерційними структурами, отримуючи краще фінансування.

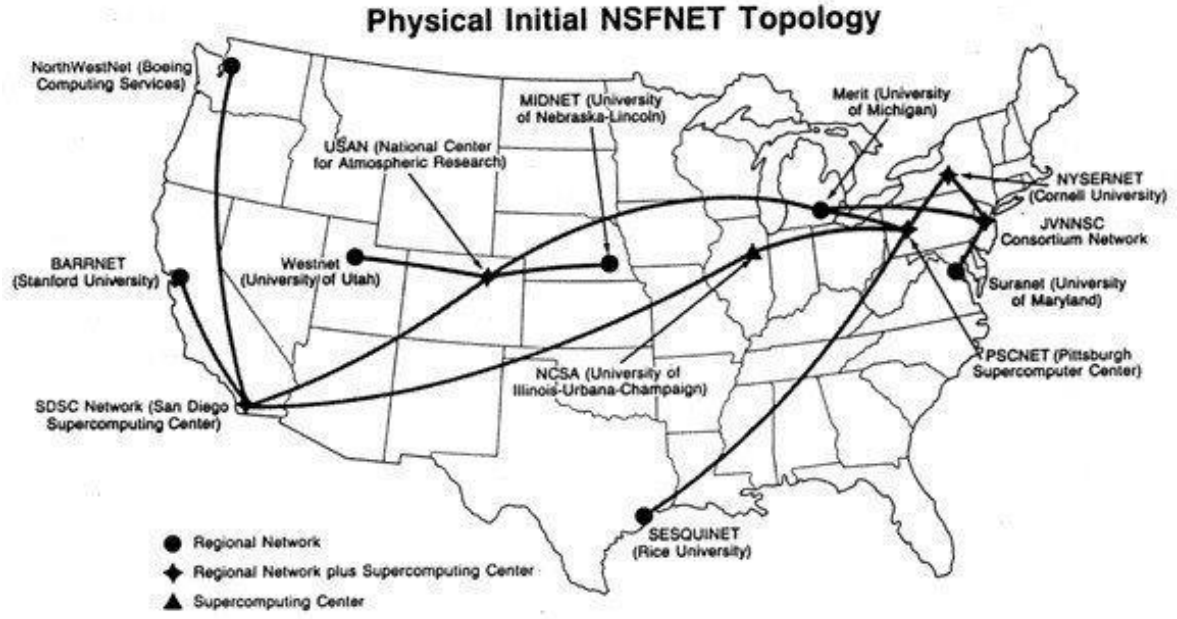



Рис. 3.21. Схема мережі NSFNet

У результаті ARPANet і NSFNet почали швидку трансформацію в сучасний Internet.

### 3.1.6. DWDM-технологія передачі та ущільнення оптичних каналів

Стрімкий розвиток телекомунікаційної галузі, починаючи з середини 2000-х рр., став можливим у тому числі завдяки появі нової волоконно-оптичної техніки. Оператори зв'язку та телекомунікаційні провайдери в процесі свого розвитку вирішують завдання збільшення територіального покриття, швидкості передачі трафіку та покращення його якості, побудували досить велику кількість оптичних магістральних транспортних мереж. Але з урахуванням динамічного збільшення абонентської бази, тривалості розмов, надання нових голосових послуг вони зіткнулися з проблемою необхідності ущільнення трафіку. Найбільш ефективним засобом для її вирішення стало впровадження технології DWDM (Dense Wave Division Multiplexing), що дозволяє багаторазово збільшити пропускну спроможність оптичної кабельної інфраструктури. DWDM є сучасною технологією передачі та ущільнення в одному оптоволокні декількох оптичних сигналів з різними довжинами хвиль. Устаткування DWDM дозволяє передавати по одному оптичному волокну до 160 незалежних інформаційних каналів на різних оптичних несучих (довжинах хвиль) трафік різних протоколів (IP, ATM, SONET, Synchronous Digital Hierarchy (SDH), Ethernet) з різними швидкостями (від 100 Мбіт/с до 2,5 Гбіт/с). І саме ця технологія – спектрального ущільнення оптичних каналів лежить сьогодні в основі більшості магістральних мереж операторів зв'язку та телекомунікаційних провайдерів.

Ця технологія використовує волокно-оптичне середовище передачі даних. Але на відміну від класичних оптичних технологій, які залучають одну пару волокон для передачі даних одного каналу, DWDM-системи дозволяють по одній парі волокон передавати n кількість каналів. Досягти цього вдається з допомогою передачі кожного потоку даних суміжних несучих частотах. Діапазон робочих частот визначений стандартом ITU-T G.694.1, і технології DWDM їх прийнято називати хвилями. Відповідно до рекомендацій ITU-T в DWDM-системах використовуються «C» (1525…1565 нм) та «L» (1570…1610 нм) вікна прозорості. Кожен діапазон потрапляють по 80 каналів з кроком 0.8нм (100 ГГц). Зазвичай використовується тільки C-діапазон, оскільки кількість каналів, які можна організувати в цьому діапазоні, і так вистачає з надлишком, до того ж згасання в волокні стандарту G.652 C-діапазоні трохи нижче, ніж L-діапазоні.

У відкритих DWDM-системах сигнал кожної хвилі формується окремим приймально-передавальним елементом – транспондером, який перетворює сигнал від клієнтського обладнання на ITU-T сумісний. У закритих системах приймання і передачі сигналу на DWDM-хвилі здійснює кінцеве обладнання, але такі системи зустрічаються набагато рідше. Перед введенням оптичну магістраль хвилі об'єднуються в композитний сигнал мультиплексором (mux), але в приймаючій стороні композитний сигнал поділяється окремі

канали демультиплексором (demux). У зв'язку з тим, що оптичний сигнал має властивість загасати у міру проходження відстані, для відновлення його рівня вздовж оптичної магістралі встановлюються спеціальні вузли-підсилювачі, або Amplifier. Якщо один або кілька каналів потрібно термінувати на шляху проходження магістралі, то у таких випадках використовується інший тип вузлів – мультиплексори, або Add/Drop-вузли (рис. 3.22). Їх основною властивістю є вміння «розібрати» і «зібрати» композитний сигнал виділення окремої хвилі чи набору хвиль, інші ж передати без змін далі магістралі. Це стало можливим завдяки появі нової лінійки спеціальних пристроїв оптичних мультиплексорів [42].

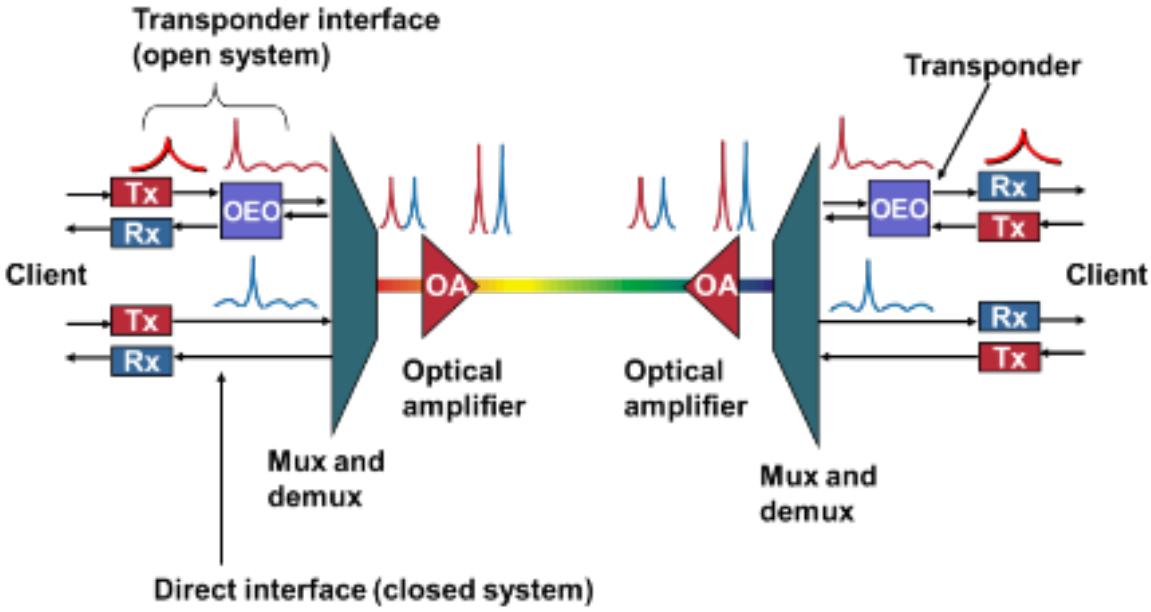



Рис.3.22. Компоненти DWDM-системи

*Fixed-OADM (FOADM)*. На початковому етапі розвитку DWDM-технології Add/Drop вузли архітектурно не сильно відрізнялися від своїх попередників, що термінують TDM-потоки в SDH-мережах, які повинні були замінити DWDM-мережі. Вони підтримували лінійні та кільцеві топології. Для «виділення» каналу на OADM-вузлі композитний канал має бути попередньо «розібраний» по діапазонах, діапазони – по окремих хвилях, і тільки тоді хвиля може бути прийнята на елементі, що перетворює її на сумісний з клієнтським обладнанням сигнал. Зворотний процес проводився при додаванні каналу на OADM-вузлі (рис. 3.23). Процес створення нового сервісу при цьому, крім виконання підключення клієнтського обладнання в точках його термінації, вимагав виконати фізичну комутацію відповідної хвилі або діапазону хвиль на всіх транзитних вузлах. Отже, комутація сервісу у разі займала кілька днів.

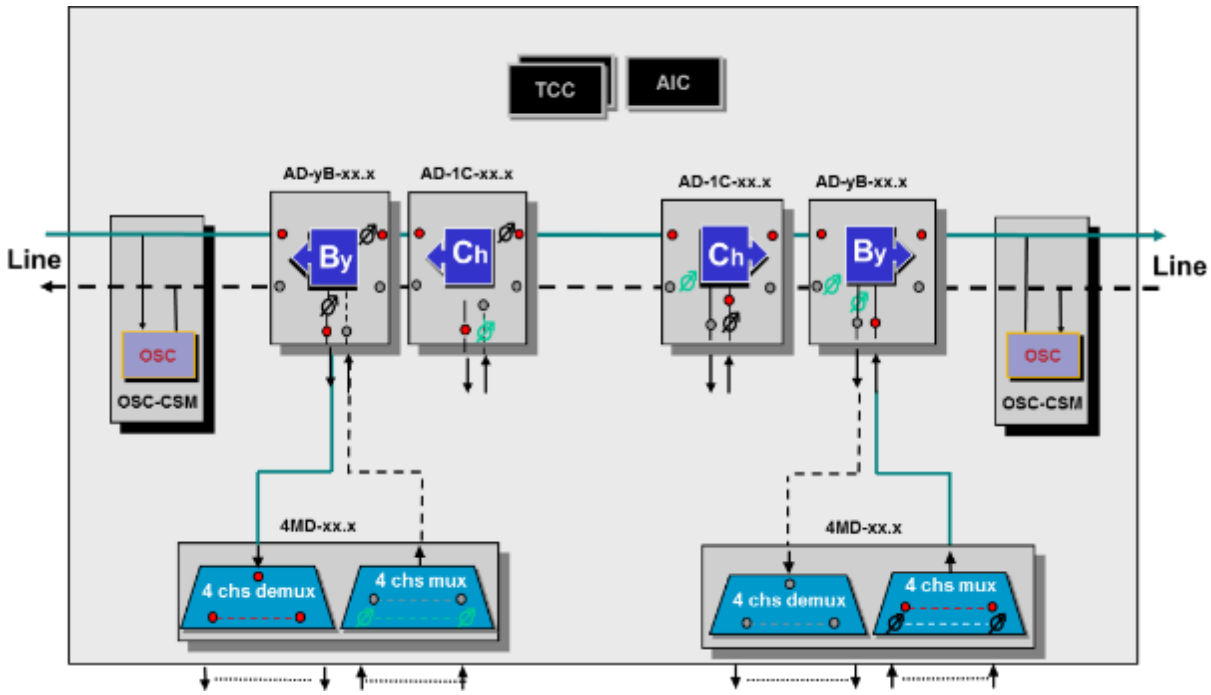



Рис. 3.23. Блок-схема типового OADM-вузла

*Reconfigurable-OADM (ROADM)*. Наступним етапом розвитку архітектури вузлів-мультиплексорів стали вузли з можливістю програмно настроюваного режиму роботи кожної окремої хвилі: «додавання/термінація» (add/drop ) або «транзит» (pass-through) (рис. 3.24).

Досягти такого результату вдалося за рахунок додавання до системи вузла двох елементів: оптичного розподільника та оптичного комутатора (2x1).

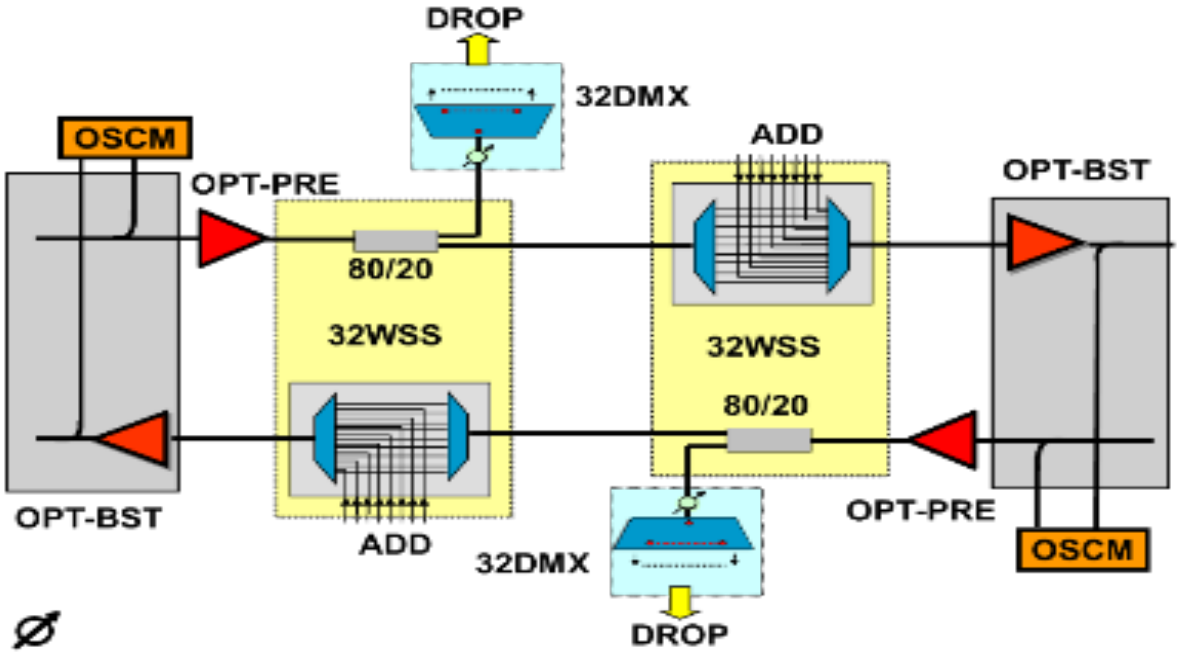



Рис. 3.24. Блок-схема типового ROADM-вузла

Завдання першого – розділити оптичну потужність вхідного композитного сигналу на дві частини: перша (слабша) передається на елемент демультиплексування того ж напрямку вузла, друга (більш потужна) – на другий бік вузла, де композитний сигнал демультиплексується і кожна окрема хвиля потрапляє на перший вхід оптичного комутатора. На другий вхід приходить локально доданий сигнал тієї ж довжини хвилі і, залежно від конфігурації комутатора, вибирається один із двох вхідних сигналів передачі. Після чого відфільтровані хвилі мультиплексуються знову композитний сигнал і передаються далі в магістраль, де процес повторюється на кожному ROADM-вузлі.

Таким чином, поява ROADM-вузлів значно зменшила кількість часу, що витрачалося на створення нових сервісів, за рахунок можливості програмно задавати режим передачі каналу на певній хвилі та виключило необхідність робити фізичну комутацію на кожному проміжному вузлі. Даний тип вузлів, як і попередній, підтримує лінійні та кільцеві топології.

*Multi-Degree ROADM*. Класичні ROADM-вузли мають одне суттєве обмеження – у них тільки два напрямки, що дозволяє приймати не більше двох магістральних ліній. Для транзитних вузлів, що стоять уздовж оптичних трас, цього цілком достатньо, але в місцях концентрації магістралей, наприклад, великих містах, для прийому всіх ліній потрібно будувати кілька ROADM-вузлів або терміналів (ROADM-вузли з одним напрямком). У разі виникають труднощі з організацією клієнтського каналу, що має йти транзитом через ці вузли. Потрібно розбивати його на два окремі DWDM-канали, а клієнтські порти транспондерів на майданчику підключати між собою для регенерації сигналу. Організація таких каналів вимагає використання додаткових транспондерів на кожній подібній ділянці, що збільшує його вартість та ускладнює обслуговування. Обійти це обмеження дозволяє побудова багатоспрямованих вузлів – Multi-Degree ROADM (рис. 3.25).

Додавання додаткової сторони до класичного ROADM-вузла стало можливим за рахунок архітектурної зміни у компонуванні сторони вузла. Між сторонами додано додатковий оптичний елемент 1xN, дзеркальний композитний сигнал від кожної сторони на інші, де для кожної хвилі оптичний комутатор Nx1 передає на лінію локально додану хвилю, або хвилю, що приходить з певного напрямку (рис. 3.26).

Багатоспрямовані вузли дозволили будувати DWDM-мережі повнозв'язкової топології, забезпечивши у своїй побудова сервісів точка-точка без необхідності розбивки сервісу частини на подібних вузлах.

*Colorless & Omnidirectional ROADM (C&O ROADM)*. Всі попередні архітектурні моделі вузлів-мультиплексорів мають один істотний недолік: забезпечення резервування сервісу на рівні транспортної мережі може здійснюватися тільки за рахунок попередньо зарезервованої хвилі через інший напрямок. Резервний шлях у разі «простоює» під час штатної роботи

мережі, і навіть блокує можливість використання тієї ж хвилі по всьому ділянці.

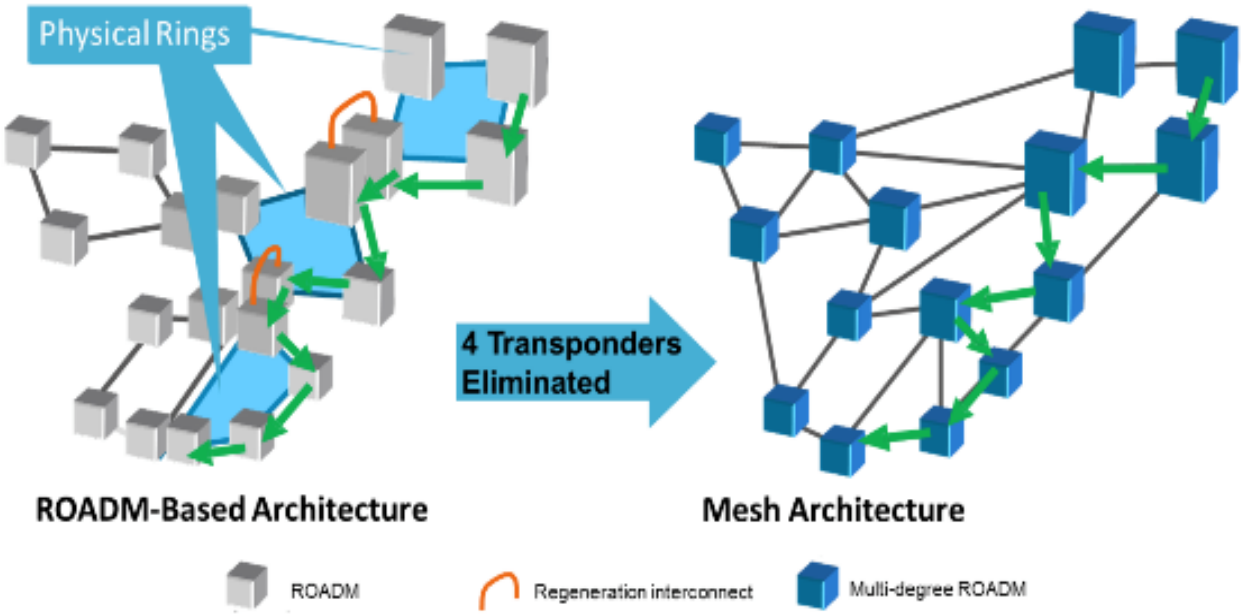



Рис. 3.25. Порівняння ROADM-based та Mesh-архітектур

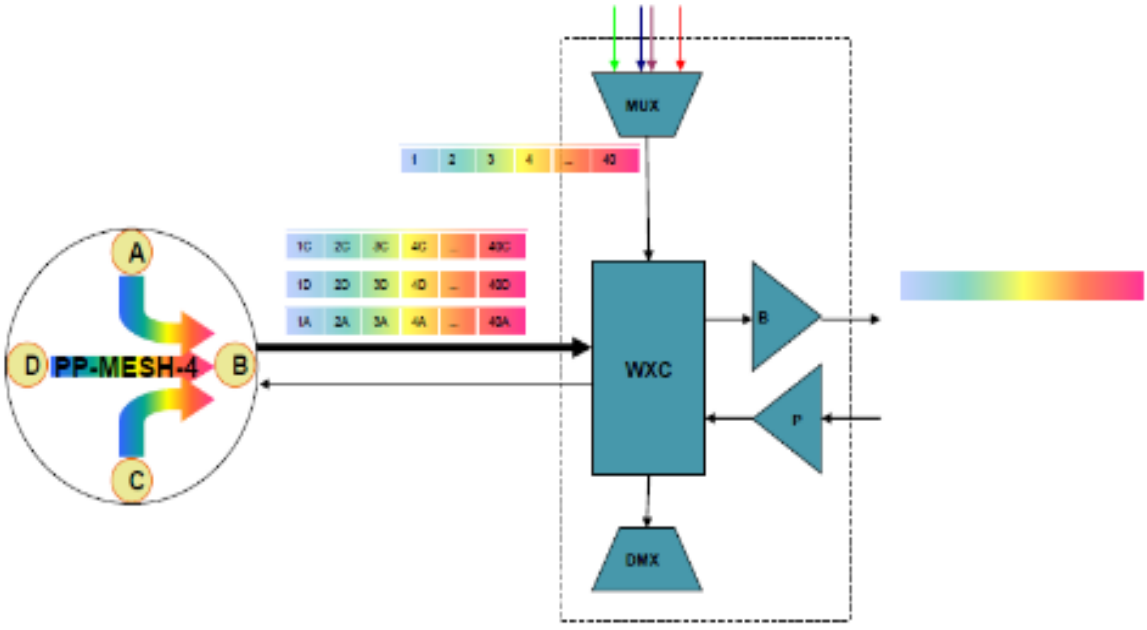



Рис. 3.26. Блок-схема одного напрямку Multi-Degree ROADM-вузла

Таким чином, резервування сервісів на рівні DWDM-мережі є досить неефективним, оскільки призводить до неоптимального використання її ресурсів. Альтернативний варіант – це перемикання сервісу в ручному

режимі на інший напрямок, у разі обриву на основному, який потребує фізичної перекомутації патчкордів на обох кінцях сервісу.

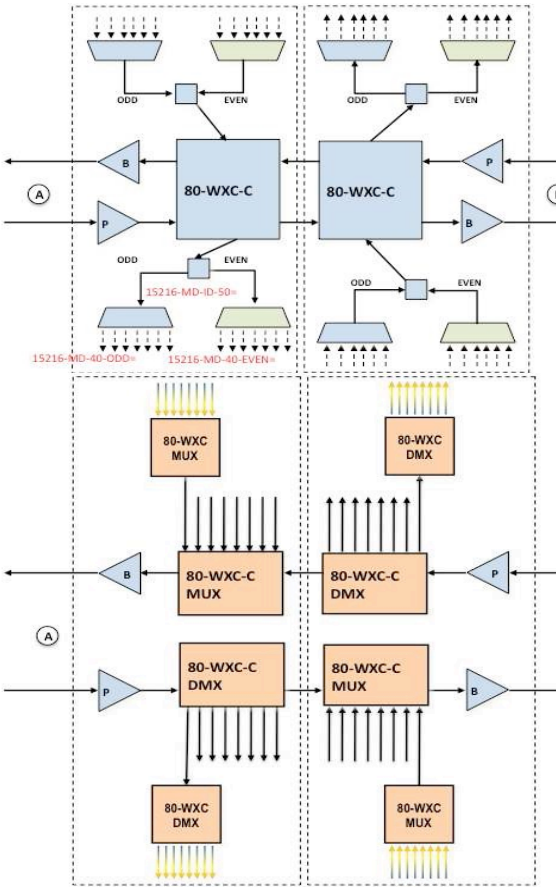



Рис. 3.27. Блок-схема 80-канального двунаправленного «цветного» и «бесцветного» ROADM-узла

Концепція «безбарвного» та «всеспрямованого» ROADM-вузла дозволяє вирішити обидві вищезгадані проблеми, тому що не вимагає постійно зарезервованої хвилі, а у разі обриву дозволяє автоматично перемаршрутизувати потрібні сервіси через вільні хвилі на іншому напрямку. У технології DWDM «кольоровими» називають оптичні інтерфейси, які випромінюють і приймають оптичний сигнал на хвилі, визначеної стандартами ITU-T. Якщо раніше виробники випускали оптичні трансівери з фіксованою довжиною хвилі, або які працювали на кількох суміжних хвилях, то в даний час акцент робиться на модулі, що підтримують цілі діапазони хвиль. В даному випадку під визначенням «безбарвний» слід розуміти можливість апаратних компонентів працювати з оптичним сигналом, сформованим на будь-якій хвилі діапазону (рис. 3.27). До появи поняття «безбарвні» транспондери підключалися до мультиплексорної частини вузла через порти з визначеним фіксованим значенням хвилі. Тобто для зміни хвилі для певного сервісу потрібно було як її зміна на оптичному модулі, а й фізичне перемикання в порт мультиплексора, відповідного нової хвилі. Концепція «безбарвності» передбачає підключення транспондера до портів, які можуть обробляти повний діапазон DWDM-хвиль, не вимагаючи фізичної перекомутації у разі зміни довжини хвилі на порту транспондера.

*Omnidirectional ROADM.* В архітектурі класичних ROADM-вузлів транспондери підключаються до портів із фіксованою довжиною хвилі, а кожна пара мультиплексор/демультиплексор, до портів якої підключаються транспондери, прив'язана до певного напрямку (рис.3.28). Для зміни напрямку для окремого сервісу, навіть при використанні тієї ж хвилі, необхідно перемикати відповідний транспондер в порти Mux/Demux потрібного напрямку.

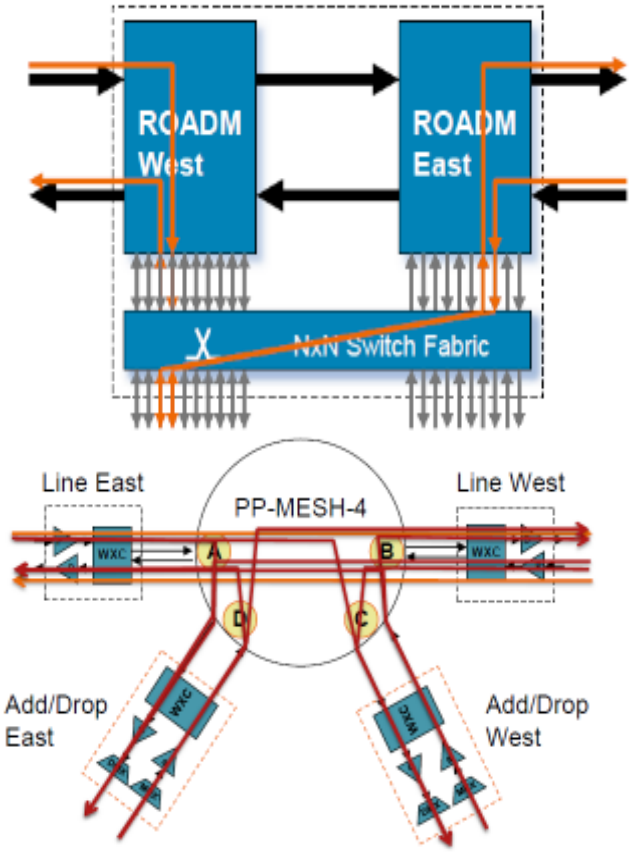



Рис. 3.28. Блок-схема «всеспрямованого» ROADM-вузла з усіма можливими маршрутами каналу

Архітектура «всеспрямованого» ROADM-вузла передбачає поділ мультиплексорної та лінійної частини таким чином, щоб перша була не залежною від другої. Для досягнення такого результату кожна пара Mux/Demux пристроїв підключається до оптичного комутатора 1xN, який дзеркає композитний сигнал на всі сторони вузла, де лінійний оптичний комутатор Nx1, виходячи з конфігурації, для кожної пари Mux/Demux пристроїв вибирає набір хвиль, який необхідно передати в лінію.

Таким чином, незалежно від того, до якої пари Mux/Demux підключено транспондер, сервіс, який він термінує, може бути направлений у будь-який напрямок. Крім того, на вузлі може бути тільки одна мультиплексорна частина хвилі якої можуть бути розподілені між напрямками.

Для більшості архітектурних рішень, що використовуються в даний час, DWDM вважається технологією організації статичних транспортних з'єднань типу точка-точка. Еволюція ROADM вузлів до «всеспрямованих» та «безбарвних» відкриває можливість будувати динамічну та гнучку повнозв'язну транспортну мережу з великою кількістю оптичних шляхів, яка дасть можливість оптимально використовувати наявні ресурси, а також зменшити втрати клієнтського трафіку під час урвищ на магістральних лініях, або під час запланованого «вікна» обслуговування.

«Всінаправлені» і «безбарвні» ROADM-вузли можуть бути інтегровані в мережі, побудовані на класичних ROADM/Multi-Degree вузлах, а існуючі

вузли можуть бути модернізовані відповідно до такої ж архітектури, забезпечуючи безшовний перехід на неї (рис.3.29).

Концепції «всеспрямованого» та «безбарвного» DWDM, разом із технологією Flex Spectrum та динамічною площиною управління WSON є ключовими елементами інноваційного рішення для транспортних мереж Cisco nLight. Прикладом реалізації проекту на основі технології Cisco nLight є побудова магістральної мережі польського кабельного оператора Vectra у 2014 р. У результаті впровадження цієї технології вдалося суттєво підвищити ефективність та ємність мережі та значно скоротити витрати на її експлуатацію. Крім того, вдалося зменшити час запуску нових сервісів з трьох місяців до одного, а також із двох годин на місяць до нуля скоротився час простою ядра мережі. Інші великі виробники DWDM-обладнання також використовують концепцію C&O DWDM, і в їхній лінійці представлено обладнання, що підтримує Multi-Degree C&O ROADM-вузли.

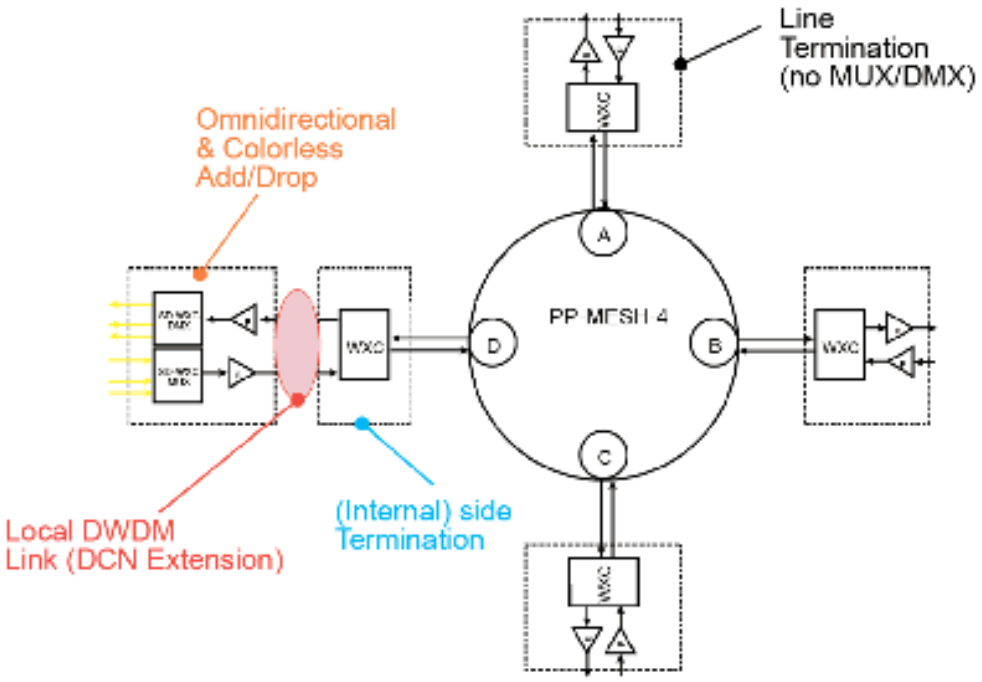



Рис. 3.29. Блок-схема «всеспрямованого» та «безбарвного» Multi-Degree ROADM-вузла

Таким чином, DWDM-технологія для спектрального ущільнення оптичних каналів є значущою, так як її використання дозволяє багаторазово збільшити пропускну здатність оптичної кабельної інфраструктури за рахунок можливості передачі по одному оптичному волокну до 160 незалежних інформаційних каналів на різних довжинах хвиль трафіку різних протоколів з різними. DWDM-технологія з використанням ROADM-вузлів, як правило, застосовується для модернізації та розширення існуючих волоконно-оптичних транспортних мереж з метою підвищення рівня їхньої пропускної спроможності та доступності.

## 3.2. Бездротові мережі передачі даних

### 3.2.1. Технології бездротового широкосмугового доступу

На сьогоднішній день бездротові технології міцно посіли своє місце серед засобів організації каналів зв'язку. Незважаючи на те, що їх поєднує використання радіоефіру для передачі інформації, кожна з бездротових технологій дуже істотно відрізняється як параметрами користувача, так і технічними характеристиками. Таким чином, після прийняття рішення про використання бездротового доступу необхідно вирішити досить складне завдання вибору технології організації каналів зв'язку [43].

Тому завдання аналізу існуючих технологій широкосмугового бездротового доступу (ШБД) та вибору найефективніших з них для організації сучасних каналів зв'язку є актуальним [44].

З погляду топології, бездротові канали зв'язку, як і дротяні, можна умовно розділити на «крапка-крапка» і «крапка- многоточка». Вибір рішень для каналів «точка-точка» обмежений переважно радіорелейними станціями та мостами, побудованими на базі широкосмугових ліній зв'язку в діапазонах частот «до 6 ГГц», при цьому мости зазвичай використовувалися на ділянці останньої милі, а радіорелейні канали – як на магістральних ділянках, так і на ділянках останньої милі. Для топології «точка-многоточка» складність вибору пов'язана з тим, що використовуються різні радіотехнології, методи реалізації якості сервісу (QoS), доступу абонентських пристроїв до базової станції (БС) і т. д. Розглянемо критерії порівняння та аналізу.

1. Радіотехнологія, закладена основою радіоінтерфейсу, – найважливіший компонент аналізу, оскільки саме тут закладено основні параметри системи зв'язку. На даний момент найбільш ефективними рішеннями є: використання широкосмугових сигналів Orthogonal Frequency-Division Multiplexing (OFDM); спосіб розподілу ресурсу БС між абонентами не тільки за часом, а й за частотою (режим Orthogonal Frequency-Division Multiple Access (OFDMA)); велика кількість компонентів широкосмугового сигналу (що більше кількість компонентів, тим вища перешкодостійкість і краще робота системи в умовах непрямої видимості); використання технології множинного приймання-передачі (Multiple Input Multiple Output (MIMO)) збільшення дальності обслуговування клієнтських пристроїв (КУ); використання технології «розумних» антен Beam Forming [45,46].

2. Підтримка якості обслуговування (QoS) для побудови мультисервісних корпоративних мереж або конвергентних послуг абонентам оператора.

3. Спосіб доступу КУ до середовища (ресурсу БС) визначає можливість надавати абоненту трафік відповідно до SLA.

Проведемо ретроспективний аналіз технологій широкосмугового доступу з використанням наведених вище критеріїв. Ще 10 років тому в Україні був відносно загальнодоступний лише діапазон 2,4 ГГц, було кілька рішень широкосмугового доступу з реальною пропускною здатністю від 2 до 14 Мб/с, включаючи Wi-Fi-IEEE 802.11 та IEEE 802.11b. Потім ситуація

кардинально змінилася: з'явилася можливість використовувати діапазон 5 ГГц, стали доступні нові рішення та технології, аналіз яких наведено у хронологічному порядку виходу на ринок.

*Wi-Fi* – найперевіреніша часом технологія, що базується на сімействі стандартів IEEE 802.11. Розроблялася та була призначена для побудови внутрішньоофісних локальних мереж. Однією з небагатьох її переваг є стандартизованість (як результат – низька вартість та масовість). Другою перевагою є висока пропускна здатність (швидкість передачі від десятків до сотень Мб/с). Незважаючи на ці переваги, використання Wi-Fi технології для побудови систем широкосмугового доступу неефективне через її орієнтацію на внутрішньоофісне використання.

*Pre-WiMAX* – сукупна назва набору рішень, яка не стандартизована (це вже не Wi-Fi, але ще не Worldwide Interoperability for Microwave Access (WiMAX)). В основному, рішення побудовані на базі радіоінтерфейсу IEEE 802.11a або IEEE 802.11g. Зазвичай такі рішення характеризуються дещо вищою стабільністю трафіку, можуть забезпечувати дуже якісну підтримку QoS, але при цьому мають низьку спектральну ефективність, характеризуються роботою тільки в умовах прямої видимості, малим і середнім радіусами дії БС.

Таким чином, дані технології, роблячи певний крок уперед у порівнянні з використанням Wi-Fi для ШБД, не відповідають сучасним вимогам до мультисервісних бездротових широкосмугових мереж.

*WiMAX* є наступним поколінням систем ШБД, збудованих на базі сімейства стандартів IEEE 802.16 WiMAX Forum [47]. Перші промислові продукти WiMAX будувалися на базі стандарту IEEE 802.16d-2004, який описує радіоінтерфейс фіксованого бездротового доступу Fixed WiMAX. Пізніше вийшов стандарт IEEE 802.16-2009, який не став розвитком IEEE 802.16d-2004, але впорядкував та зібрав усі попередні релізи цього стандарту. Поява систем WiMAX різко підвищило інтерес до бездротових технологій, оскільки ці параметри систем революційно відрізняються від систем попереднього покоління використанням широкосмугових сигналів OFDM з базою 256, яке дозволяє забезпечувати ефективний та стійкий зв'язок навіть за умов непрямої видимості; забезпеченням якісної підтримки багаторівневого QoS для побудови мультисервісних операторських та корпоративних мереж; зниженням вартості КУ порівняно з більшістю Pre-WiMAX-систем.

*Mobile WiMAX* є революційною технологією, в якій абоненти отримали можливість переміщатися між зонами дії БС без втрати з'єднання (хендовер). Зворотною стороною мобільності стала необхідність обслуговування мобільних КУ з малопотужними передавачами та «слабкими» антенами, що вимагало кардинальних удосконалень радіоінтерфейсу: застосування складних сигналів OFDM з кількістю компонентів до 2048 року; використання масштабованої OFDMA; підтримка MIMO A та MIMO B.

Все вищезазначене дозволяє значно збільшити радіобюджет каналу між КУ та БС та надавати послуги для USB-модемів усередині будівель. Поліпшення радіобюджету можна конвертувати на перевагу декількома способами: збільшення зони обслуговування БС; поліпшення модуляції, отже, і швидкості КУ; можливість використання більш простих та менш дорогих КУ у фіксованій мережі Mobile WiMAX.

Таким чином, доступність частотного діапазону накладає суттєві обмеження застосування тієї чи іншої технології. Якщо використання 2,4 ГГц обмежене розгортанням Wi-Fi та Pre-WiMAX-мереж, то в діапазон 5 ГГц можливе використання технологій Fixed та Mobile WiMAX. Якщо говорити про Mobile WiMAX в діапазоні 5 ГГц, то можливим рішенням для організації фіксованого широкосмугового доступу є використання Alvarion Breeze MAX Extreme 5000, в якому реалізовано Scalable Orthogonal Frequency-Division Multiplexing Access (SOFDMA) (кількість компонентів OFDM – до 2048), доступні MIMO A і MIMO B, а також розширена підтримка QoS і забезпечується висока інформаційна безпека. Це дозволяє будувати ефективні високошвидкісні мережі останньої милі із підключенням абонентів в умовах непрямої видимості та наданням якісних мультисервісних послуг.

### 3.2.2. Wi-Fi-мережі

Технологія Wi-Fi народилася як надання широкосмугового доступу до Internet, використовує радіосигнал. Маршрутизатор або бридж із спеціальним радіопередавачем на борту приймає трафік з Internet або локальної мережі, перетворюючи отримані дані на радіосигнал, який може бути прийнятий і рахований кінцевими пристроями, що підтримують відповідний формат. Обмін між передавачем та кінцевим пристроєм відбувається симетрично.

Офіційним народженням Wi-Fi можна вважати 1997 р., коли було створено робочу групу IEEE 802.11, що займається створенням стандартів бездротових мереж (Wireless Local Area Networks – WLANs) з наступною основною специфікацією, що передбачає обмін даними між пристроями на швидкості 1-2 Mbps на частоті 2.4 GHz. У 1999 р. технологія Wi-Fi почала проникати у сферу домашнього використання.

В абревіатурі Wi-Fi закладено словосполучення Wireless Fidelity, що буквально перекладається як «цифрова прихильність». Усі реалізації стандартів IEEE 802.11 тестуються організацією Wi-Fi Alliance – об'єднання найбільших виробників та бездротових пристроїв. Успішне тестування Wi-Fi Alliance є запорукою успішної спільної роботи пристроїв різних виробників. Протестовані пристрої мають спеціальний логотип (рис. 3.30).

Wi-Fi використовує два частотні діапазони: 2.4 GHz (зазвичай 802.11b) і 5 GHz (зазвичай 802.11 a). Багато років стандарт 802.11b був першим за популярністю стандартом серед Wi-Fi-користувачів з огляду на підтримку великою кількістю пристроїв та меншою вартістю порівняно з 802.11a. Стандарт 802.11b використовує діапазон 2.4 GHz. Максимальна швидкість

передачі даних, що підтримується, становить 11 Mbps, на практиці – не більше 6 Mbps.

Рис. 3.30. Логотип протестованих Wi-Fi-пристроїв

Стандарт 802.11 a використовує діапазон 5 GHz, що збільшує ймовірність втрати сигналу через перешкоди у вигляді стін та інших предметів. Максимальна швидкість, що забезпечується, – 54 Mbps, на практиці – не більше 25 Mbps.

У 2003 р. швидкість і відстань Wi-Fi, що покривається, збільшилася завдяки появі стандарту 802.11 g. Даний стандарт працює в діапазоні 2.4 GHz, забезпечуючи максимальну пропускну здатність 54 Mbps, на практиці – 10-27 Mbps, і має зворотну сумісність із 802.11 b.

У 2009 р. світ побачила фінальна версія стандарту 802.11 n, що дає відчутний стрибок у продуктивності та надійності сигналу в порівнянні з попередніми технологіями завдяки застосуванню способу кодування MIMO. Це метод просторового кодування сигналу, при якому для передачі та прийому використовуються групи антен по дві і більше відповідно (рис.3.31). Між передаючими та приймальними антенами одного пристрою мінімізується взаємний вплив.


Рис. 3.31. Принцип Multiple Input Multiple Out

Перший патент на використання MIMO був зареєстрований ще в 1984 р. Стандарт працює на частоті 2.4–2.5 і 5 ГГц і назад сумісний з 802.11 a/b/g, тому позначається, як 802.11 a/b/g/ n. Максимальна швидкість передачі даних стандарту – 300 Mbps.

У 2011 р . вийшов новий стандарт 802.11 ac, одним з основних завдань якого був вихід на межу пропускної спроможності 1 Gbps (табл.3.2.).

Таблиця 3.2. Параметри стандартів 802.11 n та 802.11 ac

| | 802.11n | 802.11n IEEE Specification | 802.11 ac Wave 1 | 802.11 ac Wave 2 WFA Certification Process Continues | 802.11 ac IEEE Specification |
|---|---|---|---|---|---|
| Частота | 2.4 Ghz & 5 Ghz | 2.4 Ghz & 5 Ghz | Today 5 Ghz | **5 Ghz** | 5 Ghz |
| MIMO | Single User (SU) | Single User (SU) | Single User (SU) | Multi User (SU) | Multi User (SU) |
| Ур. PHY | 450 Mbps | 600 Mbps | 1.3 Gbps | 2.34 Gbps-3.47 Gbps | 6.9 Gbps |
| Ширина каналу | 20 or 40 MHz | 20 or 40 MHz | 20, 40, 80 MHz | 20, 40, 80, 80-80. 160 MHz | 20, 40, 80, 80-80. **160 MHz** |
| Модуляція | 64 QAM | 64 QAM | 256 QAM | 256 QAM | 256 QAM |
| Простор потоки | 3 | 4 | 3 | 3-4 | 8 |
| MAC Throughout* | 293 Mbps | 390 Mbps | 845 Mbps | 1.52 Gbps-2.26 Gbps | 4.49 Gbps |

* Забезпечує 65% MAC- ефективність з більш високим MCS

Стандарт спирається лише на частоту 5 GHz , хоча в ньому заявлено підтримку всіх попередніх стандартів. Теоретично фінальна версія стандарту забезпечує максимальну швидкість 6.9 Gbps. Стандарт розвивався поетапно, і за результатами кожного їх створювався окремий реліз стандарту (802.11 ac Wawe 1, 802.11 ac Wawe 2) для якнайшвидшого застосування. Стандарт використовує технологію MU-MIMO (Multi User MIMO), що дозволяє одному користувачеві підключати кілька КУ, даючи можливість використовувати кілька одночасних вихідних потоків, що відкриває широкі можливості для Internet of Things (IoT), підтримує високу продуктивність, велику щільність клієнтів, а також передбачає економне енергоспоживання (рис.3.32).

Ще одним принципово новим кроком у стандарті 802.3. ac є можливість beamforming. Beamforming – це кероване формування сигналу, можливе з допомогою роботи кількох роздільних антен, що дозволяє автоматично у реальному часі змінювати діаграму спрямованості точки доступу залежно від розташування КУ (рис. 3.33). Кінцева мета цієї функції – концентрувати

потужність випромінюваного сигналу в районі розташування клієнтів, забезпечуючи їх якісним сигналом та заощаджуючи енергоспоживання.

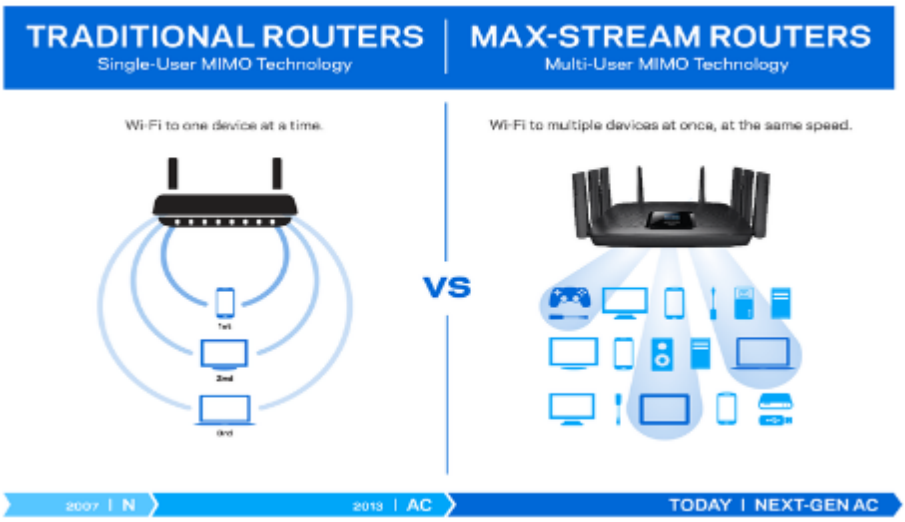



Рис. 3.32. Переваги Multi-user MIMO


Рис. 3.33. Технологія beamforming

У 2012 р. з'явився стандарт IEEE 802.11ad, який став частиною реалізації MGWS (Multigigabit Wireless System) – концепції високошвидкісної мережі, що базується на частотному діапазоні в області 60 GHz. Wi-Fi-рішення, що базуються на частотах в області 60 GHz також отримали умовну назву WiGig . Розглянутий діапазон, як і 2.4 GH, і 5 GHz. Цей діапазон (60 GHz) накладає великі обмеження на поширення радіосигналу. Сигнал не може оминати перешкоди. Область впевненого прийому сигналу обмежена радіусом не менше 10 метрів. Однак висока частота, що несе, може забезпечувати високу швидкість передачі даних, що робить технологію перспективною для таких застосувань, як, наприклад, передача стисненого відео високої чіткості. Через невелику потужність точок доступу (до 10 dBm) і поглинання хвиль стінами приміщення добре вирішується проблема засміченості ефіру.

Стандарт покриває частотний діапазон 57 ÷ 71 GHz , що ділиться на 6 каналів (табл.3.3). Кожен з каналів займає смугу 2160 MHz і забезпечує пропускну здатність 1760 MHz .

Таблиця 3.3. Частотний діапазон 802.11 ad

| Канал | Центр ( GHz ) | мін. ( GHz ) | Макс. ( GHz ) | BW ( GHz ) |
|---|---|---|---|---|
| 1 | 58.32 | 57.24 | 59.40 | 2.16 |
| 2 | 60.48 | 59.40 | 61.56 | |
| 3 | 62.64 | 61.56 | 63.72 | |
| 4 | 64.80 | 63.72 | 65.88 | |
| 5 | 66.96 | 65.88 | 68.04 | |
| 6 | 69.12 | 68.04 | 70.20 | |

Технології WiGig стикаються з проблемою пропускної спроможності комутаторів доступу, які пропонують в основному 1 Gbps , що майже вдвічі менше за пропускну здатність, що забезпечується WiGig. Також необхідно зазначити, що в багатьох країнах світу діапазон частот, що використовуються стандартом, може бути значно обмежений з причин зайнятості певних смуг (табл.3.4).

Таблиця 3.4. Обмеження на використання діапазону частот 802.11 ad

| Регіон | Нижня межа | Верхня межа | Використ . канали | Примітка |
|---|---|---|---|---|
| США | 57.05 GHz | 71.00 GHz | 1, 2, 3, 4, 5, 6 | Розширено для включення 64-71 GHz у 2016 |
| Канада | 57.05 GHz | 64.00 GHz | 1, 2, 3 | Очікується включення 64-71 GHz наприкінці 2021 |
| Південна Корея | 57.00 GHz | 64.00 GHz | 1, 2, 3 | |
| ЄС | 57.00 GHz | 66.00 GHz | 1, 2, 3, 4 | Відкриття 66-71GHz рекомендується |
| рф | 57.00 GHz | 66.00 GHz | 1, 2, 3, 4 | |
| Японія | 57.00 GHz | 66.00 GHz | 1, 2, 3, 4 | 57-59 GHz додані в 2011 |

| | | | | |
|---|---|---|---|---|
| Австралія | 57.00 GHz | 66.00 GHz | 1, 2, 3, 4 | Діапазон розширено у 2018 |
| Китай | 59.00 GHz | 64.00 GHz | 2, 3 | також IEEE 802.11aj |
| Сінгапур | 57.00 GHz | 66.00 GHz | 1, 2, 3, 4 | Станом на вересень 2019 року |

Стандарт 802.3 ad використовує прості види модуляції, такі як BPSK та QPSK – двійкова та квадратурна модуляція відповідно.

### 3.2.3. WiMAX-мережі

На даний момент найбільш ефективними системами бездротового доступу є системи, побудовані на основі сімейства стандартів IEEE 802.16 [48].

Сімейство стандартів IEEE 802.16 включає такі стандарти:

- базовий стандарт IEEE 802.16 – Air Interface for fixed BWA system (описує бездротовий інтерфейс у діапазоні 10-66 ГГц) був прийнятий у грудні 2001;
- розширення базового стандарту IEEE 802.16a – Medium Access Control Modification and additional physical layer Specification for 2-11 GHz, був прийнятий в січні 2003 р .;
- чинний стандарт IEEE 802.16-2004 – Air Interface for fixed BWA system стандарт, що описує систему бездротового фіксованого доступу, увібрав у себе і замінив собою 802.16, 802.16a, 802.16c. Було прийнято у червні 2004 р.;
- останній на сьогоднішній момент IEEE 802.16e-2005 – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands , стандарт, що описує бездротовий мобільний та фіксований доступ (Було прийнято у грудні 2005 р.).

Далі розглянемо стандарти IEEE 802.16-2004 та IEEE 802.16 e-2005, оскільки на їх основі створюються діючі системи, і саме їх просуванням займається WiMAX Forum.

WiMAX Forum, неприбуткова організація, що об'єднує понад 470 операторів та виробників систем бездротового зв'язку, організована для розвитку та просування на ринок систем на базі сімейства стандартів IEEE 802.16. Стандарти сімейства IEEE 802.16 описують загальні принципи побудови систем та діапазони можливих значень того чи іншого параметра. При цьому системи, що відповідають IEEE 802.16, можуть бути не сумісні між собою через відсутність єдиних жорстких вимог до параметрів радіоінтерфейсу . Завданням WiMAX-форуму є розробка рекомендацій (так званих профілів сертифікації) щодо створення сумісних між собою систем зв'язку в рамках рекомендацій IEEE 802.16, а також проведення сертифікації

щодо сумісності систем зв'язку, створених на базі профілів, розроблених WiMAX-форумом. В рамках кожного стандарту всередині сімейства IEEE 802.16 може бути декілька профілів.

Таким чином, системи, що пройшли сертифікацію WiMAX Forum, будуть сумісні між собою, про що говоритиме розміщений на такому устаткуванні відповідний логотип.

Стандарт IEEE 802.16-2004 (далі для стислості будемо називати все, що стосується IEEE 802.16-2004, словом WiMAX) описує інтерфейс бездротового фіксованого доступу. Системи цього стандарту мають такі параметри:

- сумарна швидкість на КУ до 13 Мб/с;
- швидкість сектора може досягти 100 Мб/с;
- дальність зв'язку – до 40 км;
- робота за умов непрямої видимості;
- смуга частот – 3,5 МГц, 5 МГц, 7,5 МГц, 10 МГц;
- капітальні витрати на побудову БС близько 70 тис. дол. США.

Операторські мережі на базі стандарту IEEE 802.16-2004 почали з'являтися наприкінці 2005 року.

Стандарт IEEE 802.16e-2005 (далі для стислості будемо називати все, що стосується IEEE 802.16e-2005, мобільний WiMAX) відрізняється від IEEE 802.16-2004 наданням послуг не тільки фіксованим користувачам, але й мобільним і, як наслідок, вимогам діапазонів нижчих частот (до 3,5 ГГц), а також деякими параметрами радіоінтерфейсу, що дозволяють системі надавати послуги в умовах поганого енергетичного бюджету радіоканалу, характерного для мобільних пристроїв, що мають малий коефіцієнт посилення ненаправленої антени та низьку потужність передавача. Мережі мобільного WiMAX можуть надавати послуги не лише рухливим користувачам. Відповідно до рекомендацій WiMAX форуму існує п'ять рівнів мобільності, які представлені в табл. 3.5.

Таблиця 3.5. Рівні мобільності

| **Рівень мобільності** | **Пристрої** | **Розташування / швидкість** | **Handover** | **IEEE 802.16-2004** | **IEEE 802.16e-2005** |
|---|---|---|---|---|---|
| Фіксований | Зовнішні та внутрішні CPE | Фіксована / стаціонарна | Ні | Так | Так |
| Мігруючий | Внутрішні CPE , PCMCIA | Множинна / стаціонарна | Ні | Так | Так |
| Портативний | Ноутбуки, PCMCIA | Множинне / прогулянкове | Жорсткий Handover | Ні | Так |
| Проста мобільність | Ноутбуки, PCMCIA , КПК, смартфони | Множина / транспорт на низькій швидкості | Жорсткий Handover | Ні | Так |

| | | | | | |
|---|---|---|---|---|---|
| Повна мобільність | Ноутбуки, PCMCIA , КПК, смартфони | Множина / транспорт на високій швидкості | М'який Handover | Ні | Так |

Розглянемо деякі параметри радіоінтерфейсу, які роблять мобільний WiMAX (IEEE 802.16e-2005) найефективнішою технологією систем радіодоступу. У WiMAX використовується OFDM. OFDM одна із методів побудови складних сигналів, тобто сигналів, які мають база сигналу набагато більше 1 [45]. Метод OFDM полягає у поділі сигналу на частини, передачі цих частин на сусідніх частотних каналах ( піднесучих-subcarrier ) (рис. 3.34) та відновлення сигналу на приймальному пристрої.

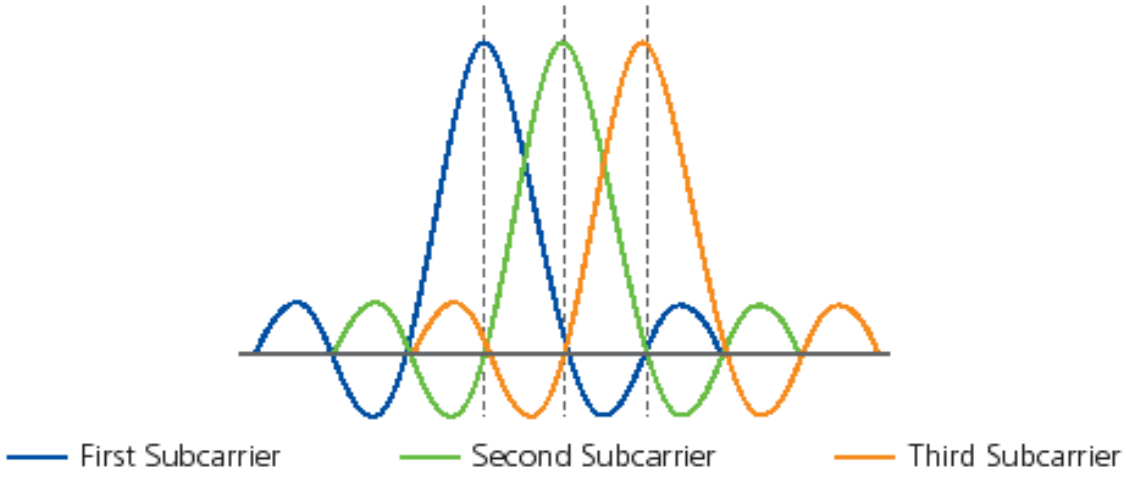



Рис. 3.34. Розподіл ортогональних піднесучих OFDM на частотній осі

Кількість таких частин і відповідно частотних піднесучих вказується як параметр OFDM, наприклад, OFDM64 або OFDM1024. OFDM дозволяє ефективно будувати складні сигнали, які мають гарну перешкодозахисність і високу достовірність прийому в умовах перевідбиття сигналу.

FDM використовується в багатьох радіотехнологіях, у тому числі в Wi-Fi, стаціонарному і мобільному WiMAX, в різних нестандартизованих рішеннях. У IEEE 802.11 a/g (Wi-Fi) використовується OFDM64, в IEEE 802.16-2004 – O

FDM256, а в IEEE 802.16e-2005 – від OFDM512 до OFDM2048.

Ефективність OFDM в умовах перевідбиття обумовлюється більшою тривалістю кожного сигналу (кадра) у кожній піднесучій порівняно з простим сигналом (більше в N разів, де N – кількість піднесучих від 64 до 2048) і, відповідно, відносно меншим пошкодженням кадру при «накладенні» «копій» сигналів, що прийшли із запізненням внаслідок багатопроменевого поширення.

У мобільному WiMAX використовується технологія доступу до середовища OFDMA, а точніше Scalable Orthogonal Frequency-Division Multiplexing (SOFDM), яка базується на OFDM. OFDMA надає конкретному користувачеві в конкретний час певні групи піднесучих об'єднаних в

підканал, побудований на базі OFDM [46]. Таким чином, користувачі можуть використовувати різні частотні підканали різні проміжки часу (рис.3.35).

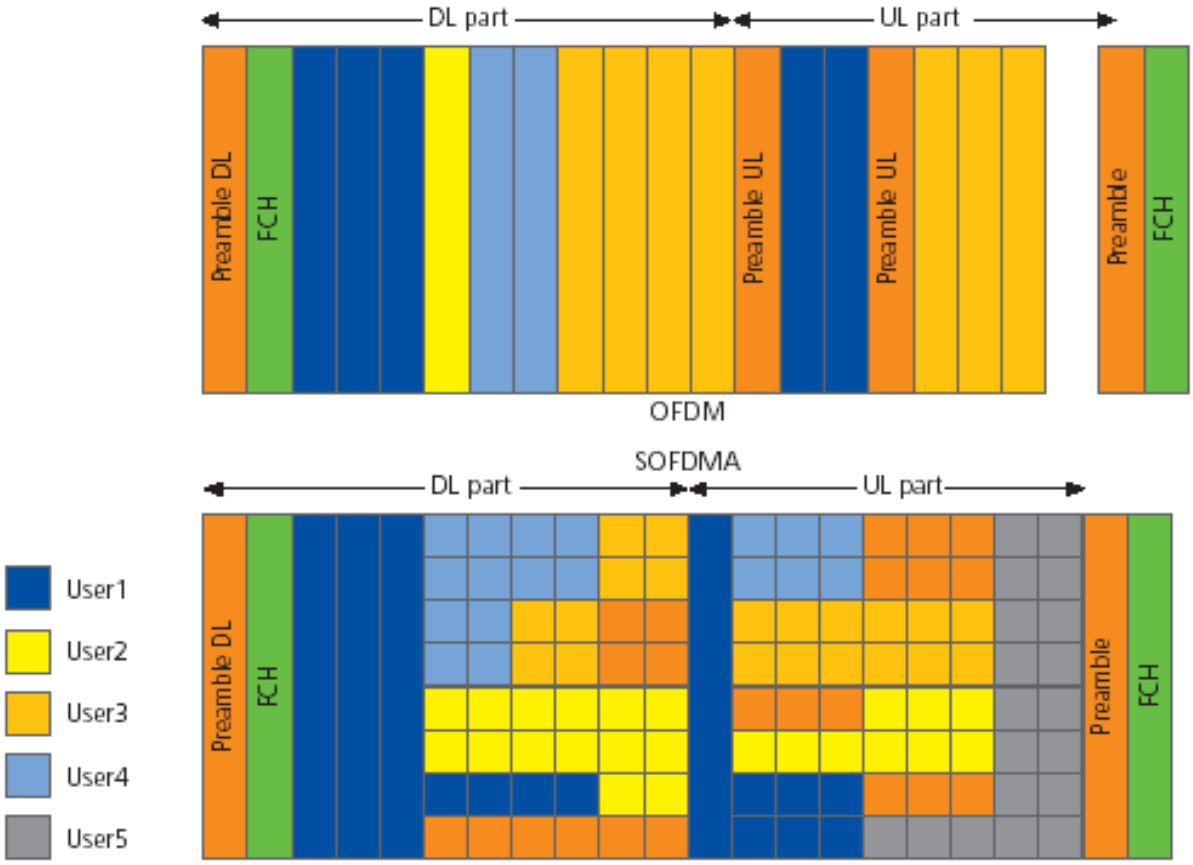



Рис. 3.35. Застосування OFDM, OFDMA, SOFDMA у IEEE 802.16e-2005

Такий поділ на підканали дозволяє ефективніше використовувати потужність передавача і підвищити спектральну ефективність, а також знизити вплив перешкод багатостанційного доступу.

*SOFDMA – Scalable OFDMA.* Є розширенням OFDMA, що дозволяє гнучко підлаштовувати систему мобільного WiMAX під доступний частотний ресурс [46].

Це відбувається шляхом адаптації розміру вибірки перетворення Фур'є під ширину смуги частот, що використовується. Справа в тому, що у приймачі системи мобільного WiMAX виконується швидке перетворення Фур'є (Fast Fourier Transformatio – FFT), а в передавачі мобільного WiMAX використовується зворотне швидке перетворення Фур'є (Inverse Fast Fourier Transformation – iFFT). Розмір вибірки FFT, рівний ступеням 2, в даному випадку дорівнює кількості піднесучих, що використовуються. Так, для ширини каналу, що дорівнює 5 МГц, використовується 512 піднесучих (OFDM512), а для 10 МГц – 1024 (OFDM1024). Кількість піднесе і, відповідно, розмір FFT змінюється пропорційно використовуваної оператором смузі частот (від 1,25 МГц до 20 МГц).

Використання SOFDMA дозволяє сконцентрувати потужність передавача на певних підканалах, тобто підвищити спектральну густину сигналу, що особливо важливо для роботи з мобільними пристроями, у яких потужність випромінювання та коефіцієнт посилення антен відносно невеликі.

Smart Antenna – розумні антени, що застосовуються для підвищення ефективності використання антенних систем [49]. Система «розумна антена» базується на використанні технологій MIMO та Adaptive Antenna System (AAS).

Технологія MIMO застосовується підвищення ефективності системи WiMAX в умовах непрямої видимості (Non-Line of Sight – NLOS) та супутнім йому умовам багатопроменевого поширення [50]. Умови NLOS характерні для стаціонарного зв'язку в умовах міської забудови та передмістя, а також для мобільного зв'язку. Відповідно до теорії поширення радіохвиль, достовірність інформації, що приймається, різко знижується за наявності будь-якого відбиває об'єкта на шляху радіохвиль, відбившись від якого хвиля може прийти на приймальну антену з спотвореннями або кілька разів зі зміщенням по фазі. Технологія MIMO полягає у використанні декількох приймачів і антен як на БС, так і на КУ. І, відповідно, побудові кількох ліній зв'язку між БС та КУ. Ефективність використання MIMO може бути представлена у двох ситуаціях.

MIMO дозволяє підвищити достовірність інформації, що приймається за допомогою аналізу, прийнятого кількома приймачами і антенами сигналу, і виділення вихідного. MIMO дозволяє підвищити швидкість передачі інформації за рахунок кількох паралельних ліній зв'язку, якими паралельно передається корисна інформація і таким чином збільшується швидкість передачі. Слід зазначити, що MIMO використовується не тільки в мобільному WiMAX, але також і в остаточній редакції стандарту IEEE 802.11n, що приймається найближчим часом.

Основними перешкодами для впровадження MIMO є складність і високі матеріальні витрати при виробництві КУ з кількома модулями, що приймають, і кількома антенами. Тому поки що більш поширена технологія Single Input Multiple Output (SIMO), з одним приймально-передавальним модулем на КУ та кількома модулями на БС. На рис. 3.36 представлена БС та два КУ, що працюють за технологією MIMO. При цьому БС використовує рознесення 4-го порядку, а КУ – рознесення 2-го порядку, що цілком виправдано за критерієм співвідношення ціна/якість.

AAS-технологія заснована на вирішенні beamforming. Нагадаємо, суть принципу beamforming полягає у формуванні кількох спрямованих «пелюстків» випромінювання антени замість одного (рис. 3.37).

Реалізація цього принципу базується на використанні фазованих антенних решіток (ФАР), які дозволяють реалізувати необхідну форму діаграми спрямованості антени за допомогою зміщення фази сигналу, що випромінюється або приймається на кожному елементі такої антени..

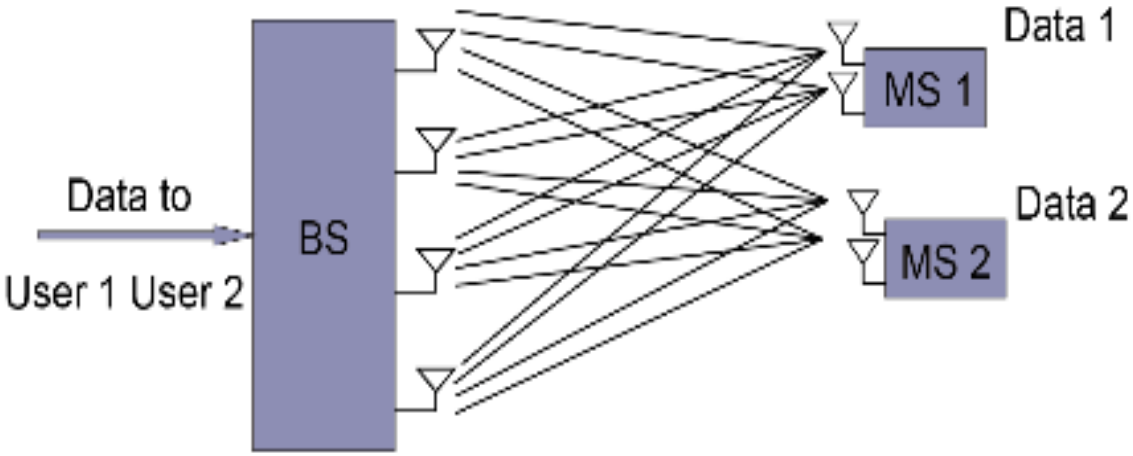



Рис. 3.36. Варіант реалізації MIMO

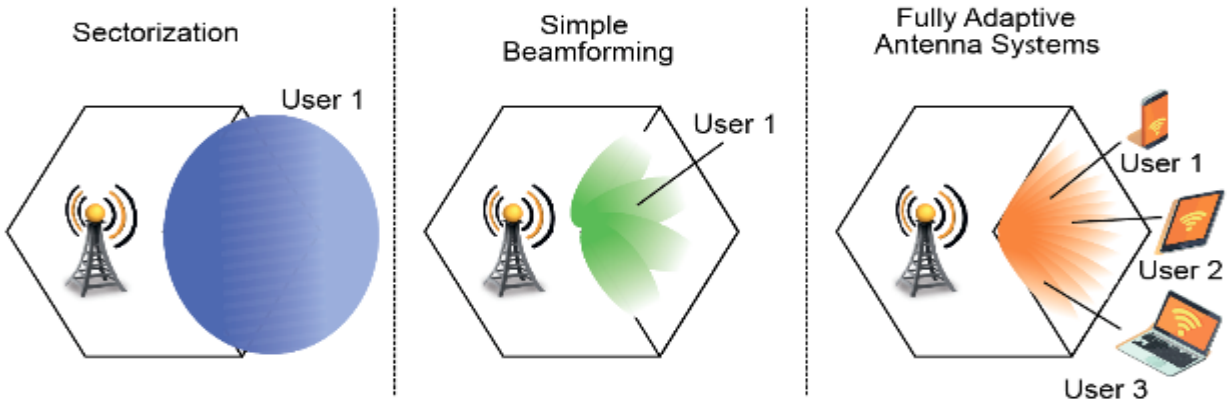



Рис. 3.37. Застосування рішення beamforming у WiMAX

Результатом використання принципу beamforming є збільшення «ефективного» коефіцієнта посилення антени для кожного КУ. В результаті проведених експериментів було з'ясовано, що 4-елементна ФАР у режимі beamforming може на 6 дБ покращити радіобюджет , тим самим суттєво покращивши параметри радіоканалу та пропускну спроможність системи для кожного користувача без побудови додаткових БС

Розглянемо структуру системи на базі IEEE 802.16-2004 (або IEEE 802.16e-2005 у стаціонарному режимі) та використання її для побудови «останньої милі» (рис. 3.38).

У цій структурі чітко виділено центральний вузол, який забезпечує обслуговування контролю доступу користувачів, управління мережею, доступ до інших мереж передачі інформації. Крім того, виділено магістральну мережу, на базі якої розгорнуто мережу доступу IEEE 802.16. Для скорочення ROI цієї мережі можливе надання стороннім користувачам інформаційних та телекомунікаційних послуг на базі пропонованої мережі. У

цьому випадку необхідна реалізація в магістралі технології MPLS та підсистеми білінгу.

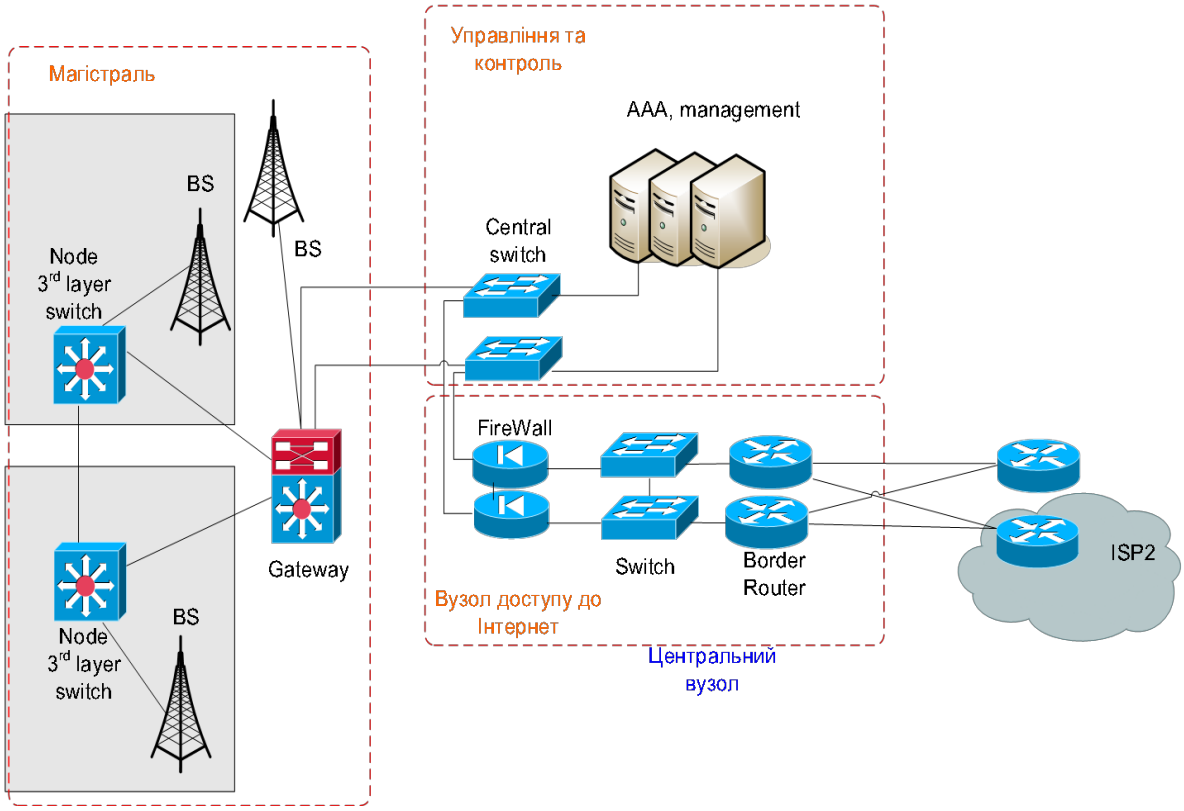



Рис. 3.38. Структура мережі доступу IEEE 802.16 для стаціонарних абонентів

Для забезпечення мобільності користувачів мережа, побудована на базі стандарту IEEE 802.16e-2005, повинна мати вузлову інфраструктуру, аналогічну до інфраструктури мобільних операторів, оскільки для абонентів при переході від БС до БС потрібно забезпечити безшовний хендовер не тільки на другому рівні моделі OSI, але так а й на третьому.

Таким чином, канали зв'язку на базі стандарту IEEE 802.16e-2005 будуть побудовані на передових технологіях бездротових комунікацій і забезпечать більшу енергетичну ефективність, навіть у порівнянні з системами IEEE 802.16-2004, що робить їх вельми привабливими для організації високоефективної бездротової останньої. Зворотною стороною медалі впроваджених передових технологій у системах мобільного WiMAX є збільшення капітальних витрат на розгортання кожної БС на 30–40% порівняно зі стаціонарним WiMAX.

Економічну ефективність розгортання корпоративної мережі на базі даної технології можна визначити за критерієм мінімізації капітальних та операційних витрат на розгортання корпоративної мережі з урахуванням зони покриття однієї БС, реальної ємності кожної БС та всієї мережі, необхідних сервісів, необхідності мобільності користувачів.

### 3.2.4. Особливості побудови бездротової корпоративної мережі

За останні кілька років мобільні бездротові пристрої міцно проникли у життя сучасної людини. Кордони робочого місця «розмиваються» та «мігрують» у бік мобільності офісного середовища. Комп'ютерний парк на підприємствах та в організаціях оновлюється значно рідше в порівнянні з особистими (персональними) пристроями співробітників, та й за зручністю використання їм істотно поступається. Масове поширення смартфонів та планшетних комп'ютерів призводить до поступового витіснення стаціонарних комп'ютерів та ноутбуків із робочих місць. В умовах, що склалися, одне з найбільш актуальних завдань у бездротовій корпоративній мережі – реалізація концепції використання власних пристроїв (Bring your own device – BYOD). Ключовим елементом концепції є впровадження системи управління політиками та побудова безпечної корпоративної бездротової мережі.

У більшості випадків питання розгортання бездротової мережі вирішується встановленням кількох точок доступу і є ніби надбудовою над провідною інфраструктурою, керованої окремо. Такий підхід виправдовує себе в домашньому сегменті та є недостатнім для застосування в корпоративному. Вимоги до бездротових мереж вже давно не обмежуються лише організацією інтерфейсу між бездротовим КУ та провідною інфраструктурою.

Сучасна корпоративна мережа повинна мати можливість передачі мультимедійних даних (дані, голос і відео), забезпечувати високу продуктивність і безпеку, мати гарну масштабованість, простоту розгортання та управління, а також надавати додатковий функціонал з розширення спектру користувацьких сервісів та їх адаптації. Крім того, при побудові корпоративної бездротової мережі рішення повинно мати можливості профілювання пристроїв, що підключаються, виконувати процедуру гостьового доступу і вміти відстежувати місце розташування випромінюючих пристроїв.

В основу архітектури бездротової мережі (рис.3.39) покладено принцип централізованого керування та розширення бездротових сервісів [51]. Основний функціонал покладається на контролер бездротової мережі, а точки доступу працюють у «полегшеному режимі». Точки доступу забезпечують радіоінтерфейс і шифрування даних користувача, передаючи всі дані користувача на контролер у зашифрованому тунелі, а також надають широкі функції з діагностики та звітності.

Для організації радіопокриття у вирішенні є широка лінійка точок доступу. Їх можна умовно поділити на три групи: системи початкового рівня, корпоративного рівня та точки доступу у зовнішньому виконанні. Всі пропоновані виробником точки доступу підтримують стандарт 802.11n і відрізняються кількістю радіомодулів, потоків передачі даних, що

підтримуються, і можливістю підключення зовнішньої антени. Пропоновані пристрої підтримують три режими роботи:

- точка доступу (обслуговування абонентів у режимі точка-багатоточка);
- міст (реалізація лінії зв'язку точка-точка);
- повнозв'язковий режим (MESH – мережа, що передбачає бездротову лінію зв'язку між точками).

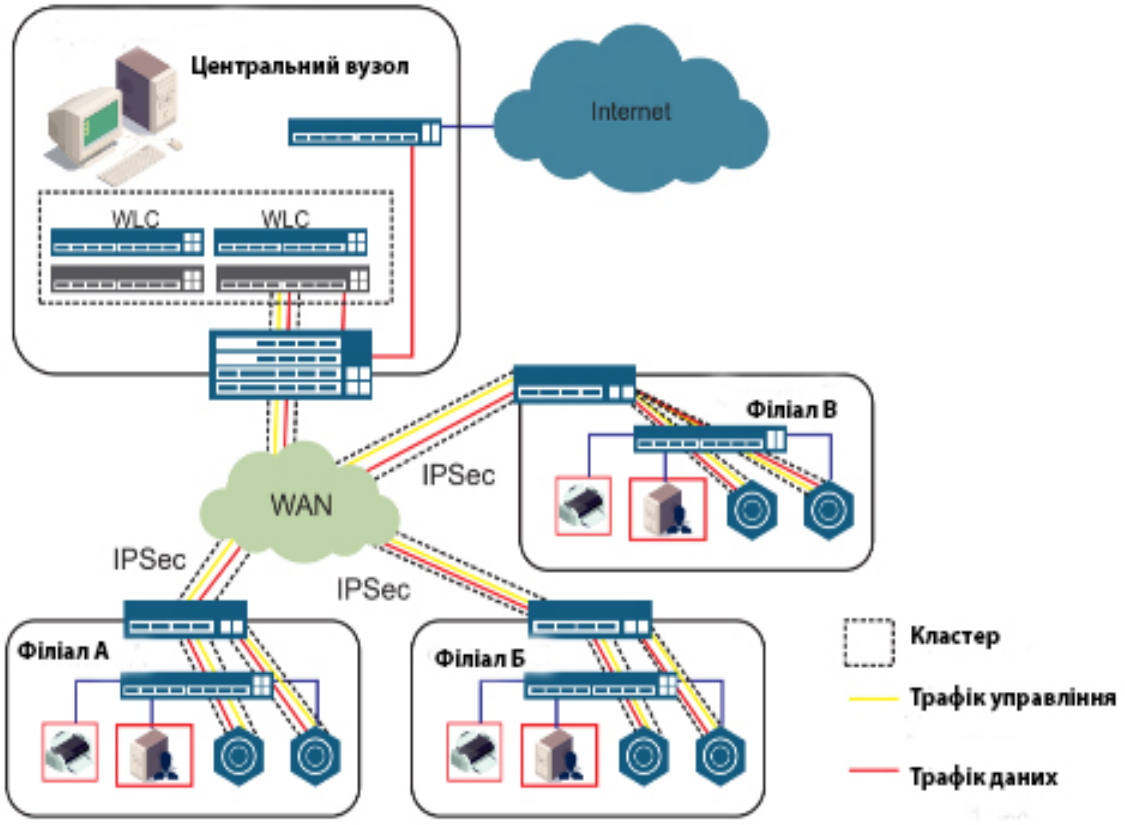



Рис. 3.39. Архітектура бездротової мережі

Застосування універсальних пристроїв у відповідних режимах роботи уможливлює побудову розподіленої бездротової мережі під будь-які вимоги абонентів. Традиційно застосовуються два типи архітектури: розміщення контролера на центральному вузлі та у філіях. При розміщенні контролера на центральному вузлі використовується централізована комутація. При цьому весь трафік проходить через контролер, що призводить до значного завантаження WAN-каналів. У представлених на ринку промислових наборах програмних та апаратних засобів для бездротової мережі точки доступу використовують власні приватні протоколи виробників обладнання, мають можливість продовжувати обробляти звернення користувачів та здійснювати взаємодію з RADIUS-сервером у разі відмови WAN-каналу. Незважаючи на відсутність перерви у наданні сервісу, дані протоколи мають приватний характер і призначені для обмеженої кількості віддалених офісів. Так, наприклад, рішення компанії Juniper Networks вільне від цього недоліку і

дозволяє використовувати локальну комутацію. При цьому через контролер проходить лише службовий трафік, а всі дані комутуються точкою доступу безпосередньо на шлюз призначення. У системі реалізована краща для надання мобільності модель оптимальної передачі трафіку користувача при збереженні централізованого контролю та обліку. Розподілена комутація забезпечує безпрецедентну якість бездротового каналу, реалізуючи мінімальну у галузі затримку передачі, що особливо важливо передачі «голосового» трафіку.

Необхідність підвищення стійкості до відмов мережі викликала відмову від ідеї використання гарячого резервування і призвела до кластеризації контролерів. Об'єднання контролерів у кластер дозволяє суттєво оптимізувати кількість використовуваних ліцензій на підключення точок доступу. Немає необхідності тримати ліцензії, що не використовуються, на випадок виходу з ладу первинного контролера. Основною відмінністю даного рішення є можливість об'єднання в кластер будь-яких типів контролерів різних апаратних серій, так і віртуальних. Реалізація загальної програмної платформи дає адміністраторам можливість проводити оновлення ПЗ без перерви у наданні сервісів.

Більшість сучасних бездротових пристроїв підтримує роботу у двох діапазонах – 2,4 ГГц та 5 ГГц. Історично діапазон 2,4 ГГц почав використовуватися раніше і зараз значно більш завантажений порівняно з діапазоном 5 ГГц. Система бездротового зв'язку компанії Juniper забезпечує автоматичне балансування клієнтів між точками, а функція групування клієнтів здійснює пріоритетне підключення КУ в діапазоні 5 ГГц, і тільки при неможливості приєднання відбувається підключення в діапазоні 2,4 ГГц.

Для забезпечення максимальної пропускної спроможності це рішення дозволяє виявляти, класифікувати та локалізувати джерела перешкод у режимі реального часу в обох робочих діапазонах. Вся інформація про перешкоди консолідується в системі управління Network director, надаючи графічний інтерфейс для усунення несправностей.

За допомогою системи управління Network director також здійснюється управління життєвим циклом бездротової мережі: планування та розгортання, конфігурування та налагодження, моніторинг, звітність та визначення розташування. Відстеження розташування користувачів, реалізація безшовного переходу між точками доступу та забезпечення заданої якості обслуговування потребують більш щільного розміщення точок доступу. Функції самовідновлення та якість роботи сервісів забезпечуються централізацією управління за допомогою контролера та залежить від правильного планування бездротової мережі.

На початковому етапі розгортання мережі використовується 3D-планувальник, який враховує загасання радіосигналу в різних видах матеріалів, взаємне розташування точок доступу та призначений для проведення розрахунків як усередині приміщення, так і на відкритій місцевості. Цей етап дуже важливий для подальшої роботи системи. На його

основі здійснюється частотно-територіальне планування бездротової мережі. Грунтуючись на плані розміщення точок доступу та використовуючи метод тріангуляції, система дозволяє визначати точне місце розташування користувача та здійснювати пошук спеціалізованих RFID-міток. Застосування радіолокації надає можливість організувати периметр безпеки та запобігти доступу до мережі за територією підприємства (рис.3.40).

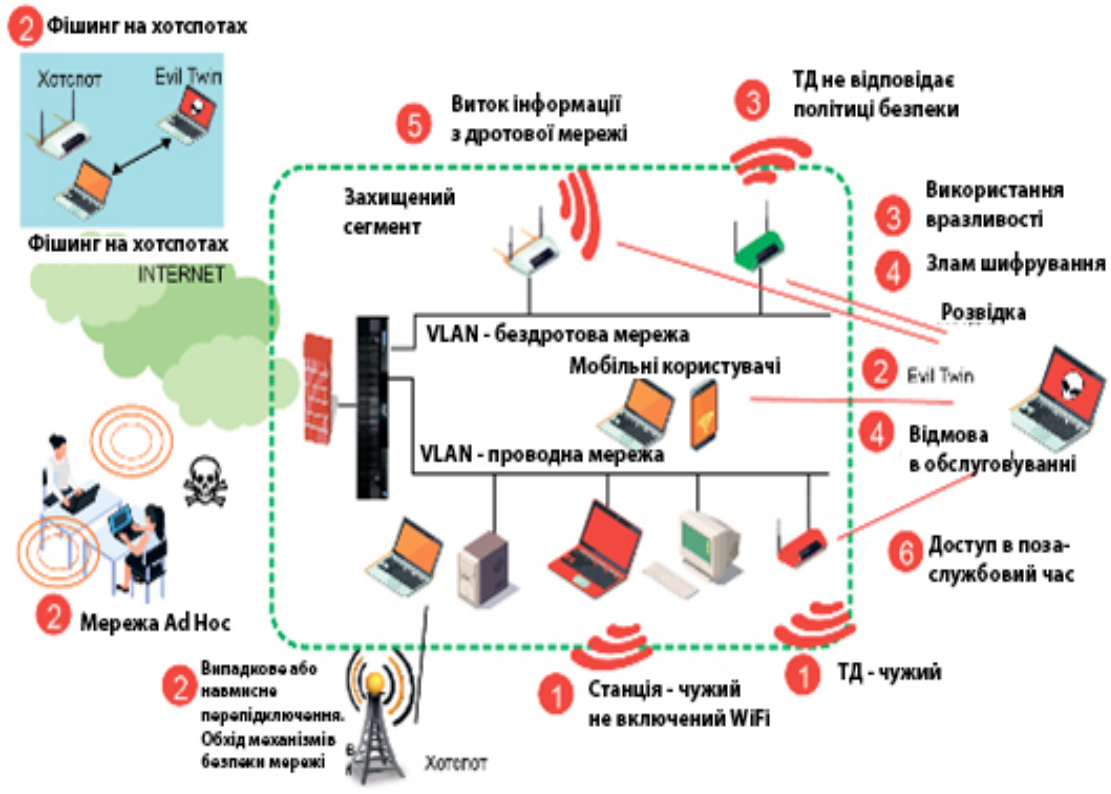



Рис. 3.40. Організація безпеки бездротової мережі

У цьому випадку, навіть володіючи діючими автентифікаційними даними (логін/пароль), зловмисник не зможе отримати доступ до мережі, перебуваючи на прилеглій до офісу території.

Також цей функціонал є цікавим при виділенні зон із забороною на використання бездротового доступу, наприклад, на території процесингового центру або серверної, або при відстеженні переміщень випромінюючого пристрою по території підприємства, надаючи можливість пошуку дорогого мобільного обладнання, з RFID-міткою, та здійснення контролю переміщень користувачів.

Підвищення рівня безпеки мережі здійснюється застосуванням бездротової системи запобігання (виявленню) вторгнень (IPS/IDS). Система проводить внутрішній аналіз на наявність атак на бездротову мережу і має можливість відправляти трафік, що цікавить, на зовнішню систему запобігання вторгнень. Можливість історичного аналізу робить систему незамінною під час розслідування інцидентів.

У сучасній бездротовій корпоративній мережі важливо здійснювати динамічний контроль доступу користувачів. Для цих цілей служить програма керування безпекою SmartPass [52]. ПЗ інтегрується з системою управління Network director та системою відстеження розташування, забезпечуючи контроль доступу на основі фізичного стану та можливість розширених звітів.

Платформа SmartPass Connect варта реалізації концепції використання своїх пристроїв. За необхідності забезпечення доступу до корпоративної мережі витрати адміністраторів значно зростають, а за їх значних обсягах можуть вимагати наявності в організаційній структурі виділених менеджерів. Платформа дозволяє автоматизувати процедуру реєстрації пристрою та організацію доступу до мережі за допомогою корпоративних облікових даних. SmartPass інтегрується з контролером домену і імплементує на пристрій, що підключається, необхідні сертифікати. При цьому система здійснює профіль пристрою – визначається його тип, ОС, її версія, інформація про додатки клієнта спільно з SRX (AppTrack і UAC) і т. д. [53, 54]. Отримувана інформація використовується в корпоративних політиках і дає можливість надавати гранульований доступ до мережі.

Для доступу незареєстрованих користувачів на підприємствах необхідно запровадити процедуру гостьового доступу. SmartPass реалізує повний життєвий цикл управління гостьовим доступом (реєстрація користувача, повідомлення про виділені облікові дані, проведення автентифікації та авторизації, здійснення обмеження доступу, логування подій безпеки та надання докладної звітності).

Для кожного ідентифікатора бездротової мережі (SSID) може бути реалізований адаптований Web-портал із можливістю самообслуговування [55]. Після реєстрації користувач отримує повідомлення одним із трьох можливих варіантів: облікові дані роздруковуються на принтері, надсилаються на електронну пошту або надсилається СМС на вказаний номер мобільного телефону. Гостьові сесії можуть бути обмежені за тривалістю та часом використання, мати різні політики доступу, але в той же час можуть підтримувати моніторинг активних сесій, обліковий запис, логування та детальні звіти. Рішення підтримує RFC 3576, що передбачають зміну авторизації та динамічну зміну параметрів під час сесії, включаючи якість обслуговування QoS, списки доступу ACLs, що виділяється пропускну здатність і т.д.

Стандартизований інтерфейс програмування програм API забезпечує значне розширення функціоналу бездротової системи за рахунок інтеграції з системами білінгу, різними платформами аналітики та звітності.

Таким чином, рішення компанії Juniper Networks для побудови бездротової мережі є одним із найбільш оптимальних за співвідношенням вартості та доступності функціоналу. Пропонований набір промислових програмних та апаратних засобів дозволяє створювати бездротові системи корпоративного класу, що володіють високою відмовостійкістю та

відповідають усім вимогам щодо безпеки, продуктивності та масштабованості. Нині корпоративні бездротові мережі переживають період розквіту. Розвиток бізнес-процесів переносить критично важливі програми у бездротове середовище, роблячи необхідним реалізацію інтерактивних бізнес-додатків. Вимоги мобільності, підвищення конкурентоспроможності та продуктивності праці збільшують вимоги до сервісів, які пропонуються в бездротовій мережі. Описаний підхід дозволяє побудувати універсальну корпоративну бездротову мережу, засновану на стандартних протоколах, адаптовану під потреби практично будь-якої організації та оптимізувати вартість володіння бездротовим сегментом.

## 3.3. Програмно-визначені мережі передачі даних

### 3.3.1. Software-Defined Networking

Класичні мережі, з їх традиційними інструментами управління та автоматизації, виявилися не готовими до сучасної динаміки змін конфігурації та масштабування, а також вимог віртуалізації.

Як відомо, роботу будь-якого класичного мережевого пристрою можна розглядати на трьох рівнях (рис.3.41):

1. Рівень керування пристроєм (Management Plane) – це вбудовані командний рядок, web-сервер, API , протоколи управління. Цей рівень відповідає за зміну конфігурації кожного пристрою та формалізує взаємодію оператора з мережею.

2. Рівень керування трафіком (Control Plane) – частина функціоналу пристрою, що дозволяє йому контролювати стан мережі, реагувати на зміни її стану та надавати пристрою інформацію про те, як перенаправляти трафік у даний момент часу. Цей рівень являє собою набір протоколів взаємодії із сусідніми пристроями мережі для обміну маршрутною інформацією, побудови топології мережі, побудови шляхів для трафіку, інформування про несправність сусіднього пристрою або лінка. Наприклад, протоколи OSPF, IS-IS, EIGRP, BGP, LDP, RSVP, BFD.

3. Рівень передачі даних (Data Plane) – частина функціоналу пристрою, відповідальна безпосередньо за передачу даних.

Як правило, робота на даному рівні є аналіз заголовків пакетів, зміна даних заголовків при необхідності, а також перенаправлення даних пакетів. Цей функціонал традиційно забезпечувався вузькоспеціалізованими мікросхемами ASIC (Application Specific Integrated Circuit), втім, що втрачають актуальність, або, що актуально на сьогодні, – мережевими процесорами (Network Processor) – гнучко програмованими пристроями для продуктивної обробки пакетів.

Концепція розподіленого управління, за якої вся інтелектуальна складова роботи мережі була розподілена по мережному обладнанню, стала недостатньо ефективною. Саме цими причинами було зумовлено появу нової

концепції та технології SDN (Software-defined Networking) – програмно-визначувана мережа [56].

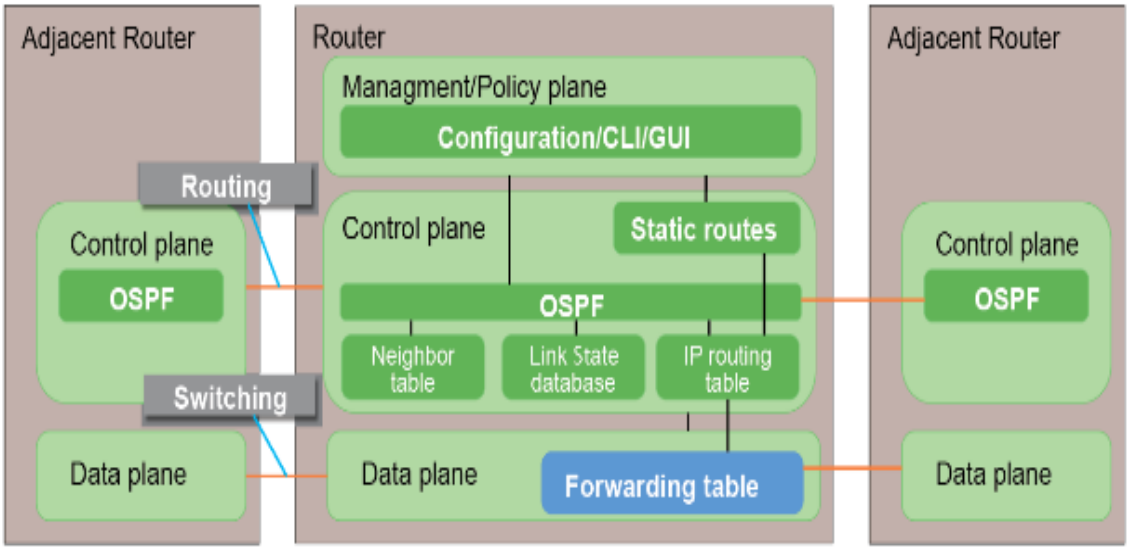



Рис. 3.41. Рівні мережевих пристроїв

SDN – це мережа, де рівень управління відокремлений від рівня передачі і реалізований програмно [57]. Таким чином, вся логіка управління мережею, відповідно до концепції SDN, має бути вилучена з мережевих пристроїв та реалізована на окремому сервері – SDN-контролері.

Мережеві пристрої повинні обмежитися функціоналом Data Plane та спеціальним програмним інтерфейсом, що дозволяє SDN-контролеру керувати роботою їх Data Plane [58]. Функціонал конфігурування та візуалізації також виноситься на окремий рівень (Application Layer) та може бути реалізований за межами SDN-контролера (рис.3.42).

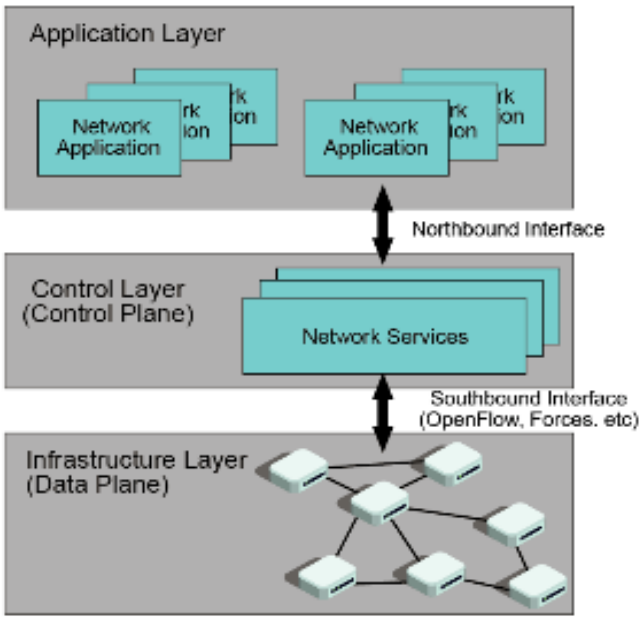



Рис. 3.42. Рівні SDN-мережі

Взаємодія SDN-контролера з мережевими пристроями відбувається через його інтерфейс, що традиційно зветься Southbound Interface (південний інтерфейс). З різними програмами контролер взаємодіє через так званий Northbound Interface (північний інтерфейс).

В результаті описаних вище нововведень замовник отримує функціонально просте та дешеве мережеве обладнання, на ринку зростає кількість вендорів, відсутність необхідності розбиратися в особливостях роботи конкретного обладнання полегшує програмування мережевого функціоналу, прив'язаного до контролера. Найбільш поширеним протоколом взаємодії мережевих пристроїв з контролером (Southbound Interface) є протокол OpenFlow [59]. Пристрої, що використовують протокол OpenFlow, маркуються відповідним логотипом (рис.3.43). Крім OpenFlow, використовуються також протоколи: Network Configuration Protocol (NETCONF), Open vSwitch Database Management Protocol (OVSDB) .


Рис. 3.43. Логотип OpenFlow

Взаємодія контролера з додатками ( Northbound Interface ) здійснюється за допомогою RESTful API.REST (RE presentational State Transfer – передача стану уявлення) – це архітектурний стиль взаємодії компонентів розподіленої програми у мережі. Даному стилю можуть відповідати і HTTP запити. У тілі таких HTTP-запитів можна використовувати такі формати представлення даних, як JSON чи XML. До веб-сервісу, що відповідає REST, застосовується термін RESTfull. RESTfull API дозволяють розробникам створювати програми для керування мережею без необхідності вивчення роботи конкретних мережевих пристроїв.

Зміна вектора розвитку мережевих технологій змушує всіх учасників IT-ринку звернути увагу на технологію SDN, яка є привабливою для замовників. Саме тому організація Open Network Foundation (ONF) об'єднала безліч виробників SDN на базі протоколу OpenFlow, що, безумовно, зміцнило його позиції та перспективи [60].

### 3.3.2. SDN-технологія від Cisco Systems

Компанія Cisco Systems – світовий лідер у галузі мережевих технологій, також не залишила поза увагою SDN-технологію. Cisco створила власний аналог OpenFlow під назвою OpFlex [61]. Компанія розраховує з часом перетворити OpFlex на галузевий стандарт. Тим не менш, сьогодні компанія

Cisco в контексті SDN представляє рішення, які концептуально відрізняються від SDN , але схожі на нього зовні.

Подібність полягає у можливості централізованого управління мережами та великої гнучкості. Відмінність – у невідповідності даних рішень основному принципу SDN, який полягає у розподілі control-plane с data-plane. У своїх рішеннях, таких як ACI, SD-Access, Cisco зберігає на мережевих пристроях значний control-plane функціонал, розширивши його деякими додатковими можливостями [62]. Основою даних технологій є overlay-мережі – логічна топологія, яка використовується для віртуального з'єднання пристроїв, побудована поверх довільної фізичної (underlay) топології (рис.3.44).

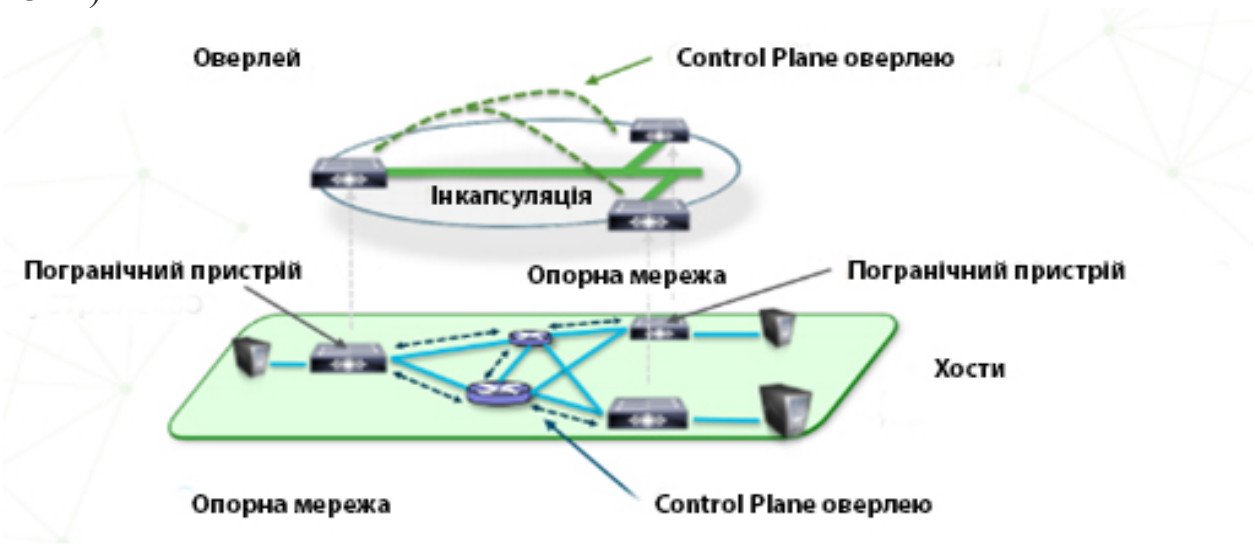



Рис. 3. 44. Опорна мережа (overlay) та віртуальна мережа (underlay)

Поверх фізичної інфраструктури будуються тунелі (наприклад, VXLAN, LISP), що є основою для бажаної логічної топології, яка може докорінно відрізнятися від топології опорної мережі [63]. У технології активно використовуються такі інструменти, як OSPF або IS-IS, VXLAN, LISP, VRF, Cisco TrustSec [64]. Інкапсуляція для VXLAN усередині SD-ACCESS представлена на рис. 3.45.

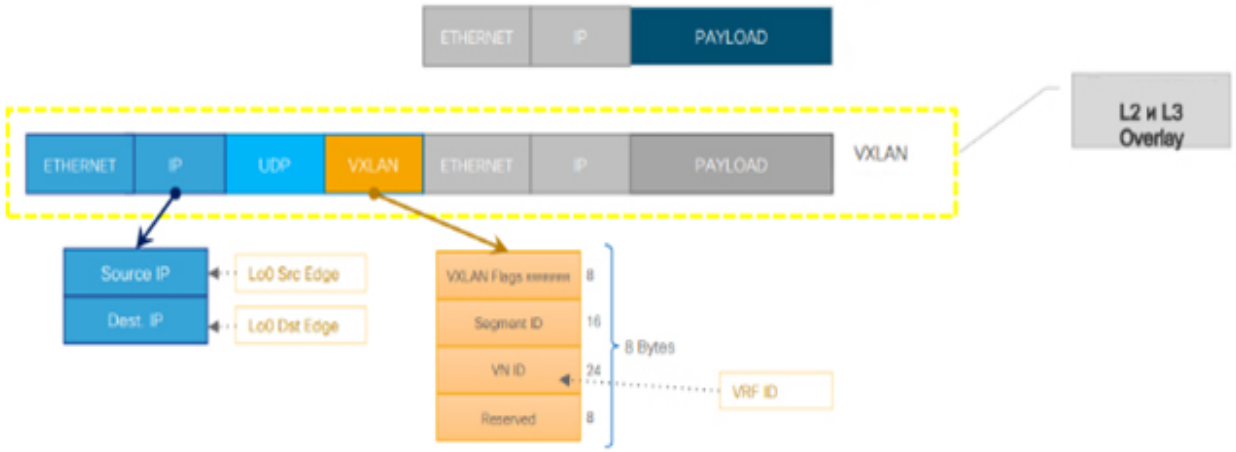



Рис. 3.45. Інкапсуляція для VXLAN усередині SD ACCESS фабрики

Одним з базових інструментів, застосовуваних SD-Access, є Cisco TrustSec (CTS) [65]. Крім того, CTS виділяється в окрему площину управління – Policy-Plane. Policy-Plane на основі TrustSec дає можливість гнучко налаштовувати обмеження доступу до мережі, легко застосовуючи їх на межі мережі, у тому числі на рівні доступу (рис.3.46). З'являється можливість застосовувати профіль користувачів, застосовуючи до них спеціальні групи доступу. Приналежність користувача до групи доступу визначається в процесі аутентифікації. Далі всьому вхідному трафіку користувача призначається спеціальний тег-SGT (Security Group Tag), що дозволяє не враховувати IP-адреси під час управління доступом [66].

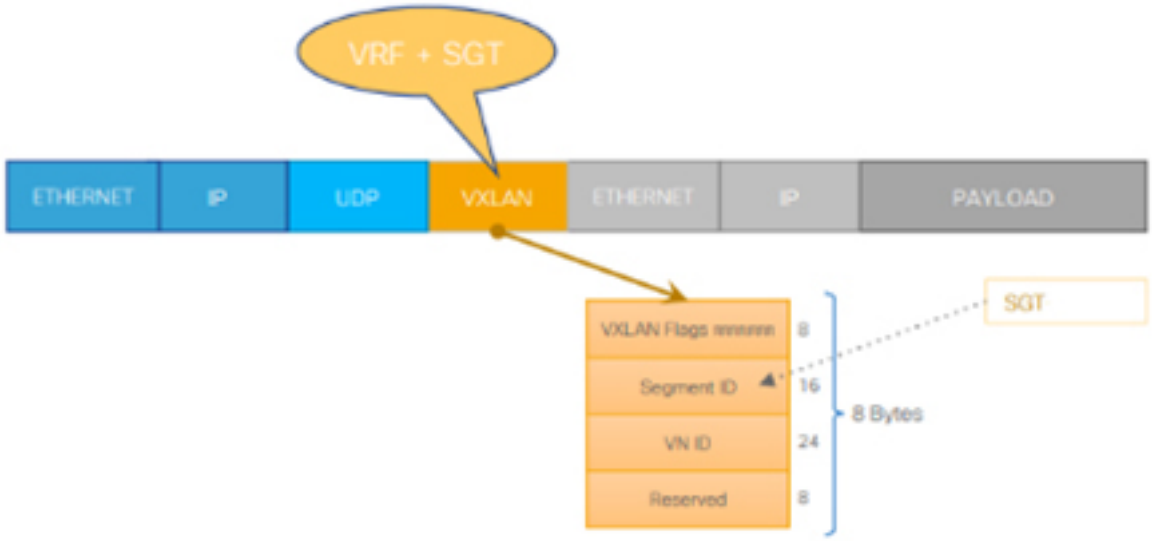



Рис. 3.46. Розміщення VN ID і SGT всередині VXLAN -заголовка

Технологія в принципі знімає обмеження, що накладаються на IP-адресацію. Крім зручного управління доступом, це означає так само, що завдяки overlay адресація відтепер не прив'язується до фізичного розташування пристроїв і їх логічного групування (як, наприклад, приналежність до загального VLAN), завдяки чому користувачі стають мобільними.

Опорна мережа є єдиною мережевою фабрикою, побудованою відповідно до Leaf-and-Spine архітектурою [67]. Набір компонентів мережі зі своїми коротким описом представлений на рис. 3.47.

Як видно зі схеми, у складі мережі присутні також компоненти управління та моніторингу, такі як DNA Center, ISE [68]. Це основні точки взаємодії адміністратора з мережею, що полегшують централізоване управління та візуалізацію, що дозволяють уникнути деталей фізичної інфраструктури та скоротити роботи зі конфігурування мережі.


Рис. 3.47. Компоненти SD-Access

SD-Access успішно працює з бездротовими мережами (рис.3.48).

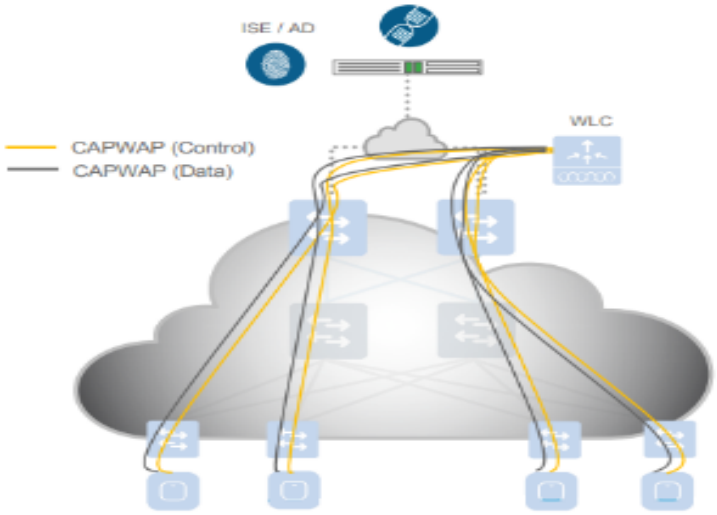



Рис. 3.48. Wi-Fi та SD-Access (Local mode)

Як завжди, точки доступу (AP) використовують WLC і можуть працювати у складі SD-Access-мережі як у традиційному local mode, так і fabric mode, що дає низку концептуальних переваг [69].

AP у Fabric Mode-режимі на рівні control-plane взаємодіє з WLC , однак як Data Plane використовується VXLAN , який встановлюється між AP і Fabric Edge-пристроєм (рис. 3.49).

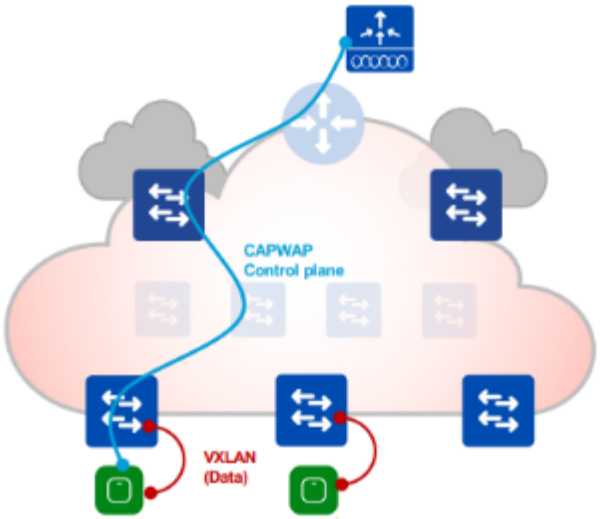



Рис. 3.49. Wi-Fi та SD-Access (Fabric mode)

Необхідною вимогою є безпосереднє підключення точки доступу до комутатора фабрики. Контролер WLC також має підтримувати цей режим роботи. Режим fabric mode дозволяє:

- трафіку клієнта оптимально використовувати ресурси мережі в обхід WLC ;
- прозоро використовувати SGT завдяки VXLAN інкапсуляції (рис.3.50);
- прозоро використовувати Virtual Networks (VNs) завдяки VXLAN інкапсуляції (рис.3.51).

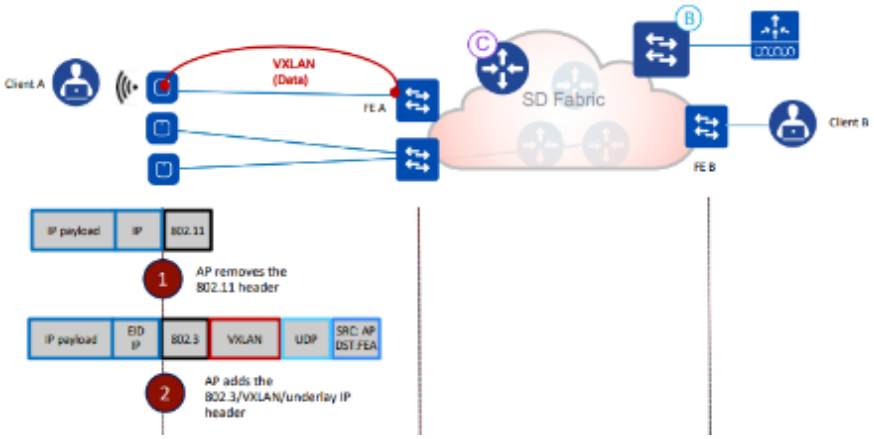



Рис. 3.50. Інкапсуляція у режимі fabric mode

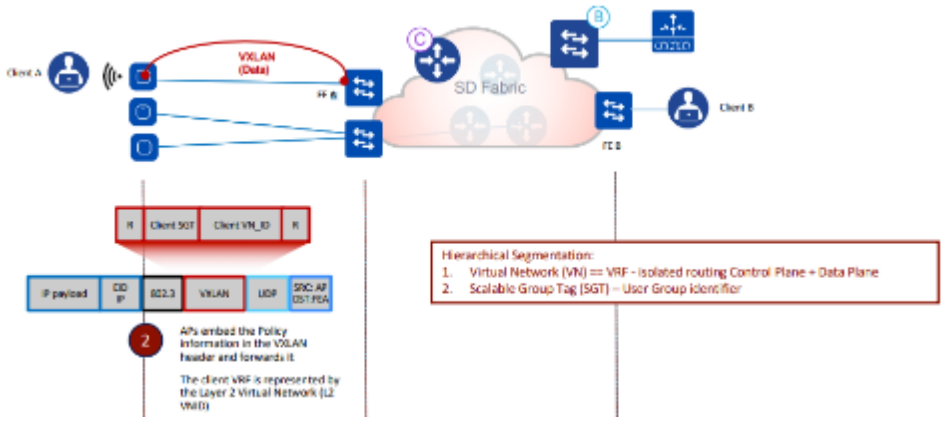



Рис. 3.51. Додавання SGT та VN ID у заголовок VXLAN в режимі fabric

### 3.3.3. Технологія SD-WAN від Cisco Systems

Традиційні глобальні мережі перестали задовольняти досить велику кількість сучасних вимог, серед яких: простота розгортання та адміністрування, легка масштабованість, гнучкість конфігурації, мобільність клієнтів, висока пропускна здатність, надійні засоби захисту інформації, забезпечення якості роботи додатків. Нові запити до дизайну та функціоналу WAN сформували подальший план роботи основних розробників мережевих технологій.

Новим рішенням від Cisco в області WAN є технологія SD-WAN. Слід зазначити, що Cisco SD-WAN базується на розробках поглиненої Cisco компанії Viptela. SD-WAN є результатом застосування SDN-концепції до розподілених мереж [70]. Середовище передачі SD-WAN – це оверлей, працюючий через Internet. Розробники SD-WAN виділяють у цій технології чотири основні переваги: забезпечення гнучкої експлуатації, гнучкої та безпечної зв'язності, якості роботи додатків та підтримка хмарних середовищ.

Як і властиво SDN-технологіям, в SD-WAN , на відміну від SD-Access, дотримано поділ Control Plane та Data Plane з винесенням функціоналу Control P lane на окремі спеціалізовані пристрої. Крім того, над Control Plane додано надбудову у вигляді «Плоскості Адміністрації та Оркестрації», що дозволяє централізовано з мінімальними оперативними витратами адмініструвати мережу.

vBond реалізує функціонал оркестрації фабрики, забезпечує зв'язність між площинами адміністрування, управління та передачі даних, є допоміжною ланкою для обходу NAT. vBond є початковою точкою автентифікації, передає список vSmart, vManage пристроїв на всі vEdge-пристрої. Вимагає публічного IP-адреси та високої відмовостійкості.

vManage – площина адміністрування. Забезпечує єдину консоль управління, централізований провіжинінг, формування політик та шаблонів,

моніторинг та траблшутинг, оновлення ПЗ, програмний інтерфейс (REST, NETCONF). Компоненти технології SD-WAN представлені на рис.3.52.


Рис. 3.52. Компоненти технології SD-WAN

vSMART – площина керування. Забезпечує виявлення пристроїв у фабриці, розповсюджує Control Plane інформацію на всі vEdge-пристрої, що розповсюджує політики Data Plane та політики маршрутизації за додатками на всі vEdge-пристрої та застосовує політики Control Plane (рис.3.53).

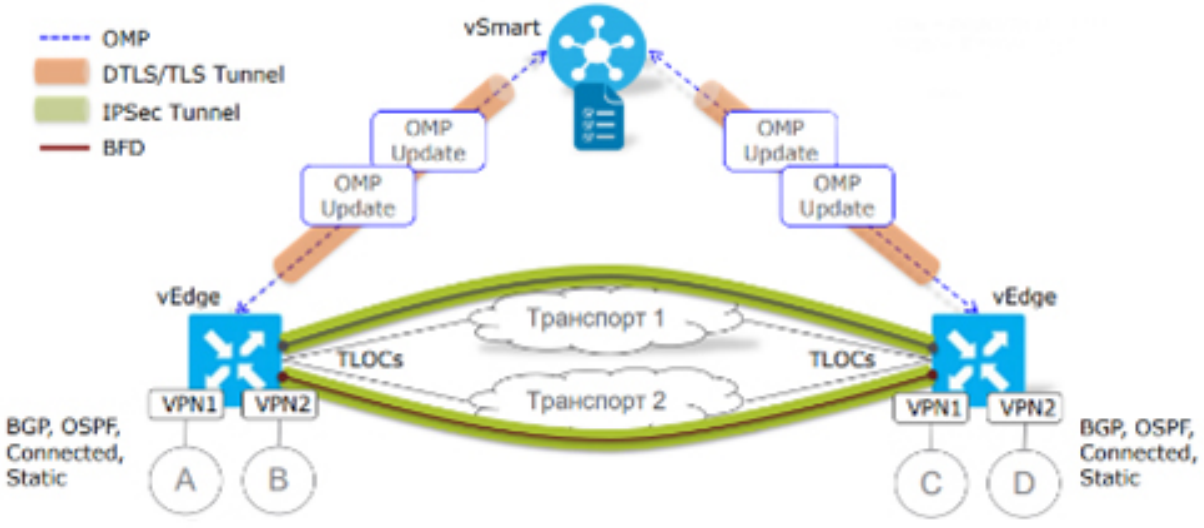



Рис. 3.53. Взаємодія Control Plane та Data Plane у Cisco SD-WAN

vEdge – Data Plane. Граничні маршрутизатори WAN. Забезпечують безпечну передачу даних з віддаленими vEdge-маршрутизаторами, а також маршрутизацію на основі політик за додатками. Підтримує в повному обсязі стандартні протоколи маршрутизації, такі як OSPF, BGP, та FHRP, такі як VRRP, із зовнішнім світом. Здійснює безпечні керуючі з'єднання (Overlay

Management Protocol – OMP) з vSMART – контролерами [71]. Підтримує Zero Touch Provisioning ( ZTP ) [72]. Експортує статистику щодо продуктивності. Пристрої vEdge можуть бути як фізичні (100 Mbps ÷ 20+ Gbps), так і віртуальними. Контролери vBond, vManage, vSMART можуть бути розгорнуті, як у корпоративній мережі ( ESXi, KVM), так і в публічній хмарі (Azure, Amazone Web Service (AWS )). vSmart- контролер взаємодіє з vEdge за протоколом OMP. Протокол функціонує всередині Transport Layer Security (TLS)/DTLS-з'єднань, що забезпечує йому безпеку. Усередині оверлейної мережі працює BFD, що значно підвищує збіжність мережі. На відміну від iWAN, SD-WAN-інфраструктура може підтримувати одночасно безліч незалежних VPN-мереж, тобто є Multi-tenant архітектурою (рис.3.54). Кожна VPN може мати свою власну логічну топологію.

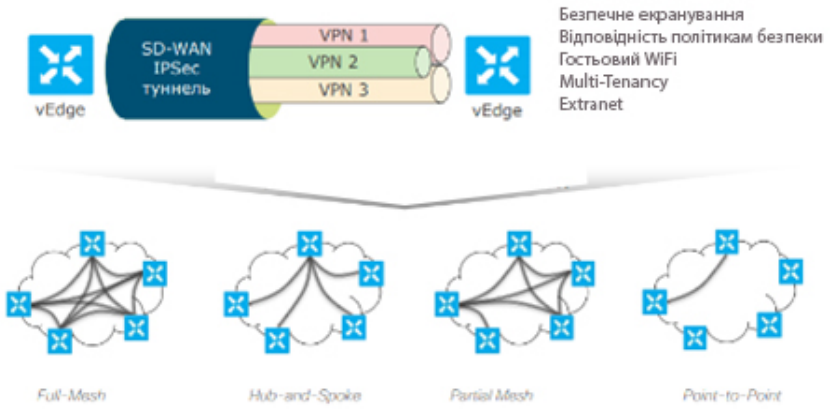



Рис. 3.54. Multi-tenant-можливості Cisco SD-WAN

### 3.3.4. Об'єднання нових технологій та Digital Network Архітектура

Тотальне проникнення IT в область процесів функцінування організацій підвело розробників мережевих технологій до чергового перегляду та трансформації ідеології enterprise-мереж. Трансформація відбувалася відразу за кількома напрямками:

- віртуалізація мережевих функцій (Network Functions Virtualisation – NFV);
- використання SDN-рішень;
- автоматизація процесів керування;
- аналітика;
- безпека;
- використання хмарних послуг.

В результаті такої трансформації мережа перетворювалася на уніфіковану гнучку і орієнтовану на роботу додатків високонадійну інфраструктуру з функціоналом, що легко перебудовується і розширюється, єдиним центром управління, єдиними політиками безпеки, можливістю швидкого і детального аналізу процесів, що відбуваються в ній, а також низькими оперативними

витратами. Як результат зміни ідеології побудови enterprise-мереж, продиктованої ринком, компанія Cisco представила нову концепцію побудови мереж-DNA (Digital Network Architecture) (рис.3.55).


Рис. 3.55. Концепція DNA

Функціонал NFV перейшов у enterprise-сегмент з операторських мереж, дозволивши рівноцінно замінити безліч окремих мережевих пристроїв різного призначення віртуальними сутностями всередині обмеженого набору фізичних пристроїв-хостів з можливістю майже миттєвого розгортання, клонування та переконфігурування (рис.3.56).


Рис. 3.56. Network Functions Virtualization

Віртуальні версії вже існують для більшості апаратних рішень Cisco . Наприклад: Cisco CSR 1000 v (програмний аналог Cisco ASR 1000), Cisco ASAv (програмний аналог Cisco ASA) і т. д. Для хостингу VNF можуть бути

використані безпосередньо мережеві пристрої. Наприклад, у деяких випадках це можуть бути пристрої серії Cisco Catalyst 3650/3850, Cisco ISR 4000, Cisco ASR 1000. Рішення Cisco Enterprise NFV покликане забезпечити весь життєвий цикл віртуалізованої інфраструктури дистанційного офісу підприємства. Управління організоване через відкриті програмні інтерфейси Netconf API, RESTconf API.

Одним із невід'ємних інструментів взаємодії з мережевою інфраструктурою є засоби автоматизації. Ці інструменти власними силами не нові, оскільки й колишній підхід до роботи мереж припускав наявність NMS (Network Management System). Однак сучасний погляд на автоматизацію передбачає набагато тіснішу інтеграцію засобів управління та автоматизації в мережеву інфраструктуру для забезпечення повноти управління. У великих складових мережах складно досягти єдиного підходу до автоматизації і, тим більше, реалізації цього підходу можливостями єдиного інструментарію, а DNA дозволяє без особливих труднощів реалізувати цей підхід.

Інструментом автоматизації, запропонованим Cisco, є продукт Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM). Cisco APIC-EM – це перший комерційний SDN-контролер Cisco для корпоративної кампусної, розподіленої дротової та бездротової мереж, що дозволяє взяти під керування всі домени корпоративної мережі (рис.3.57).


Рис. 3.57. Застосування узгоджених політик у межах складової мережі

Однією із завдань управління мережею, не вирішуваної інструментами автоматизації, є завдання контролю якості послуг. Для вирішення цього завдання служить набір програмних засобів аналітики, що зветься DNA Аналітика. Програми аналітики отримують телеметрію з пристроїв мережної інфраструктури з можливістю її подальшого аналізу в реальному часі, наприклад, вивчення тенденцій, порівняння станів, оцінки відповідності послуг критеріям якості. Прикладами засобів аналітики є продукти Cisco Tetration Analytics та Cisco Connected Mobile Experience (CMX).

Cisco Tetration Analytics – це найновіша платформа від Cisco для реалізації аналітики програм та користувачів у рамках ЦОД.

Cisco CMX – технологія для аналізу бездротових мереж, що дозволяє будувати звіти про місцезнаходження бездротових клієнтів, будувати профілі їхньої поведінки у мережі.

Безпека мережі повинна бути обов'язково забезпечена спеціальним набором інструментів. Яскравим прикладом таких інструментів є такі продукти: Cisco ISE – рішення для контролю доступу до корпоративної мережі, що включає сервіси аутентифікації, авторизації та обліку (AAA), оцінки стану, профілювання, Cisco Stealthwatch – рішення для моніторингу та аналізу безпеки мережі, засноване на зборі телеметрії із мережевих пристроїв (рис.3.58).

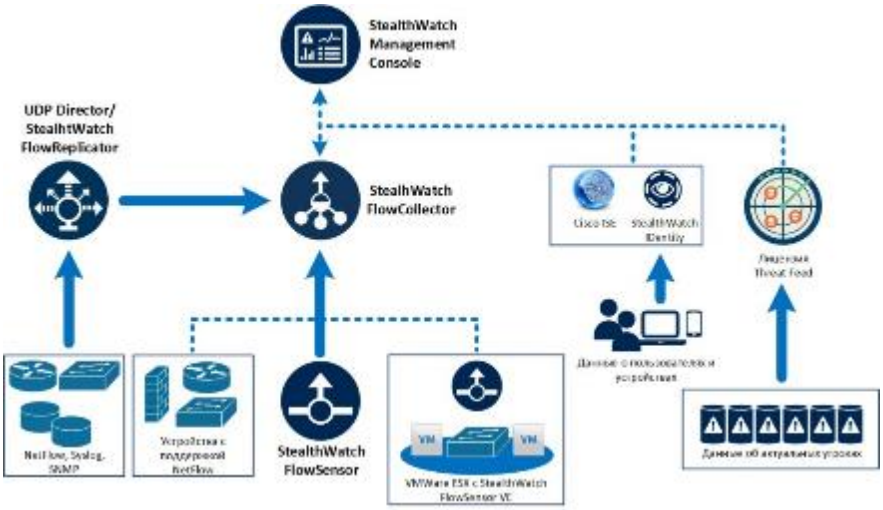



Рис. 3.58. Взаємодія Cisco Stealthwatch з інфраструктурою

Рішення Cisco ISE і Cisco Stealthwatch пред'являють особливі вимоги до мережного обладнання, що перебувають у його можливості працювати, з одного боку, як засіб контролю (Network-as-Enforcer) і як сенсор (Network-as-a-Sensor) – з іншого.

Ще одним інструментом, що активно використовується сьогодні, є хмарні сервіси. Cisco DNA пропонує низку рішень на основі хмарних технологій, які дозволяють замовникам отримувати сервіси з хмари Cisco або надавати подібні послуги самостійно на базі власних датацентрів. Одним із прикладів таких рішень є Cisco CMX Cloud – хмарний варіант реалізації інструментів аналітики CMX.

Таким чином, корпоративна мережа пройшла довгий еволюційний шлях розвитку від незручного співіснування розрізнених технологій до побудови сучасної уніфікованої інтелектуальної мережевої інфраструктури з високою безпекою та легким управлінням, що, безумовно, втілює концепція DNA, запропонована Cisco.

# РОЗДІЛ 4
# ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНІ ІНФРАСТРУКТУРИ

IT-інфраструктура – це комплексна структура, що об'єднує всі інформаційні технології та ресурси, що використовуються конкретною організацією або підприємством [73]. IT-інфраструктура включає всі комп'ютери, сервери, СЗД, ЦОДи, мережі, системи та канали зв'язку, що використовується ПЗ та БД.

Головне завдання IT-інфраструктури – забезпечення стабільного доступу до відповідних інформаційних та технічних ресурсів організації чи підприємства для певного кола користувачів. Тому необхідно забезпечити повну відповідність IT-інфраструктури потребам конкретної організації чи підприємства. Основною перевагою правильно збудованої IT-інфраструктури є оптимізація витрат підприємства на її утримання та експлуатацію, а також підвищення продуктивності за рахунок використання IT-сервісів.

## 4.1. Еволюція та особливості IT-інфраструктур

Говорячи про еволюцію та розвиток IT-інфраструктур, можна виділити такі етапи (рис.4.1):

- використання традиційних IT-інфраструктур;
- конвергентні системи, які комбінують два або більше інфраструктурних компонентів, як попередньо інтегроване рішення;
- поширення гіперконвергентних інтегрованих систем, що є програмно-визначуваною технологією, в якій всі компоненти інтегровані.

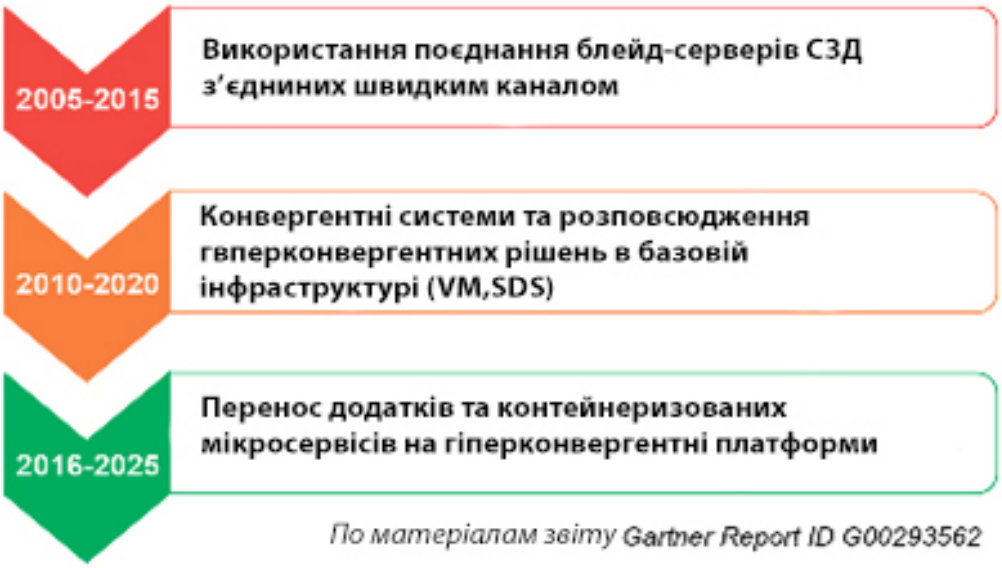



Рис. 4.1. Еволюція IT-інфраструктур

Останні кілька років стрімкими темпами розвиваються гіперконвергентні інфраструктури. Поява гіперконвергентних інфраструктур є закономірним етапом розвитку IT-інфраструктур та наступним логічним кроком від конвергентних [74]. Концепція конвергентних інфраструктур передбачає комбінування кількох інфраструктурних компонентів у попередньо інтегрований комплекс з допомогою сполучного ПЗ. Ця концепція, своєю чергою, є розвитком традиційних підходів до побудови IT-інфраструктури.

Термін «конвергентна інфраструктура» було запропоновано компанією Hewlett-Packard. У термінології Gartner цей тип інфраструктури називається інтегрованою системою, а Cisco Systems – системою уніфікованих обчислень (Cisco Unified Computing System – UCS). Але незалежно від назви в них закладена та сама ідеологія: об'єднання пам'яті, обчислювальних та мережевих ресурсів у загальний пул, попередньо налаштований для роботи в ЦОД. Такий підхід дозволяє скоротити час на розгортання інфраструктури від кількох місяців до кількох днів.

Гіперконвергентні інфраструктури розвивають концепцію конвергентних структур, додаючи до неї поняття модульності, завдяки цьому всі необхідні віртуалізовані обчислювальні ресурси, мережні та СЗД працюють автономно всередині окремих модулів, які є готовими віртуалізованими обчислювальними ресурсами. Вони зазвичай об'єднуються в групи, щоб забезпечити стійкість до відмов, високу продуктивність і гнучкість у створенні ресурсних пулів.

### 4.2. Гіперконвергентні інфраструктури

Гіперконвергентна інфраструктура почала завойовувати ринок з 2014 р., та її ключову відмінність у поєднанні всієї обчислювальної функціональності в єдине інтегроване високовіртуалізоване рішення, що базується на серверах. За 2–3 роки найбільші виробники IT-обладнання створили свої лінійки гіперконвергентних систем, у тому числі спільно з іншими виробниками програмно-апаратних платформ.

Згідно з даними компанії IDC, на гіперконвергентні інфраструктури в 2014 р. припадало 10,9% ринку конвергентних інфраструктур, а до 2020 р. їхня частка зросла до 32% і досягнула 4 млрд дол., а за оцінками Gartner, ринок гіперконвергентних інтегрованих систем щорічно збільшувався на 68% – з 371,5 млн дол. у 2014 р. до 5 млрд у 2020-го. Таким чином, інтерес до гіперконвергентних інфраструктур продовжує стрімко зростати, про що свідчать обсяги продажу та їх динаміка.

Одна з причин затребуваності гіперконвергентних інфраструктур полягає в тому, що не всі організації та підприємства для зниження витрат на побудову власної IT-інфраструктури готові перевести свої сервіси та додатки в публічну хмару, в першу чергу, через жорстку залежність від компанії – провайдера послуг, необхідність зберігання конфіденційної інформації не на своїх ресурсах та неможливості повного контролю безпеки даних, хоча

багато хто з них зацікавлений у реалізації переваг хмарних технологій у власній інфраструктурі, і гіперконвергентні інфраструктури дають можливість це зробити. Вони є альтернативою оренди хмарних сервісів у сторонніх компаній – провайдерів послуг, оскільки за допомогою гіперконвергентних інфраструктур стало можливим розгортання своїх приватних хмар, якими повністю розпоряджаються організації та підприємства [75].

Під терміном « гіперконвергентна інфраструктура» (Hyper-Converged Infrastructure – HCI) розуміється програмно-визначувана IT-інфраструктура, яка включає такі обов'язкові компоненти, як гіпервизор обчислювальної віртуалізації, програмно-визначені сховище даних і мережа.

Hyper (visor) + Convergence = Hyperconvergence. Ця формула дозволяє зрозуміти, чим гіперконвергентні інфраструктури відрізняються від конвергентних інфраструктур, що просто об'єднують в одній коробці кілька окремих інфраструктурних компонентів, пов'язаних між собою традиційними мережами (SAN, LAN). Масштабування ресурсних пулів таких компонентів здійснювалося незалежно від інших, а конвергенція обмежувалася застосуванням транспортного протоколу FCoE (Fibre Channel over Ethernet) та єдиною консоллю управління [76].

Термін «гіперконвергенція» передбачає об'єднання в одній з інфраструктурних компонентів кількох різних технологічних шарів ЦОД ще на стадії його створення. Використання гіперконвергентних структур дозволяє більше не розділяти технологічні шари ЦОД на окремі пули ресурсів (обчислення, зберігання), оскільки вони спочатку вбудовані за допомогою гіпервізора в кожен уніфікований елемент, з яких створюється нова інфраструктура. Розвиваючи функціональність гіпервізорів, вдалося подолати обмеження, пов'язані з доступом до даних на локальних носіях окремих серверів та відмовитися від класичної SAN-мережі, замінивши її на віртуальну. Аналогічно справи і з мережею передачі даних, яка емулюється програмними комутаторами, маршрутизаторами і може бути повністю віртуалізована. Уніфікація та простота вузлів, горизонтальне масштабування та балансування навантажень через швидкий інтерконнект, програмна визначальність більшості інфраструктурних компонентів та управління ними за допомогою єдиної системи – це основні особливості сучасних гіперконвергентних інфраструктур.

Сьогодні дуже актуальними є завдання зниження операційних витрат та скорочення часу, необхідного на розгортання ЦОД. Використання традиційних та конвергентних інфраструктур, що мають на увазі наявність виділених СЗД, не завжди є оптимальним підходом для вирішення вищезгаданих завдань. Так, навесні 2016 р. компанія Cisco Systems поповнила свою лінійку рішень для ЦОД продуктами абсолютно нового класу – гіперконвергентною інфраструктурою Cisco HyperFlex (рис.4.2) .

Cisco HyperFlex є системою гіперконвергенції, яка комбінує в собі інноваційне ПЗ для зберігання даних і ПЗ Cisco UCS, і являє собою надійну

систему, яка об'єднує сервери і мережі в одне ціле. Cisco HyperFlex розширює переваги Cisco UCS, додаючи до них ефективність платформи HX Data Platform. Остання поєднує твердотільні та дискові накопичувачі кластера в єдине розподілене багаторівневе об'єктне сховище даних, в основі якого лежить файлова система, що дозволяє записувати та зчитувати дані з усіх вузлів системи паралельно.

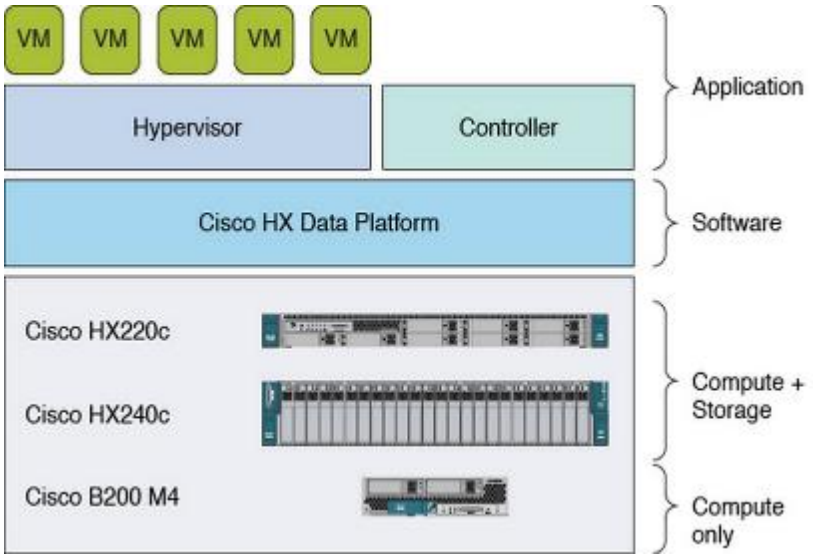



Рис. 4.2. Cisco HyperFlex

Платформа забезпечує високу доступність за допомогою паралельного розподілу та реплікації даних, а також високу швидкість завдяки низькій затримці та великій смузі пропускання Cisco Unified Fabric. Процеси дедуплікації та компресії, що постійно функціонують, в реальному часі виконують безперервну оптимізацію даних, що допомагає мінімізувати вартість зберігання без погіршення продуктивності. Динамічний розподіл даних у пам'яті сервера, кешування та наявність різних рівнів зберігання максимізують надмірність та продуктивність додатків. Всі ці функції допомагають підвищити продуктивність без збільшення складності. Лінійка HyperFlex-ідеальна платформа як для розгортання корпоративних додатків у головних ЦОДах, так і для віддалених офісів та філій.

Компанії Hewlett Packard Enterprise (HPE) і Pure Storage також приступили до випуску гіперконвергованих систем. HPE представила призначену для середніх підприємств платформу Hyper Converged 380, яка поєднує обчислення та зберігання. Pure Storage пішла ще далі, випустивши платформу FlashBlade, що поєднує обчислення, зберігання та мережі. Перехід до гіперконвергентності та програмно-визначувана інфраструктура (Software-Defined Infrastructure – SDI) стимулюють появу спілок виробників. Так, наприклад, Juniper Networks і Lenovo співпрацюють у розробці технологій SDI, які можуть застосовуватись у ряді сценаріїв використання гіперконвергентності.

Таким чином, істотною відмінністю гіперконвергентних інфраструктур є те, що в конвергентній інфраструктурі кожен компонент у будівельному блоці є дискретним і може використовуватися окремо, а гіперконвергентна інфраструктура є програмно-визначеною технологією, в якій інтегровані всі компоненти. Також гіперконвергентні інфраструктури відрізняються покращеннями на рівні програмного контролера, що дає можливість їх легкого масштабування. Для збільшення ємності та продуктивності необхідне лише додавання нового блоку. Замість збільшення потужності за рахунок збільшення числа дисків, кількості пам'яті або процесорів продуктивність збільшується за рахунок додавання більшого числа модулів. Відповідно, гіперконвергентна інфраструктура – це інфраструктура, в якій обчислювальні потужності, СЗД, сервери, мережі об'єднуються в одне ціле за допомогою програмних засобів, а керування ними відбувається через загальну консоль адміністрування, що дає можливість замість групи IT-фахівців для управління СЗД та серверним обладнанням, задіяти лише одного системного адміністратора.

Крім того, гіперконвергентні інфраструктури є альтернативою оренди хмарних сервісів у компаній – провайдерів послуг, оскільки з їх допомогою стало можливим розгортання власних приватних хмар, якими повністю розпоряджаються організації та підприємства. Саме ця можливість – одна із причин затребуваності гіперконвергентних структур як великими, так і невеликими підприємствами та організаціями. Тому на сьогоднішній день гіперконвергентна інфраструктура стала домінантною апаратною платформою для розміщення приватних хмар, віртуальних робочих місць та середовищ розробки нових додатків.

### 4.3 . Гіперконвергентна технологія з відкритим кодом

У середині 2017 р. компанія Red Hat, лідер у галузі розробки відкритого ПЗ, представила першу гіперконвергентну інфраструктуру з відкритим кодом, поповнивши свій набір для підприємств інтегрованою платформою для обчислень та зберігання даних – Red Hat Hyperconverged Infrastructure (RHHI) [77].

#### 4.3.1. Технологія RHHI

Технологія RHHI об'єднала у собі:

- Red Hat Virtualization – платформа віртуалізації на основі технології KVM;
- Red Hat Gluster Storage – масштабована програмна система зберігання на основі GlusterFS, яка може бути встановлена безпосередньо на хості RHV, без виділення окремого сервера, що суттєво спрощує її розгортання;

- Red Hat Enterprise Linux – корпоративна Linux-платформа, яка виступає як надійна і перевірена основа, де як гостьові ОС підтримуються як ОС RHEL 5, 6 і 7, так і SUSE Linux Enterprise Server 10,11,12, а також Microsoft Windows, включаючи нові версії 8, 10, 2008, 2008 (R2, 2012, 2016);
- Ansible – систему централізованого автоматизованого розгортання та керування конфігураціями без використання програмних агентів (одноіменна компанія-розробник була придбана Red Hat у 2015 р.).

Також у RHHI вбудована функція інтеграції з Red Hat Cloud Forms для управління та оркестрації IT-інфраструктури. На сьогоднішній день це єдина технологія корпоративного рівня, у складі якого є весь інфраструктурний стек ЦОД з повністю відкритим кодом. А використання компанією Red Hat лише власних програмно-визначуваних компонентів для побудови гіперконвергентної інфраструктури значно спрощує її супроводження та підтримку.

### 4.3.2. Особливості застосування технології RHHI

Технологія RHHI орієнтована на віддалені офіси та/або філії (Remote Office/Branch Office, ROBO), оскільки дозволяє реалізувати практично весь функціонал ЦОД, що представляється на базі традиційної IT-інфраструктури, та розміщуватись у місцях з обмеженими ресурсами (рис.4.3).


Рис. 4.3. Гіперконвергентна інфраструктура компанії Red Hat

Якщо проаналізувати потреби корпоративних інфраструктур з розвиненою мережею філій, особливо фінансового та телекомунікаційного секторів економіки, то можна зробити висновок, що таким організаціям у філіях необхідні ті ж інфраструктурні сервіси, що і в центральному офісі, а це

вимагає розгортання бізнес-критичних додатків на локальних серверах та СЗД у філіях.

При цьому основна проблема полягає в тому, що технології, що використовуються у корпоративному ЦОД, не підходять для віддалених офісів. Крім того, у віддалених офісах, як правило, немає можливості розмістити технологічний ЦОД та забезпечити наявність кваліфікованих IT-фахівців. У таких випадках необхідні інші технології, які давали б можливість реалізувати інфраструктурні сервіси за допомогою невеликої кількості серверів, але разом з тим забезпечували необхідний рівень стійкості до відмов, керованість і простоту масштабування в міру зростання потреб у ресурсах.

RHHI інтегрує СЗД та обчислювальний вузол на одному сервері, що відповідає обмеженням для віддалених майданчиків. Завдяки централізованому розгортанню та управлінню вдалося автоматизувати складні операції розгортання та з'явилася можливість використовувати високопродуктивні системи у віддалених філіях, не маючи кваліфікованих IT-фахівців на місцях. Основним варіантом для використання такого підходу стає широка мережа філій, де кожен віддалений офіс регулярно синхронізує дані з основним ЦОД, але при цьому не вимагає підключення до нього для своєї роботи.

Досить ймовірно, що в найближчій перспективі сферою застосування технологій на базі RHHI стануть і такі напрямки, що активно розвиваються, як Граничні обчислення (Mobile edge computing) та Інтернет речей (Internet of Things) [78,79].

Граничні обчислення – тенденція, що набирає популярності, пов'язана з прагненням телекомунікаційних операторів до перенесення обчислювальних ресурсів, зазвичай розміщених у великих ЦОД, в локальні офіси або на віддалені майданчики, що дозволяє більш рівномірно розподіляти навантаження, підвищуючи тим самим продуктивність мережі в цілому. Друга сфера застосування пов'язана з особливостями деяких архітектурних рішень IoT, коли поблизу кінцевих точок потрібно розгортання невеликих обчислювальних ресурсів у форматі мікроЦОД.

### 4.3.3 . Архітектура та технічні характеристики технології RHHI

Для тестування нової технології було розгорнуто стенд на базі RHHI, який дозволив дослідити функціональні можливості технології у тестовій лабораторії. На рис.4.4 представлена архітектура стенду з одиночним кластером (POD), розгорнутим на трьох фізичних серверах з використанням компонентів Red Hat Gluster Storage 3.2 та Red Hat Virtualization 4.1.

Весь процес розгортання хостів автоматизований з використанням Red Hat Virtualization Host (RHVH) – спеціально розробленої ОС на базі Red Hat Enterprise Linux для забезпечення простого настроювання фізичної машини як гіпервізор. Вона містить лише необхідні пакети для роботи сервера як

гіпервізор у середовищі віртуалізації Red Hat Virtualization і має інтерфейс Cockpit для моніторингу хоста і виконання завдань адміністрування.

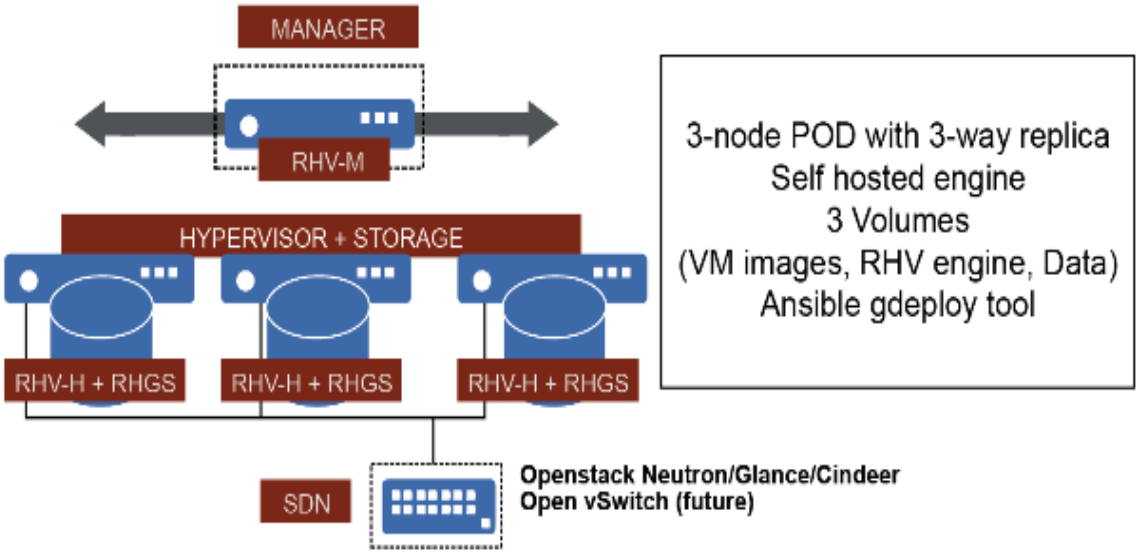



Рис. 4.4. Архітектура стенду з одиночним кластером

При розгортанні та конфігуруванні використовується вбудований портал адміністратора, а для користувачів передбачений вбудований user-портал самообслуговування. Установка передбачає такі кроки:

1) розгортання необхідної кількості RHEV Node;

2) налаштування мережі;

3) налаштування GlusterFS та підключення сховища з готового образу OVA;

4) запуск RHEV-Virtualization Manager; підключення RHEV Node до RHEV Virtualization Manager;

5) налаштування ЦОД і подальше розгортання ВМ.

Всі операції, починаючи від створення ЦОД, кластера, додавання хоста або домену зберігання і закінчуючи операціями з підготовки шаблонів, побудовані у вигляді послідовних закладок в графічному інтерфейсі і максимально автоматизовані за допомогою вбудованих візардів, а також користувально-орієнтовані.

Мінімальні вимоги для побудови кластера RHHI – три фізичні сервери з двома мережевими інтерфейсами на кожному. Також рекомендується забезпечити 10 GbE для потреб мережі зберігання Gluster та перенесення трафіку між вузлами (Back- end Network) та окремий інтерфейс (у цьому випадку можливе використання 1GbE) для створення віртуального мосту підсистеми управління ovirt (Front-end Network). Кожен із цих інтерфейсів необхідно дублювати при побудові стійких до відмови конфігурацій. Крім конфігурації лабораторного стенду, підтримується ще дві: 6-і 9-вузлові кластери, розраховані на застосування в більш ресурсоємних інфраструктурах. Діапазони основних технічних параметрів окремого хоста для різних конфігурацій представлені у табл.4.1:

Таблиця 4.1. Діапазони основних технічних характеристик окремих хостів

| Тип конфігурації | Кількість процесорних ядер | Розмір ОЗУ | Місткість сховища |
|---|---|---|---|
| Мінімальна | Не менше 12 cores | Не менше 64 GB | Не більше 48 ТВ |
| Середня | Не менше 12 cores | Не менше 128 GB | Не більше 64 ТВ |
| Велика | Не менше 1 6 cores | Не менше 256 GB | Не більше 80 ТБ |

Параметри самих ВМ варіюються в межах: не більше 4 virtual CPUs і трохи більше 2 ТВ віртуального дискового простору. Для забезпечення відмовостійкості ресурсів зберігання застосовується триразова реплікація блоків даних Red Hat Gluster Storage, а для доступності ресурсів управління – RHVM необхідно налаштувати в режимі High Availability (HA).

Важливою функціональною особливістю, що дозволяє технології RHHI забезпечувати необхідний рівень катастрофостійкості для більшості корпоративних інфраструктур, є можливість кластерної файлової системи Red Hat Gluster Storage підтримувати геореплікацію на рівні тому. Налаштовуючи геореплікацію при побудові disaster Recovery рішення, необхідно враховувати такі обмеження для RHHI версії 1.0:

- RHHI підтримує лише один геореплікований том;
- джерела та кінцеві томи для геореплікації повинні керуватися різними RHVM.

Такі технології, як Secure Virtualization (sVirt) та Security-Enhanced Linux® (SELinux) захищають гіпервізор від атак, спрямованих на хост або на ВМ. RH VM також підтримує мережне шифрування з використанням TLS та SSL (Secure Sockets Layer) для автентифікації та авторизації на рівні віртуалізації та зберігання. Референсна модель архітектури гіперконвергентної інфраструктури Red Hat із застосуванням кількох рівнів зберігання, спрямованих як на підтримку інтенсивного введення-виведення, так і забезпечення великої ємності СЗД, показана на рис.4.5.

Гіперконвергентні технології переводять концепцію конвергентності на якісно новий рівень. Істотною відмінністю між двома технологіями є те, що у конвергентній інфраструктурі кожен компонент у будівельному блоці є дискретним і може використовуватися окремо. Що стосується гіперконвергентної інфраструктури, то це програмно-визначувана технологія, в якій усі компоненти інтегровані. Також гіперконвергентні технології відрізняються покращеннями на рівні програмного контролера, що дає можливість їх легкого масштабування. Для збільшення ємності та продуктивності необхідне лише додавання нового блоку. Замість збільшення потужності за рахунок збільшення числа дисків, кількості пам'яті або

процесорів продуктивність збільшується за рахунок додавання більшого числа модулів.

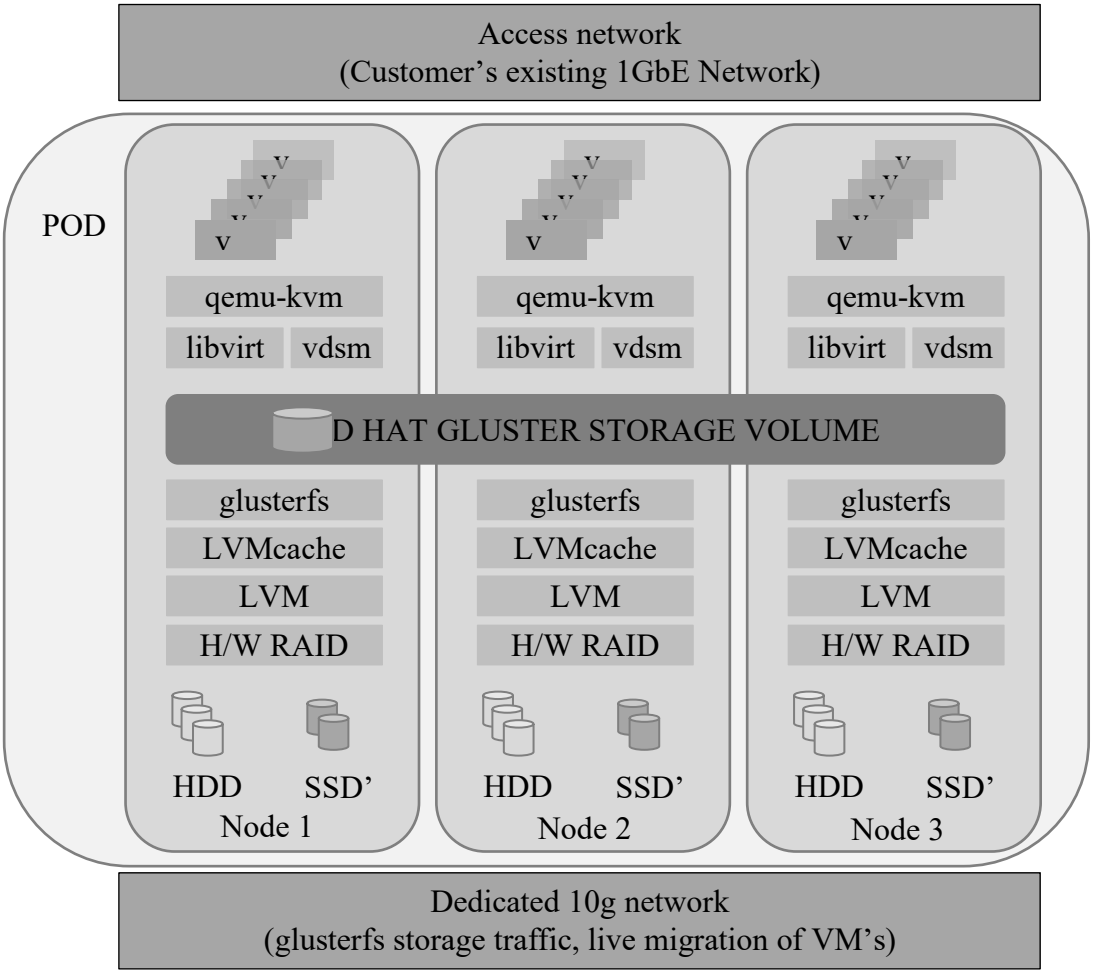



Рис. 4.5. Референсна модель архітектури гіперконвергентної інфраструктури

Відповідно, гіперконвергентна інфраструктура – це інфраструктура, в якій обчислювальні потужності, СЗД, сервери, мережі об'єднуються в одне ціле за допомогою програмних засобів, а керування ними відбувається через загальну консоль адміністрування, що дає можливість замість групи IT-фахівців для управління СЗД та серверним обладнанням задіяти лише одного системного адміністратора.

На сьогоднішній день гіперконвергентна інфраструктура стала домінантною апаратною платформою для розміщення приватних хмар, віртуальних робочих місць та середовищ розробки нових додатків. До представлених раніше на нашому ринку HCI-технологій від традиційних виробників інфраструктурних компонентів, таких як HC 380 HCI від компанії HPE, VxPail HCI від компанії Dell EMC, HyperFlex HX від компанії Cisco, які працюють на базі гіпервізора vSphere ESXi від VMware, додалася технологія RHHI. Унікальність цієї технології полягає в тому, що повністю відкритий код не тільки виключає прив'язку до конкретного виробника, але й дозволяє

підтримувати високий рівень інновацій, використовуючи переваги та новітні технології від спільноти розробників з відкритим кодом. Проведені дослідження показали, що технологію RHHI можна використовувати не тільки для віддалених офісів та філій, але і для вирішення завдань з певним типом навантажень в основних ЦОД підприємств та організацій.

Аналіз існуючих на сьогоднішній день IT-інфраструктур ЦОД дозволяє зробити висновок, що, використовуючи сучасні багатоядерні серверні вузли у поєднанні з високопродуктивною дисковою підсистемою з великою ємністю, можливо побудувати інфраструктуру на базі технології RHHI, яка здатна задовольнити потреби в ресурсах не тільки віддалених офісів, а й основних ЦОД підприємств корпоративного рівня.

Горизонтальна масштабованість такої інфраструктури здійснюється шляхом простого додавання набору однотипних серверів, що полегшує процеси планування потужностей. А підтримка всього інфраструктурного стеку ЦОД, починаючи від віртуальних обчислювальних ресурсів і ресурсів віртуального сховища від його виробника, істотно спрощує взаємодію IT-персоналу підприємства зі службою техпідтримки. Також у порівнянні з традиційним підходом до побудови інфраструктури, для всіх можливих варіантів застосування, RHHI дозволяє суттєво знизити капітальні витрати, операційні витрати та час на розгортання інфраструктури. Це досягається завдяки використанню однієї й тієї ж одиниці серверного обладнання як для гіпервізора віртуалізації, так і для контролера підсистеми зберігання.

Таким чином, технологія RHHI може бути рекомендована для застосування у всіх організаціях та підприємствах, які хочуть побудувати гнучку інфраструктуру хмарного рівня, не використовуючи для цього публічних ресурсів, а розміщуючи обладнання у власних ЦОД.

### 4.4. Віртуалізація: динаміка розвитку та перспективи

В останні роки все більшої популярності набувають технології віртуалізації [80]. Нині вони стають одним із ключових компонентів сучасної IT-інфраструктури великих підприємств та організацій. І це невипадково. Зростають обчислювальні потужності комп'ютерів, зростає пропускна спроможність їх інтерфейсів, а також ємність та чуйність СЗД. В результаті, маючи такі потужності на одному фізичному сервері, можна перенести у віртуальне середовище всі сервери, що функціонують в організації. Це можна зробити за допомогою сучасних технологій віртуалізації.

Наразі вже складно уявити побудову серверного вузла організації без використання технології віртуалізації. Визначальні чинники такої популярності – економія грошей та часу, а також високий рівень безпеки та забезпечення безперервності бізнес-процесів. Якщо подивитися на зріз останніх кількох років, то розвиток технологій віртуалізації в Україні відбувався так [81].

2009 рік – здебільшого чітке розмежування окремих напрямків: віртуалізація настільних систем, серверів та додатків, СЗД. Замовники:

корпоративний сектор. Досягнуто промисловий рівень відмовостійкості віртуальних платформ, який можна порівняти з рівнем мейнфреймів .

2010 рік – змішання напрямків попереднього року до різних «міксів». Напрями залишалися приблизно тими самими. Відбувся перелом у питанні можливості перекладу «важких» систем (СУБД Oracle, MS SQL, IBM DB2) та серверів додатків у віртуальне середовище. До корпоративних замовників додався сектор малого бізнесу.

2011 рік – кордони між окремими напрямками практично стираються, а віртуалізація у всіх виробників йде шляхом комплексних рішень для настільних систем, малого та середнього бізнесу, ЦОДів та хмарних обчислень. Незважаючи на те, що фінансові переваги хмарних обчислень очевидні, глобальної міграції до хмар не відбувається. Основна причина – неготовність компаній довірити основу свого бізнесу чи менеджмент IT-інфраструктури стороннім організаціям. Приватні хмарні середовища, контрольовані самою компанією, поки що більш правдоподібні щодо їхньої якнайшвидшої появи. Хоча гібридна модель з публічною/приватною хмарою може виявитися ще більш цікавою та ефективною.

2012 рік – продовження переходу компаній на віртуальну IT-інфраструктуру (особливо середній бізнес), оптимізація витрат на її утримання шляхом реалізації окремих проектів із хмарними рішеннями та продовження конкуренції між виробниками на тлі відсутності домінуючого лідера.

На сьогоднішній день основні гравці за величиною частки ринку в питанні віртуалізації x86 потужностей розташовані в наступному порядку (рис.4.6): VMware, Microsoft, Citrix Systems, Oracle, Parallels і Red Hat. Найближчим часом нових гравців не додасться, і розстановка сил буде приблизно такою самою.

Слід зазначити ще дві можливі тенденції: найближчим часом ринок виробників серверів почне поступово стискатися; серйозні зміни виникнуть над ринком ОС і ПО. Цілком імовірно, що в так звану епоху проникаючої віртуалізації головної ОС цілком може стати гіпервізор (а тут ще й виникнення додаткових питань безпеки у зв'язку з появою нового об'єкта атак – власне гіпервізора). Внаслідок того, що основною технологією побудови великих та малих інформаційно-обчислювальних платформ дуже швидко стає середовище віртуалізації, основним виробникам ОС та СУБД доведеться це враховувати.

Компанія Veeam Software запропонувала безкоштовний сервіс (V-INDEX) для відстеження ступеня віртуалізації по всьому світу (http://www.v-index.com). Цей індекс визначається щокварталу і відображає ступінь впровадження технологій віртуалізації в різних країнах світу, а також перешкоди на шляху віртуалізації та відсоток використання різних гіпервізорів. Він може бути корисним для прояснення актуальної картини того, які технології більш потрібні в даний момент і тим самим допомогти зробити більш обґрунтований вибір для впровадження.


Рис. 4.6. «Магічний квадрант» для серверної ( x86) віртуалізації

## 4.5. Технології віртуалізації від Oracle

Історично компанія Oracle асоціюється з БД, але сьогодні Oracle, крім БД, має у своєму арсеналі сервери, дискові підсистеми, стрічкові бібліотеки, інженерні системи, Java та технології віртуалізації [82].

Подивившись на магічний квадрант для серверної (x86) віртуалізації від Gartner за 2016 р., видно, що лідерами були VMware і Microsoft, а Oracle – нішевий гравець. Однак, якщо в організації вже використовуються будь-які програмні продукти або обладнання компанії Oracle, то застосування технологій віртуалізації Oracle найчастіше технічно виправдане та економічно доцільне, оскільки в цьому випадку віртуалізація від Oracle становить певні переваги. По-перше, віртуалізація дозволяє ефективно завантажити процесорні ресурси, які стають дедалі потужнішими і складаються з дедалі більшої кількості ядер і потоків. Зазначимо, що на CPU Oracle можна досягти максимального ефекту, тому що і сам CPU, і технологія віртуалізації розробляються однією компанією. По-друге, віртуалізація від Oracle дає можливість економити на ліцензіях ПЗ, оскільки дозволяє знижувати витрати за рахунок зменшення кількості ядер, що ліцензуються.

На сьогоднішній день у компанії Oracle існують три основні типи віртуалізації для серверів:

1) Oracle VM for x86 (Oracle VM) – віртуалізація для серверів x86. Можна використовувати на серверах Noname.Xen-гіпервізор;

2) Oracle VM for SPARC (LDOM) – віртуалізація для Oracle SPARC-серверів (T-серія). Гіпервізор виступає домен з Solaris 11;

3) Dynamic Domains (HW domains ) – віртуалізація для Oracle SPARC-серверів рівня High-End (M-серія). Гіпервізора немає, віртуалізація лише на рівні апаратної частини.

Розглянемо детальніше кожен із цих типів віртуалізації.

### 4.5.1. Oracle VM for x86

Віртуалізація Oracle VM for X86 побудована на базі гіпервізора Xen (рис.4.7).

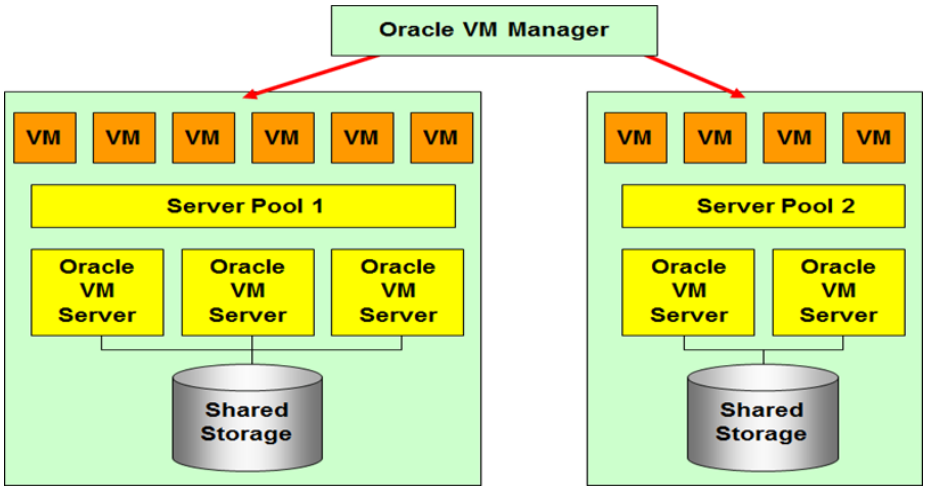



Рис. 4.7. Віртуалізація Oracle VM for x86

Як Oracle VM Server може виступати практично будь-який сервер із процесорами архітектури x86. На кожному фізичному сервері встановлюється прошарок Xen-гіпервізора. Далі всі ці сервери об'єднуються в серверні пули, де відбувається конфігурування ВМ . ВМ може мати до 256 virtual CPUs і 2 ТВ ОЗУ, можливе встановлення наступних ОС: Oracle Linux, Oracle Solaris, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS, Microsoft Windows. Можлива конфігурація із забезпеченням високої доступності (high availability): автоматичний перезапуск VM, що відмовили, на інших серверах серверного пулу.

### 4.5.2. Oracle VM for SPARC

Конфігурування ВМ походить з Oracle VM Manager. Цей тип віртуалізації може застосовуватися в оточенні OpenStack. В останніх релізах свого флагманського продукту Oracle Exadata вже застосовує цей тип віртуалізації для створення Exadata Virtual Machines, що говорить про зрілість продукту.

Віртуалізація Oracle VM for x86 надається безкоштовно (zero license cost), і кожен бажаючий може використовувати її у своїх рішеннях. У разі критичного бізнес-програми можна оформити підтримку цієї віртуалізації від виробника за додаткову плату. Oracle надає безліч готових Oracle VM Templates для швидкого розгортання потрібного програмного продукту.

Даний тип віртуалізації можна порекомендувати власникам серверів x86, які хочуть заощадити на купівлі дорогого ПЗ для віртуалізації від інших вендорів. Для SPARC-серверів застосовується віртуалізація Oracle VM for SPARC (раніше називалася Logical Domains). SPARC (Scalable Processor ARChitecture) – це RISC процесор від компанії Sun Microsystems, купленої Oracle у 2010 р.

Oracle VM for SPARC використовує вбудований гіпервізор для поділу ресурсів сервера (процесора, пам'яті, мережі та дискової підсистеми) шляхом розподілу на логічні домени (Logical Domains – LDOM). На одному SPARC-сервері, застосовуючи цю віртуалізацію, можна створити до 128 віртуальних серверів. Для швидкого розгортання віртуальних серверів можна використовувати готові шаблони (Oracle VM Server for SPARC templates ) в форматі OVF. Сервери цього класу відрізняються великою продуктивністю та надійністю. Так, наприклад, сервер Oracle SPARC T5-8 має 4 ТВ ОЗУ та 1024 потоки, які можна розділити і віддати під різні логічні домени. У цьому типі віртуалізації Control Domain виступає у ролі гіпервізора. У ньому встановлена ОС Solaris 11 і з його допомогою здійснюється вся необхідна конфігурація. Маючи два і більше сервери з віртуалізацією Oracle VM for SPARC, можна виконувати онлайн міграцію гостьових доменів (Guest domains) з сервера на сервер. Такий тип міграції називається Live Migration .

Суть даної міграції полягає в тому, що можна переносити робочі гостьові домени з одного сервера на інший без припинення додатків всередині доменів. Тобто завжди можна мінімізувати простий критичних програм, виконавши Live Migration на інші сервери. На рис.4.8 показано, як можна мігрувати гостьовий домен на резервний сервер.

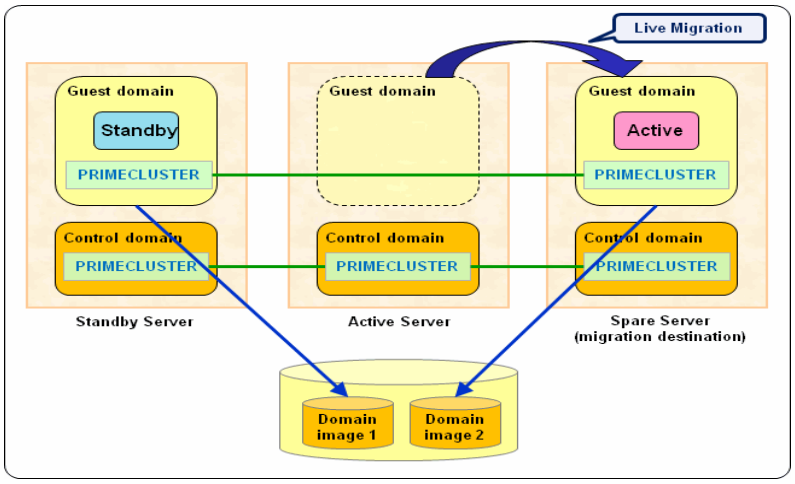



Рис. 4.8. Віртуалізація Oracle VM for SPARC

Застосування віртуалізації Oracle VM for SPARC можна порекомендувати для критичних програм, яким необхідно мінімізувати простий та забезпечити можливість онлайн-міграції.

### 4.5.3. Dynamic Domain

Для серверів класу Mid-range, High- end у Oracle застосовується окрема віртуалізація – це динамічні домени (Dynamic Domain). Прошарок гіпервізора при даному типі віртуалізації немає. Через системний контролер сервера створюються динамічні домени, незалежні друг від друга лише на рівні заліза. можливо застосування динамічної реконфігурації ресурсів сервера Dynamic Reconfiguration (DARE), що дозволяє виконувати онлайн-додавання або вилучення ресурсів з діючого домену, що додає гнучкості та мінімізує простої. Даний тип віртуалізації є найнадійнішим і застосовується для висококритичних завдань, простий яких призводить до значних фінансових втрат. При ідеальному варіанті час безперервної роботи (uptime) динамічного домену дорівнює терміну служби сервера і, зазвичай, обчислюється роками. Ремонти, додавання нових ресурсів – все це відбуватиметься у режимі онлайн. Як приклад назвемо флагманський продукт Oracle SuperCluster M8, що застосовує динамічні домени. Dynamic Domain буде цікава для тих, кому необхідно уникати простою навіть за кілька хвилин і забезпечувати фізичне додавання ресурсів (CPU, ОЗУ, I/O) онлайн.

### 4.5.4. Solaris Zone

Крім трьох основних типів віртуалізації, слід зазначити віртуалізацію лише на рівні ОС Solaris Zone. Усередині ОС створюються зони, які є віртуалізованими ОС. Процесори, пам'ять, дискове місце розподіляються між зонами.

Цей тип віртуалізації дуже зручний і може використовуватися як самостійно, так і накладатися на інші типи віртуалізації, коли це необхідно. Іншими словами, ОС Solaris із створеними в ній Solaris Zone можна розгортати як фізично (апаратної частини), так і всередині одного з трьох вище наведених типів віртуалізації.

Останнім часом все частіше починають практикувати багатошарову віртуалізацію, коли один тип віртуалізації накладається зверху іншого. Іноді це дійсно дуже зручно для безлічі застарілих систем на один новий сервер. Так, всередині гостьових доменів, створених з використанням Oracle VM for SPARC або Oracle VM for x86, можна виділити декілька Solaris Zones. У Solaris Zones можуть працювати різні версії ОС Solaris (рис. 4.9).

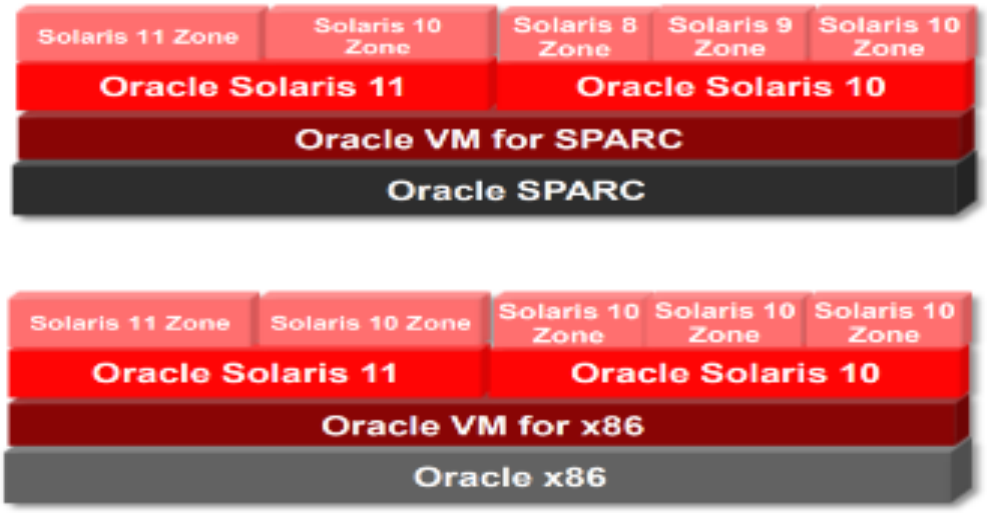



Рис. 4.9. Вкладена віртуалізація Oracle VM + Solaris Zones

Приклад застосування вкладеної віртуалізації представлено на рис. 4.10.

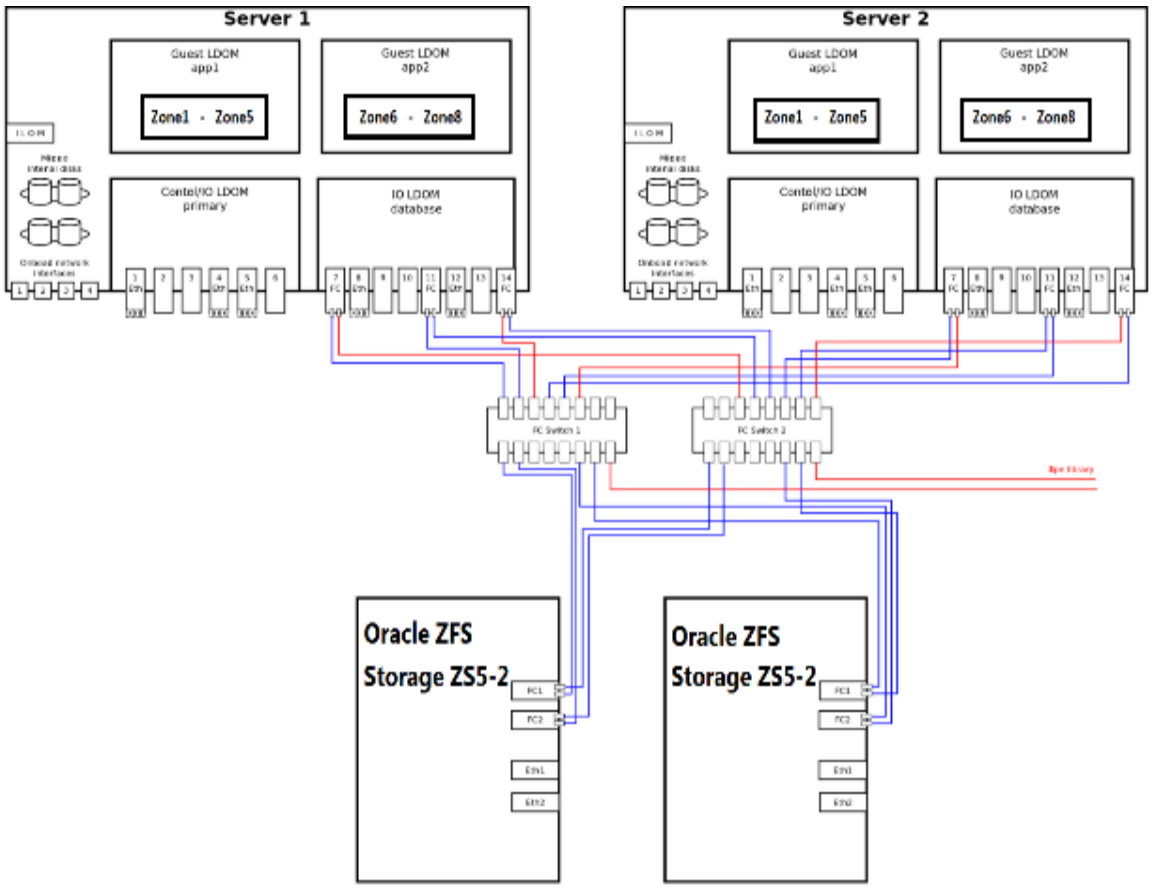



Рис. 4.10. Приклад віртуалізації Oracle VM for SPARC + Solaris Zones

На двох SPARC-серверах створено по два гостьові домени з використанням технології Oracle VM for SPARC. Один сервер працює в

активному режимі (Active), а другий знаходиться в режимі Standby. Сервери підключені до масивів Oracle ZFS Storage ZS5-2 через оптичні комутатори. Всередині кожного гостьового домену створені Solaris Zones , усередині яких працюють програми (SAP ERP, SAP CRM, Oracle DB, Cisco Info Center). Конфігурація всіх доменів здійснюється з Control Domain, в якому встановлений Oracle Solaris 11. Весь введення-виведення реалізується через IO Domain, який може бути суміщений з Control Domain. Зазвичай для критичних завдань створюють два IO Domain, щоб забезпечити максимальну надійність вводу-виводу. За необхідності програми можуть бути переключені з Active на Standby з мінімальним даунтаймом. За аналогічною схемою можна звести безліч систем однією сервер з віртулізацією, що найчастіше буває економічно доцільно.

Хмари від Oracle також активно використовують розглянуті у статті типи віртуалізації. Зокрема, Oracle IaaS Cloud є наступним стіком: мережа – дискова підсистема – сервери – віртуалізація – ОС. Весь стек реалізований на устаткуванні та програмних продуктах від Oracle. Стабільні та перевірені роками рішення щодо віртуалізації дозволяють реалізувати якісний Oracle Cloud, що призводить до зростання його популярності, у тому числі й у нашій країні.

Продукти Oracle для віртуалізації серверів підтримують архітектури x86 та SPARC та різні види ОС, такі як Oracle Linux, Windows та Oracle Solaris. Крім рішень на основі гіпервізора, Oracle пропонує віртуалізацію, вбудовану в апаратне забезпечення та ОС Oracle. Застосування серверів, БД та віртуалізації від Oracle дозволяє побудувати надійне віртуальне середовище для бізнес-критичних програм та отримати підтримку від одного виробника, що дозволяє зменшити витрати та отримати максимальний ефект у результаті синергії.

Нині вже складно уявити інформаційні технології без віртуалізації. Розвиток інформаційних систем підприємств та організацій тісно пов'язаний із їх застосуванням. Впровадження технологій віртуалізації дозволяє значно скоротити витрати, пов'язані з придбанням та підтримкою серверних систем, скоротити час на відновлення інформації або розгортання аналогічних систем у новому устаткуванні. Крім того, дає можливість скорочення серверного парку, штату IT-співробітників, клонування ВМ, а також спрощує їхнє обслуговування.

Якщо в будь-якій організації ще не використовуються переваги віртуалізації, варто про це задуматися вже сьогодні. І навіть якщо парк організації налічує лише кілька серверів, то перейти до впровадження описаних вище технологій доцільно.

# РОЗДІЛ 5
# ХМАРНІ ТЕХНОЛОГІЇ

В останні роки в усьому світі швидкими темпами розвиваються хмарні технології або, як їх ще називають, – хмарні обчислення. Це модель надання повсюдного та зручного мережевого доступу до загального пулу конфігурованих обчислювальних ресурсів (мереж передачі даних, серверів, СЗД, додатків та сервісів), які можуть бути оперативно надані та звільнені з мінімальними зусиллями з управління та необхідності взаємодії з провайдером.

Існує чотири основні моделі розгортання хмарних технологій: приватна хмара; публічна хмара; громадська хмара та гібридна хмара.

Приватна хмара (від англ. private cloud) це обчислювальні ресурси, розгорнуті для використання в рамках однієї організації з кількома споживачами (структурні підрозділи, віддалені офіси тощо). Також можливий варіант використання цих ресурсів замовниками та підрядниками цієї організації. Фізично приватна хмара може перебувати як у, так і поза юрисдикцією власника, і може обслуговуватися та керуватися або власником або перебувати під зовнішнім керуванням.

Публічна хмара (від англ. cloud) це обчислювальні ресурси, розгорнуті для вільного використання широкими масами користувачів. Громадською хмарою можуть і управляти, як комерційні, і державні, чи наукові організації. Перебувають вони у юрисдикції власника, який надає відповідні хмарні послуги.

Громадська хмара (від англ. community cloud) це обчислювальні ресурси, розгорнуті задоволення потреб конкретного співтовариства користувачів з організацій, пов'язаних спільними завданнями, цілями тощо. Громадська хмара може спільно владнатися, управлятися, експлуатуватися однією і більше організацією спільноти або третьою стороною; фізичне існування суспільної хмари можливе як у, так і поза юрисдикцією власника.

Гібридна хмара (від англ. Hybrid cloud) є комбінацією з двох або більше різних хмарних інфраструктур (приватних, публічних або громадських). З точки зору експлуатації та володіння вони залишаються унікальними об'єктами, однак між ними існує зв'язок за допомогою стандартизованих або пропрієтарних технологій передачі даних та додатків.

Також є кілька моделей обслуговування хмарних обчислень: з яких основними є «ПЗ як послуга» (від англ. Software-as-a-Service або SaaS), «Інфраструктура як послуга» (від англ. Infrastructure-as-a-Service або IaaS), «Платформа як послуга» (від англ. Platform-as-a-Service або PaaS).

«ПЗ як послуга» означає, що хмарний провайдер надає користувачеві ПЗ, таке як бізнес-додатки, бази даних, коди додатків у формі сервісу.

«Інфраструктура як послуга» означає, що хмарний провайдер надає лише базові елементи IT-інфраструктури, сервери, СЗД, ВМ, БД як основу для вирішення різних завдань.

«Платформа як послуга» означає, що хмарний провайдер надає користувачеві цілу платформу для використання, забезпечуючи доступність всіх базових елементів IT-інфраструктури: серверів, СЗД, ВМ і т.д., а також деяких програмних інструментів, наприклад, для розробки власного програмного забезпечення.

Різниця між трьома основними моделями обслуговування хмарних обчислень та варіантом використання власної IT-інфраструктури (on premise) представлена на рис.5.1:

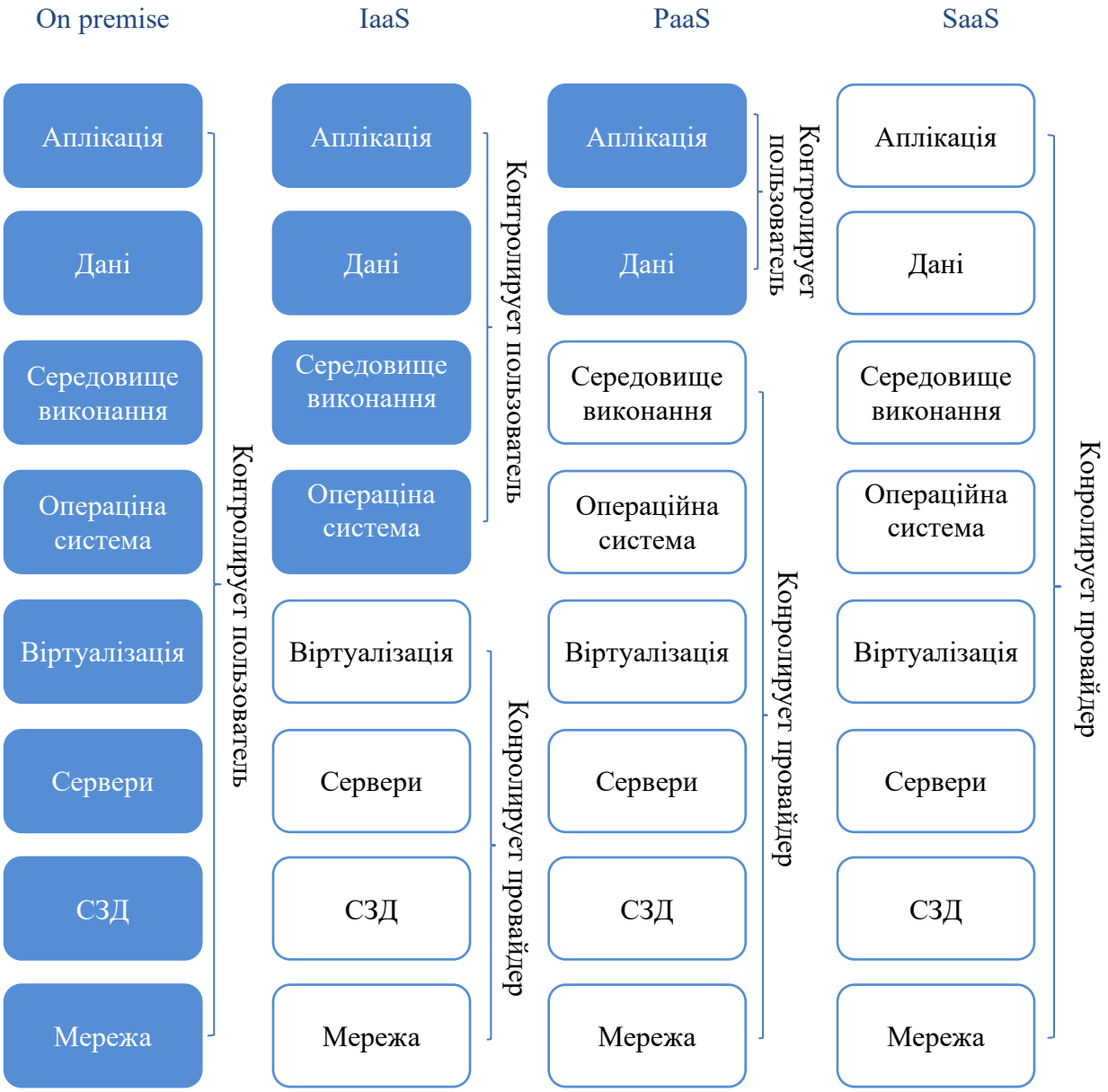



Рис. 5.1. Моделі обслуговування хмарних обчислень

Крім наведених вище хмарних послуг ще надаються такі:

«Робочий стіл як послуга» (від англ. Desktop-as-a-Service або DaaS) означає, що хмарний провайдер надає користувачеві доступ до віртуальних робочих столів, розміщених у хмарі та доступних з будь-якого місця. Ця послуга, як правило, пропонується на основі моделі передплати, і підвищує як продуктивність віддаленого доступу до ресурсів , так і безпеку даних.

«Аналітика як послуга» (від англ. Analytics-as-a-Service або AaaS). Цей різновид SaaS означає, що хмарний провайдер надає користувачеві аналітичне ПЗ за моделлю передплати.

«Бекенд як послуга» (від англ. Backend-as-a-Service або BaaS) позначає, що хмарний провідник надає, наприклад, розробнику ПЗ усі базові служби програми, такі, як управління базою даних, автентифікація користувачів, хмарне сховище, що дозволяє йому зосередитися виключно на написанні ПЗ, розробці його інтерфейсу користувача та дизайну.

«Дані як послуга» (від англ. Data-as-a-Service або DaaS ) позначає, що хмарний провайдер пропонує користувачам послугу надання попередньо агрегованих та розширених даних, для прийняття аргументованих бізнес-рішень і т.д. Хмарні технології в даному випадку використовуються для зберігання та обробки даних.

«База даних як послуга» (від англ. Database-as-a-Service або DBaaS) означає, що хмарний провайдер надає користувачеві функціональність бази даних як сервісу для внутрішніх або зовнішніх замовників, дозволяючи не покладатися на внутрішніх адміністраторів баз даних.

«Інформаційна безпека як послуга» (від англ. Security-as-a-Service або SECaaS) позначає сценарій, при якому хмарний провайдер забезпечує захист програмної або апаратної інфраструктури користувача. Найпростішим прикладом може бути антивірусне ПЗ, хмарні служби автентифікації, ідентифікації тощо.

«Уніфіковані комунікації як послуга» (від англ. Unified Communcations-as-a-Service або UCaaS) позначає сценарій, при якому хмарний провайдер забезпечує корпоративні комунікації, такі як телефонія, аудіовідеоконференцзв'язок і т.д.

Основна перевага хмарних технологій полягає в тому, що, не маючи власної інфраструктури, ОС систем та прикладного ПЗ, користувач отримує можливість доступу до своїх даних та роботи з ними. Також до переваг належать: доступність, мобільність, економічність, гнучкість, висока технологічність та надійність.

Докладніше вивчення всіх існуючих варіантів надання хмарних послуг потребує окремого та достатнього глибокого дослідження. У реальній роботі більш детально розглянуті хмарні комунікаційні сервисаы , оскільки з низки глобальних економічних, технологічних і політичних процесів, роль засобів віддаленої комунікації у вирішенні завдань різного характеру і масштабу зростає з великою швидкістю. Лавиноподібно збільшується кількість користувачів комунікаційними сервісами хмарної телефонії,

відеоконференцзв'язку, уніфікованих комунікацій та спільної роботи над проектами, що надаються за моделлю SaaS, при якій сервіс-провайдер пропонує передплатникам готове прикладне ПЗ як послугу [83].

Враховуючи затребуваність таких сервісів та досить велику конкуренцію на ринку комунікаційних послуг, компанії-виробники пропонують різні рішення, як, наприклад, об'єднання всіх комунікаційних служб в одному додатку [84].

## 5.1. Хмарні комунікаційні платформи

Хмарні та мобільні технології дають можливість доступу до таких програм з будь-якого робочого місця (веб-браузер, ноутбук, мобільний телефон та ін.). У цих програмах можна вести листування з групою людей, організовувати аудіо- та відеоконференції, робити аудіо та відеодзвінки користувачам додатків, а також на номери телефонних мереж загального користування (ТфЗК) та IP-телефонії, інтегрувати необхідні для роботи інструменти. Одна з таких програм Spark розроблена компанією Cisco – лідером серед виробників on-premise систем комунікаційних сервісів та провайдера однієї з найпопулярніших хмарних служб WebEx [85].

Cisco Spark Service – основна служба хмарної платформи, що є набором інструментів для спільної роботи. У сервісі для спілкування виділено три базові інструменти: Message для обміну повідомленнями та файлами; Meeting для проведення голосових та відеоконференцій; Call для телефонних дзвінків Реалізація та налаштування цих інструментів здійснюється через додаток Cisco Spark App та веб-портал Cloud Collaboration Management Portal (CCMP). За допомогою програми можна обмінюватися повідомленнями та ділитися файлами з можливістю попереднього перегляду як з командою, так і один з одним, створювати або приєднуватися до голосових та відеоконференцій з демонстрацією на екран, здійснювати голосові та відеодзвінки по SIP-протоколу. До кімнат через веб-портал Cisco Spark Depot можна підключати роботів і інтегрувати різні хмарні програми: ZenDesk, GitHub, Zapier та ін.

Для роботи з Cisco Spark використовується клієнт на робочому столі під керуванням Mac або Windows, веб-клієнт або мобільний клієнт для Android або iOS. Автоматизація програми можлива за допомогою служби Spark for Developers. З її допомогою Cisco Spark Service може використовуватись як REST API додаток для інтеграції розробниками у службу своїх рішень. Налаштування сервісу здійснюється за допомогою CCMP, який надає зручний інтерфейс адміністрування користувачами, службами та ліцензіями, а також звіти щодо використання служб та моніторингу сервісів. З його допомогою до сервісу можна «прив'язати» DNS компанії, налаштувати SIP URI та інтегрувати свій SingleSignOn-сервіс. На порталі можна придбати контракт на надання послуг ТфЗК у Preferred Media Partner (PMP) Cisco, після чого платформа стає хмарною АТС, з можливістю реєстрації телефонів моделей 7800 і 8800 або підключення системи для проведення конференцій

SX10. Також можна використовувати Spark Hybrid Services для інтеграції хмарного сервісу із on-premise сервісами замовника. Сервіс включає такі інструменти, як Hybrid Call, Hybrid Calendar, Hybrid Directory. При підключенні Hybrid Directory до Directory Connector на стороні клієнта можливі синхронізація списку користувачів хмарного сервісу зі списком користувачів компанії у службі каталогів Active Directory та використання SSO-служби компанії для роботи з Cisco Spark App та CCMP. Підключення Hybrid Call, Hybrid Calendar до клієнтського Cisco Expressway дозволяє використовувати календар MS Exchange із програмою Cisco Spark для планування конференцій та як програмний клієнт для Cisco Unified Communication систем.

Потрібно відзначити, що не тільки компанія Cisco активно розвиває свої хмарні комунікаційні платформи за моделлю SaaS, але і її конкуренти в цій галузі – Microsoft, Facebook, Google, оскільки з розвитком хмарних та мобільних технологій з'явилася можливість змінити традиційні механізми спілкування між людьми, об'єднати всі комунікаційні сервіси в одній хмарній службі, а також на їх базі розвивати віртуальні керовані сервіси (Virtual Managed Services, vMS) [86].

## 5.2. Хмарні технології як основа віртуальних керованих сервісів

У світі IT дедалі більше уваги приділяють новим концепціям, і з них – віртуальні керовані послуги [87]. Називаємо їх концепцією, оскільки це поняття не є новою технологією, а являє собою, швидше, новий підхід до побудови IT-інфраструктури та надання сервісів.

Слід зазначити, що підходи до представлення сервісів існували на IT-ринку до появи технологій віртуалізації, але завдяки їм отримали можливість еволюціонувати концепцію vMS. Відповідно з'явилося поняття Service Provider, яке поступово витісняє інше поняття – Telecom/Internet Provider. Таким чином, концепція vMS органічно виросла з технологій SDN, NFV та технологій оркестрації віртуальної інфраструктури, під якою розуміється технологія автоматизації розгортання та налаштування віртуального середовища відповідно до конкретних вимог [88].

Технології SDN дозволяють консолідувати всю логіку прийняття рішень щодо роботи мережного обладнання в одній точці, що, у свою чергу, дозволяє отримати більш повний контроль над інфраструктурою, а NFV дозволяють створювати віртуальні мережеві елементи для виконання вузькоспрямованих завдань (фільтрація, моніторинг та вивчення трафіку, антивірус). Раніше один фізичний пристрій міг виконувати кілька функцій, зараз за допомогою NFV з'явилася можливість розмежовувати мережеві функції на необхідну кількість віртуальних пристроїв, що дозволяє спростити схему підключення та усунути апаратні збої.

Саме на стику цих технологій знаходиться vMS – автоматизація процесу розгортання та керування IT-сервісами (рис.5.2).


Рис. 5.2. Поєднання технологій оркестрації, SND, NFV та традиційної IT-інфраструктури в vMS

З погляду кінцевого користувача, IT-сервіс – це будь-яка функція з певним набором характеристик, реалізація якої забезпечується IT-інфраструктурою. Наприклад, можливість друкувати на мережному чорно-білому принтері – це IT-сервіс (назвемо його «Basic Printer Access»). Якщо користувач є керівником певного рівня, йому має бути наданий сервіс VIP Printer Access – доступ до кольорового принтера. Якщо користувач – рядовий співробітник, йому мають бути надані сервіси: «Basic Printer Access» та «Plotter Printer Access» – друк на звичайному принтері та на плоттері. Наведений приклад, хоч і дуже простий, проте ілюструють сервісний підхід до побудови IT-інфраструктури. Інші приклади сервісів зображено на рис.5.3.

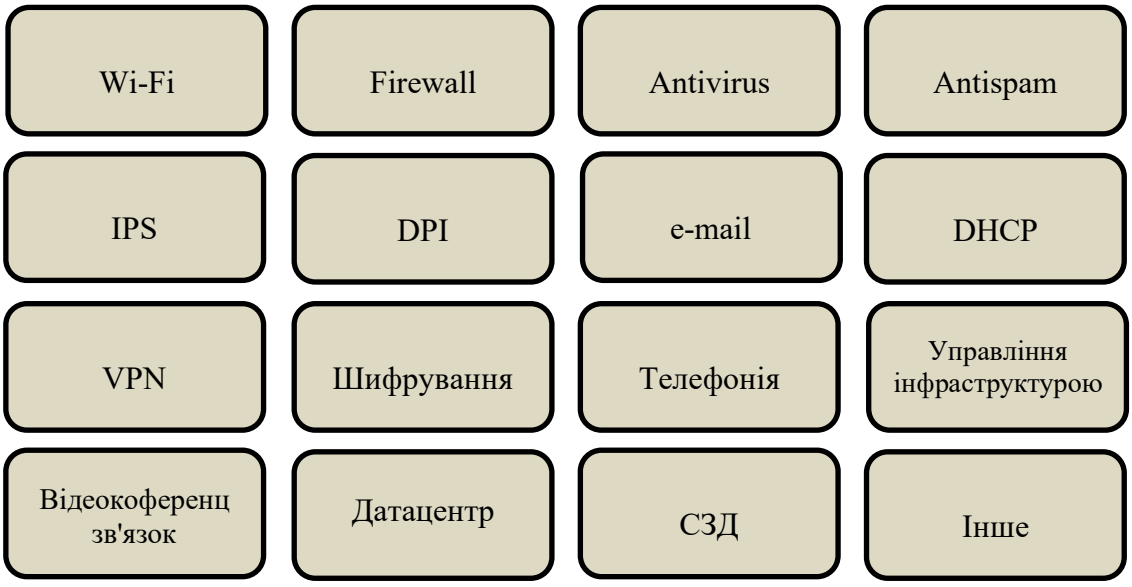



Рис. 5.3. Приклади IT-сервісів

Таких прикладів можна навести дуже багато, враховуючи, що кожен тип сервісу може мати свої підтипи, в залежності від характеристик сервісу, що надається, як, наприклад, швидкість передачі даних, резервованість, доступність, період дії, якість передачі даних (застосовується для відео), пріоритетність даних та ін. Питання затребуваності vMS треба розглядати як з погляду сервіс-провайдера (продаж сервісів у концепції vMS), так і з погляду власника бізнесу (використання vMS для забезпечення потреб бізнесу). Підхід до проектування IT-інфраструктури з погляду надання сервісів дозволяє спочатку проектувати IT-інфраструктуру виходячи з вимог бізнесу, що, у свою чергу, дозволяє власникам бізнесу краще зрозуміти свої потреби, формалізувати та систематизувати їх.

У яких випадках треба впроваджувати IT-інфраструктуру, що дозволяє надавати vMS ? З погляду власника IT-інфраструктури, впровадження vMS виправдане для організацій корпоративного рівня, які мають територіально-розподілену мережу філій. У цьому випадку набагато вигідніше замість великої кількості розрізнених програмно-апаратних систем створити віртуальні сервіси, які можна точно використовувати, але вже в єдиному віртуальному середовищі. Розгортання будь-якого необхідного сервісу займатиме невеликий час, а витрати на його надання в кожній крапці значно зменшаться.

Також використання vMS може бути привабливим для організацій, у яких динамічно змінюється мережа філій. У разі для надання корпоративних сервісів у новому відділенні потрібна лише організація надійного каналу передачі. Всі сервіси, які необхідні цьому відділенню, розгортаються автоматично, у віртуальній IT-інфраструктурі та у найкоротші терміни, оскільки немає необхідності купувати обладнання, доставляти у відділення, обслуговувати, зберігати запасні модулі тощо.

Для відповіді на запитання: «Навіщо vMS потрібні провайдерам?» необхідно провести невеликий аналіз ринку телекомунікаційних послуг.

Сьогодні найбільшого поширення набули три основні види послуг: стільниковий зв'язок, Інтернет, VPN-доступ (рис.5.4).

Якщо розглянути детальніше кожен із видів послуг, то виявиться, що кількість абонентів стільникового зв'язку в Україні – 60 млн при населенні в 42 млн. Тому ринок надання послуг доступу до мережі Інтернет настільки конкурентний та насичений, що підвищення вартості послуг навіть на 1 USD може призвести до втрати клієнта. Ринок послуг VPN досить невеликий і специфічний, тому можна не виділяти його в окрему категорію.

З урахуванням вищевикладеного очевидно, що вітчизняним сервіс-провайдерам необхідно вибрати одну з наступних стратегій подальшого розвитку:

- розвиток послуг – надання нових сервісів на ринку;
- розвиток ринку – пошук нових ринків із існуючими продуктами;
- диверсифікація – пошук нових ринків із новим продуктом.


Рис. 5.4. Послуги сучасних телеком-операторів

Реалізацію таких стратегій ми можемо спостерігати на прикладі трійки лідерів вітчизняного ринку телекомунікацій:

- Київстар – впровадження Інтернет-магазину, співпраця з Viasat для надання послуг телебачення та відео на запит. Такий підхід можна як приклад стратегії диверсифікації.
- Vodafone – співпраця з Word of Tanks, можливість купівлі авіаквитків, співпраця з мережею АЗС WOG – і це приклад стратегії розвитку послуг;
- lifecell – відкриття Інтернет-магазину, надання послуг «CINEMA», «ІМПЕРІЯ ІГОР» та ін. – також є прикладом стратегії розвитку послуг.

Якщо проаналізувати цільову аудиторію нинішніх телеком-провайдерів, її можна поділити на такі сегменти:

- користувачі мобільних пристроїв (смартфони, планшетні комп'ютери, ноутбуки, годинник та ін.) – передача голосу, відео, Інтернет, мобільні ігри, музика тощо;
- домогосподарства – домашній Інтернет та додаткові супутні сервіси;
- малий та середній бізнес – доступ до Інтернету, канали зв'язку. Рідше оренда обладнання чи хостинг;
- великий бізнес – доступ до Інтернету, канали зв'язку.

У різних джерелах оцінки ємності та відносні частки ринку дещо відрізняються один від одного, але загальна картина приблизно така, як на рис.5.5.

Якщо розглянути кожен із цих сегментів, то:

1. Сегмент мобільних користувачів перенасичений. Нові сервіси тут потрібні скоріше утримання існуючих абонентів, ніж залучення нових.
2. Сегмент домогосподарств дуже конкурентний. Локальні гравці («домашні» Інтернет-провайдери) показують себе набагато краще в цьому

сегменті, тому що вміють працювати у своїх нішах швидше та якісніше, і в їхньому бюджеті немає витрат на підтримку великого управлінського апарату, маркетингових програм тощо.

3. Малий та середній бізнес – об'єднані в одному сегменті ринку, оскільки мають спільні характеристики. Представникам цього бізнесу вже потрібна мінімальна інфраструктура, але вони ще не мають розуміння, як вони її обслуговуватимуть і розвиватимуть.

4. Великий бізнес зазвичай характеризується наявністю своєї власної інфраструктури, своїм штатом професіоналів та розумінням вимог до інфраструктури. Їхня основна потреба полягає в передачі великого обсягу даних.

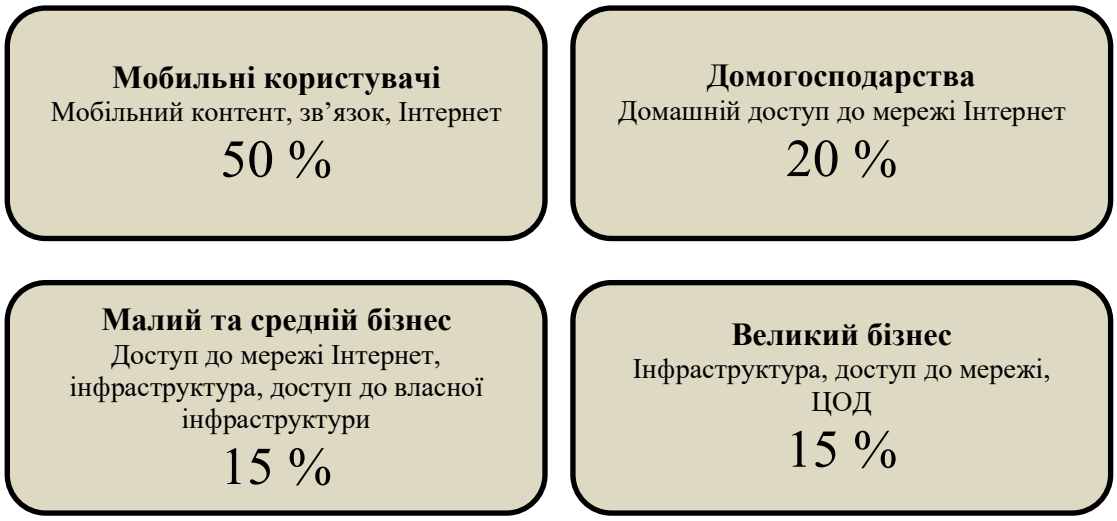



Рис. 5.5. Сегменти ринку телеком-провайдерів

З аналізу послуг телеком-провайдерами можна зробити висновок, що в їхньому портфелі практично відсутні послуги для вирішення інфраструктурних завдань у сегменті «малий і середній бізнес», представники якого стикаються з наступними типовими проблемами:

- яке обладнання встановити?
- де його взяти та як налаштувати?
- де зберігати дані та як захистити їх від несанкціонованого доступу?
- як поєднати кілька відділень в одній інфраструктурі?
- хто буде експлуатувати, обслуговувати та надавати технічну підтримку?
- у кого отримати необхідні консультації?

У мобільних користувачів та домогосподарствах такі проблеми відсутні, оскільки вони не мають власної IT-інфраструктури, а великий бізнес змушений вирішувати ці проблеми власними силами. Що стосується малого та середнього бізнесу, то тут підхід до вирішення аналогічних проблем, як правило, ситуативний та спонтанний. Саме в цих галузевих сегментах

вітчизняні телеком-провайдери можуть себе показати в новій ролі – провайдера послуг або Service Provider, оскільки концепція vMS уможливила надання послуг у вигляді сервісів, а автоматизація всіх процесів робить це економічно вигідним для провайдера та доступним для кінцевого споживача. Особливо з огляду на те, що навіть невелика організація потребує мінімально необхідного набору сервісів, як, наприклад: доступ до мережі Інтернет; обмін даними між користувачами; корпоративна пошта; мережевий екран (Firewall).

У міру зростання потреб організації до цього списку можуть додатися: доступ до Wi-Fi; Anti-SPAM; гостьовий доступ до мережі; веб-сервер; сховище даних (що резервується або не резервується); корпоративна телефонія та/або відеоконференції; БД.

Також vMS дозволяє автоматизувати процес замовлення та розгортання сервісу для надання послуги кінцевому споживачеві. У цьому необхідно реалізувати алгоритм, куди входять такі кроки (рис.4.6):

Крок 1 – на порталі самообслуговування замовник заповнює форму, в якій вказує місце підключення, кількість користувачів та набір сервісів, які він хоче замовити та виконує оплату.

Крок 2 – протягом певного часу (до кількох годин) у віртуальній інфраструктурі сервіс-провайдера автоматично створюються та налаштовуються необхідні ВМ, після чого сервіси готові до використання (наприклад, поштовий сервер та мережевий екран).

Крок 3 – на об'єкт замовника виконується доставка устаткування підключення робочих станцій до мережі (це може бути комутатор чи точка доступу).

Крок 4 – обладнання підключається до Інтернету, після чого можна використовувати замовлені сервіси.

З погляду сервіс-провайдера, цей процес є алгоритмом, що включає наступні кроки (рис.5.7):

Крок 1 – у віртуальній інфраструктурі провайдера створюється область під виділеним замовником.

Крок 2 – у цій галузі створюються ВМ, необхідні надання замовленого набору сервісів.

Крок 3 – в автоматичному режимі створюються зв'язок між ВМ, права доступу, конфігураційні параметри.

Крок 4 – налаштовується канал зв'язку у точці включення обладнання користувача.

Крок 5 – підключається обладнання на об'єкті замовника, та пристрої отримують доступ до інфраструктурних елементів, створених у віртуальному середовищі провайдера.

Крім цього, замовники можуть користуватися сервісами, не маючи фізичного підключення від цього ж провайдера. Іншими словами – маючи

будь-який доступ до Інтернету, можна отримати доступ до замовлених сервісів.


Рис. 5.6. Алгоритм розгортання сервісів кінцевим споживачем

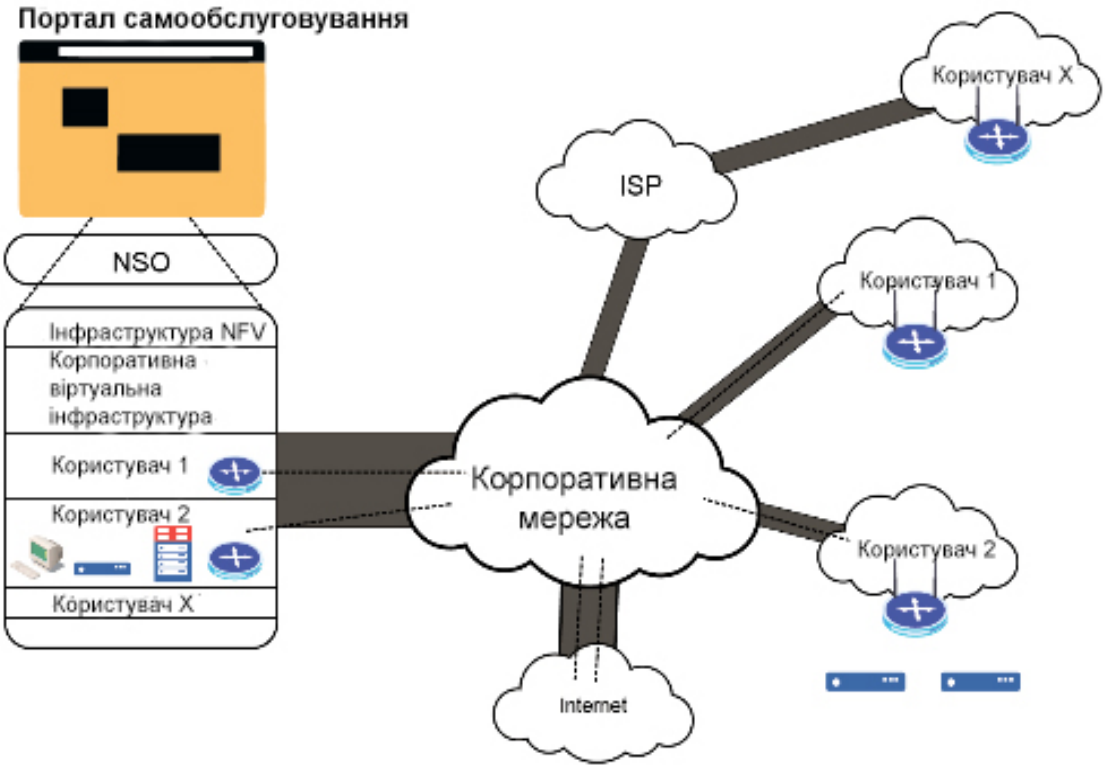



Рис. 5.7. Алгоритм розгортання сервісів сервіс-провайдером

Переваги даної моделі надання послуг для сервіс-провайдера:

- можливість повторно використати ресурси віртуальної інфраструктури;
- мінімізація кількості використання апаратного забезпечення, що веде до зменшення витрат на технічне обслуговування та зберігання запчастин;
- надання послуг через будь-який канал зв'язку;
- автоматизація процесів за допомогою vMS та портал самообслуговування;
- розширення ринку та спектру послуг.

При цьому кінцевий споживач отримує такі переваги:

- фокусування на бізнесі, а чи не на інфраструктурі;
- збереження інформації та резервування;
- відсутність витрат на обладнання та його обслуговування;
- швидкість розгортання нового відділення визначається лише часом доставки обладнання доступу;
- відкриття та/або закриття відділення не тягне за собою додаткових витрат на обладнання (купівлю, модернізацію, монтаж, демонтаж та ін.);
- експлуатація та технічна підтримка здійснюються відповідною службою сервіс-провайдера.

На вітчизняному ринку вже присутні глобальні провайдери, які надають сервіси за такою ж моделлю. Прикладом можуть бути компанії Google, Microsoft, Amazon та ін. Але конкуренція з ними не така складна, оскільки вони не мають представництв у кожному місті України та локальної команди технічної підтримки. Також великим недоліком цих провайдерів є практично повна відсутність відповідальності за порушення умов надання сервісів.

Таким чином, використання vMS дає можливість сформувати принципово нові набори послуг, які можуть бути потрібні на ринку України, і тим самим надати досить потужного імпульсу розвитку IT-галузі в цілому. Враховуючи, що існуючі можливості вітчизняних телеком-провайдерів дозволяють впровадити сервісну модель надання послуг без істотних додаткових витрат, це дає їм добрі шанси стати повноцінними і конкурентними сервіс-провайдерами.

# РОЗДІЛ 6
# ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

В останні роки з'явилося нове і дуже велике сімейство пристроїв, підключених до Інтернету та об'єднаних у різні групи, що отримало назву «Інтернет речей » (від англ. Internet of Things, або IoT) [89]. В основному це побутові або промислові пристрої, які для керування або обміну інформацією мають можливість підключення до Інтернету або сервера управління та контролю через Інтернет. Згідно з прогнозами виробника мережевого обладнання – компанії Cisco Systems до 2030 р. таких пристроїв буде підключено до мережі понад 500 мільярдів. Це приблизно по 80 IoT-пристроїв на кожного жителя планети. Кожне з них має сенсор для збору та передачі даних при взаємодії із зовнішнім середовищем. З точки зору завтрашнього дня сучасне місто немислиме без різного роду датчиків, камер, сенсорів, які збирають дані про рівень забруднення води, повітря, кількість машин на дорогах, стан грунту, температуру зовнішнього середовища, вологість, тиск, вільні місця на парковках, скупчення людей і т. д. Вся ця сукупність пристроїв та інструментарію, що забезпечує збирання даних, їх передачу, обробку та подальший аналіз, і є технологія Інтернету речей [90].

## 6.1. Інтернет речей як етап розвитку глобальної мережі

Інтернет речей описує дуже важливий етап розвитку глобальної мережі, що характеризується підключенням великої кількості пристроїв, що здійснюють автоматизовану обробку даних, без участі людини.

Основним призначенням мережі Інтернет є здійснення транспортної функції, поєднуючи приватні обчислювальні мережі, індивідуальних користувачів та ЦОД. Фізичний рівень глобальної мережі досить статичний і удосконалюється в основному в кількісному відношенні шляхом підвищення пропускної спроможності каналів зв'язку та каналоутворювального обладнання.

Значне збільшення трафіку призводить до розробки все більш потужних маршрутизаторів та вдосконалення протоколів маршрутизації та принципів функціонування мережі. У побудові сучасних мереж крім традиційного інфраструктурного рівня передачі, що містить маршрутизуюче і комутуюче устаткування, виділяється рівень управління. Поділ функцій передачі та управління дозволяє віртуалізувати мережну інфраструктуру та значно підвищити утилізацію та централізувати управління ресурсами, реалізуючи технологію програмно-визначуваних мереж, призначену для роботи в умовах динамічних змін.

Такий підхід вже сьогодні знаходить своє застосування в ЦОД при побудові хмарних сервісів та стрімко набирає популярності в корпоративних та мережах провайдерів.

Прикладною цінністю мережі Інтернет є ряд спеціалізованих сервісів, реалізованих на її базі – DNS, електронної пошти (e-mail), передачі файлів (FTP), всесвітньої павутини (World Wide Web), потокового мультимедіа і т. д. Сервіси, що надаються, знаходяться в безперервному розвитку, трансформуючи суспільство та соціологізуючи взаємодію у межах мережі. Більшість додатків використовує модель взаємодії «користувач – сервіс» і є відображенням інформаційного суспільства, що формується.

Важливим етапом розвитку Інтернету є поява концепції хмарних обчислень (Cloud Computing). В основі концепції покладено принцип загального використання програмно-апаратної інфраструктури провайдера. Такий підхід дозволяє користувачам зменшувати витрати та за необхідності гнучко нарощувати інформаційні ресурси.

Цифрові технології стають все доступнішими і є основним елементом підвищення продуктивності праці, впровадження інновацій та підвищення якості життя. Все більше різноманітних пристроїв, що використовують технологію міжмашинної взаємодії M2M, machine-to-machine, підключаються до мережі Інтернет. В рамках такого технологічного рішення використовується ряд спеціалізованих пристроїв, що збирають телеметричні властивості. Ключовою властивістю таких систем є їх індустріальна спрямованість та необхідність участі людини у прийнятті управлінських рішень. Саме цей аспект сильно обмежує застосування M2M-технологій та привів до вдосконалення концепції та появи поняття Інтернет речей.

Інтернет речей або, як його ще називають, «мережа мереж» є мережею різноманітних підключених до Інтернету пристроїв, що реалізують різні моделі взаємодії – «річ–річ» (від англ. Thing-Thing), «річ–користувач» (від англ. Thing -User) та «річ–веб-об'єкт» (від англ. Thing-Web Object).

Поєднання «розумних речей» (від англ. Smart Things ) в єдину мережу надає критично важливі якісні зміни у розвиток людської життєдіяльності. Однією з головних передумов до цього є перехід до використання в мережі Інтернет протоколу IPv6, що дає можливість надати виділену унікальну адресу кожному пристрою, що підключається. При цьому основну частину об'єктів, що підключаються, будуть складати різноманітні спеціалізовані пристрої, що мають у своєму складі мікроконтролер з різними платами. розширення – модуль передачі даних, модуль пам'яті, засоби вимірювання (датчики) та засоби ідентифікації. Для управління пристроєм, обробки та передачі даних на контролері використовується ОС реального часу, що відповідає за збирання та первинну обробку даних для мінімізації трафіку.

Повсюдне поширення «розумних речей» робить нераціональним використання традиційної моделі «клієнт-сервер» з погляду обміну трафіком. У місцях їх знаходження дуже важко забезпечити високошвидкісні канали з низькою затримкою, а власна обчислювальна потужність дозволяє проводити

необхідну обробку даних, реалізуючи концепцію туманних обчислень (Fog Computing) (рис.6.1). Функціональним елементом туманних обчислень є мікроконтролери, що поєднуються в розподілену обчислювальну мережу. Їх завдання – здійснювати зберігання та обробку інформації, що надходить, надаючи обчислювальні потужності для різноманітних прикладних завдань, що здійснюють адміністрування систем без участі людини. А структуровані дані, що отримуються на цьому рівні, можуть передаватися через спеціалізовані інтерфейси програмування додатків (API) у різноманітні системи хмарних обчислень для подальшої обробки, у тому числі і із залученням людських ресурсів.

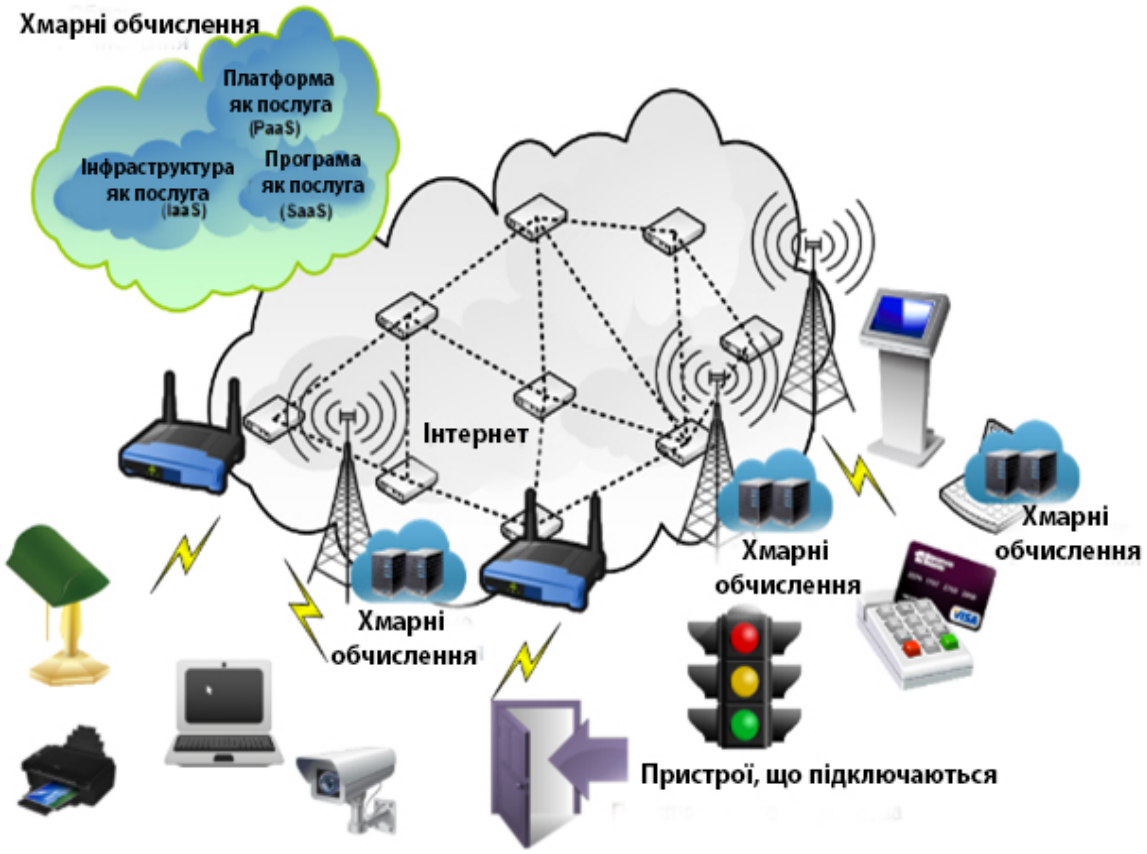



Рис. 6.1. Архітектура Інтернету речей

Як канали зв'язку використовуються конвергентні мережі на базі протоколу IP, а місця встановлення датчиків настільки різноманітні, що використання провідної інфраструктури дуже обмежене. Їхнє підключення все частіше здійснюється за допомогою бездротових технологій. Донедавна для цього використовувалися традиційні технології, призначені для користувальної передачі даних – Wi-Fi, 2G, 3G, 5G .

Зараз у технології міжмашинної взаємодії для зв'язку досі застосовують ієрархії протоколів, розроблені IEEE. Відповідно до її принципів, всі бездротові мережі сьогодні прийнято ділити на чотири типи: персональні WPAN (Wireless Wide Area Network), локальні WLAN, міські WMAN

(Wireless Metropolitan Area Network) і глобальні WWAN (Wireless Wide Area Network) бездротові мережі.

Складнощі з організацією електроживлення знижують популярність мереж сімейства стандартів 802.11. Для підключення розумних пристроїв на невеликих відстанях (до 10 метрів) застосовуються стандарти, що використовують mesh -архітектуру, мають підвищену живучість і розроблені для мінімізації енергоспоживання – LoWPAN , Bluetooth Low Energy (BLE), ZigBee IP і т.д. А для організації зв'язності на Великих відстанях розробляється ряд спеціалізованих радіотехнологій із низьким енергоспоживанням.

На вертикальних ринках вже використовується ряд технологій – C-UNB (Cooperative Ultra Narrowband), LoRa (Long Range), але найперспективнішою для Інтернету речей є технології EC-GSM (Extended Coverage GSM) та NB-CIoT (Narrowband Cellular IoT), що передбачають використання існуючих мереж мобільного зв'язку. Для цієї мети планується виділяти смуги частот нижче використовуваних у мобільних мережах, і операторам необхідно лише додати відповідні трансівери на базових станціях та оновити програмне забезпечення.

З'єднання «розумних об'єктів» в єдину мережу за допомогою IP-протоколу утворює «мережа мереж», що продукує велику кількість різноманітних телеметричних даних. І цінність одержуваної інформації цілком визначається протоколами прикладного рівня, що працюють поверх мережі. Головним завданням є однозначна ідентифікація кожного елемента. Враховуючи необхідну розрядність, найкраще для цього підходить унікальна IPv6-адреса, що виділяється кожному пристрою в сучасних мережах. Ідентифікатор використовується не тільки для маршрутизації пакетів, але і для порівняння з фізичними параметрами, властивими пристроям (mac адреса, RFID, Electronic Identification (EID), QR-кодами ...).

Маючи унікальний ідентифікатор, «розумні об'єкти», залежно від конструкції, здатні не тільки передавати потоки даних, що збираються сенсорами, а й здійснювати передачу команд для зміни стану підключених до них пристроїв.

Протоколи взаємодії між цими компонентами є стеком стандартів, що добре зарекомендували себе, адаптованих для використання через низькошвидкісні канали. Обмін повідомленнями працює за схемою «видай/підпишись» (publish/subscribe). І тому виділяється спеціалізований «сервер» передачі інформації – брокер. Вся інформація, що передається, розділяється за напрямками на різні канали. Різноманітні датчики передають інформацію про різні фізичні величини по відповідних каналах, тоді як споживачі підписуються на їх отримання, дуже гнучко обмінюючись необхідною інформацією. Описаний принцип набув широкого поширення у ряді протоколів – MQTT (MQ Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advanced Message Queuing Protocol) тощо.

Найцікавішим є протокол CoAP (Constrained Application Protocol). Він вважається адаптацією протоколу Web (web transfer protocol) до роботи з технології міжмашинного взаємодії. Він не тільки добре інтегрується з HTTP, а й підтримує адміністрування підключених пристроїв.

Система управління відповідає за конфігурування, оновлення та моніторинг роботи обладнання. Можливості управління «розумними об'єктами» значно менші порівняно з «класичними» пристроями (маршрутизаторами, комп'ютерами, серверами) і мають свою специфіку. Для цього розроблено низку стандартів, що працюють за технологією клієнт-сервер – CWMP, OMA-DM, Lightweight M2M.

Все частіше ми чуємо про злам пристроїв та їх використання в шкідливих цілях, а всі питання безпеки вирішуються індивідуально кожним виробником пристроїв та ПЗ. Враховуючи широту поширення «розумних об'єктів» та ускладнення цільових атак, не дивно, що посилена увага у розробці протоколів приділяється безпеці.

Заходи щодо безпеки можна умовно розділити за чотирма напрямками – підключення, ідентифікація, шифрування трафіку, що передається, та безпека додатків.

Збереження цілісності та конфіденційності даних досягається застосуванням шифрування для автентифікації та збереження цілісності повідомлень. Процедура передбачає підтвердження даних користувача та ліквідності використовуваних сертифікатів, що досить складно реалізувати у глобальних масштабах, тому виробники найчастіше жорстко вбудовують облікові дані у програмно-апаратний комплекс. Ця інформація дозволяє чітко ідентифікувати пристрій, але не підходить для забезпечення цілісності даних.

На транспортному рівні питання безпеки передачі даних вирішується у рамках протоколів TLS та Datagram TLS (DTLS) шляхом створення захищеного тунелю для додатків. Але, незважаючи на це, додатки є найуразливішою частиною рішення. Їхнє безконтрольне поширення становить серйозну загрозу. Надання розподіленої платформи для обробки даних різними додатками – одна з особливостей архітектури Інтернету речей та основні тенденції у вдосконаленні протоколу їх безпечного підключення OAuth 2.0 Internet of Things – виявлення «розумних речей» та їхня аутентифікація, використання цифрових ідентифікаторів та централізоване управління доступом до ресурсів.

І майбутнє глобальних туманних обчислень повністю залежить від можливості взяти процеси під контроль і забезпечити безпечну розподілену інформаційну мережу, що самоконфігурується.

Використання повсюдного Інтернету речей – це все-таки віддалена перспектива; «розумна держава», «розумні міста», «розумний дім» на даному етапі розвитку – поки що рідкість. Впровадження Інтернету речей відбуваються над глобальних масштабах, а всередині компаній. Технологія «розумних речей» здатна підвищити продуктивність праці насамперед у виробничому сегменті, логістичному бізнесі, транспортних та енергетичних

компаніях. Складність застосування полягає в тому, що жоден виробник не має у своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників, і від їх правильного підбору та інтеграції залежить те, наскільки точно реалізоване рішення відповідатиме завданням та вимогам конкурентного середовища.

### 6.2. Глобальна мережа малої потужності для Інтернету

У 2020 році кількість пристроїв, підключених до Інтернету, перевищила 30 мільярдів, а у 2025 році досягне 75 млрд. І всі ці пристрої обмінюються даними один з одним, а якість їхньої роботи багато в чому визначається якістю зв'язку між пристроями. У «розумних будинках», на виробництві для цього часто використовуються Wi-Fi, Bluetooth, ZigBee і т.д. Їхній радіус дії дозволяє забезпечити надійний зв'язок з Інтернетом речей в межах від десятків до сотень метрів. У випадках, коли потрібно підключити більшу кількість об'єктів до Інтернету речей та на більшій території, необхідно шукати інші рішення. В даний час це можна організувати на існуючих стільникових мережах або за допомогою LPWAN (Low-power Wide Area Network) – глобальної мережі малої потужності [91].

У 2015 р. була створена некомерційна організація LoRaAlliance для прийняття та просування протоколу LoRaWAN як єдиний стандарт для глобальних мереж з низьким енергоспоживанням – LPWAN [92]. Час автономної роботи LoRaWAN-пристроїв може досягати кількох років, що робить їх ідеальними для використання у віддалених місцях або енергонезалежних системах. Ця технологія має такі переваги: низьку вартість кінцевих пристроїв; тривалий час автономної роботи (до 10 років); безпека (подвійне шифрування); діапазони частот, що не ліцензуються; відкритий стандарт; велику ємність мережі.

Мережева топологія LoRaWAN є класичною зіркою, в центрі якої знаходиться шлюз, що працює в режимі прозорого моста, що передає повідомлення між кінцевими пристроями і центральним мережевим сервером. Шлюзи підключаються через протокол IP. Кінцеві пристрої підключаються через радіоканал безпосередньо до шлюзу або кількох шлюзів. З'єднання найчастіше одноадресне (unicast), але підтримується режим багатоадресної розсилки (multicast). В основі бездротової передачі лежить лінійна частотна модуляція, яка добре працює на малопотужних пристроях і має великий радіус дії. Швидкість передачі у каналі – від 0,3 до 50 кбіт/с. Використовується технологія адаптації канальної швидкості різних параметрів, наприклад, від відстані до БС. Мережевий сервер LoRaWAN виконує функції керування, у тому числі параметрами радіоканалу (швидкість передачі, потужність тощо). Безпека в мережах LoRaWAN забезпечується досить надійно, для чого використовуються шифрування на рівні програми та на рівні мережі, а всі ключі використовують алгоритм шифрування AES з розміром блоку 128 біт.

Радіомодулі в стандарті LoRaWAN поділяються на три основні класи залежно від потужності енергоспоживання:

- Клас А – пристрій передає повідомлення БС, після чого деякий час слухає ефір на предмет повідомлень від БС. Дані передаються кілька разів на добу. Термін служби ~ 10 років.
- Клас В – пристрій реалізовано аналогічно класу А, але додатково кілька разів на добу слухає повідомлення від БС. Термін служби ~ 3-5 років.
- Клас С – пристрій постійно «слухає» ефір, перериваючись лише з передачі даних. Необхідне джерело постійного електроживлення.

Для малопотужних мереж M2M немає єдиного рішення, яке б задовольнити всі можливі сценарії використання, і LoRaWAN теж виняток. LoRaWAN використовує протокол доступу ALOHA з деякими модифікаціями, але за своєю суттю це метод випадкового доступу, коли кожен клієнт може почати передавати дані в будь-який момент, що в навантажених мережах неминуче призводитиме до накладення сигналів від клієнтських станцій, їх втрати і як наслідок – погіршення загальної продуктивності стільники загалом. Шлюзи LoRaWAN мають радіус дії близько 10 км і можуть обслуговувати тисячі кінцевих пристроїв, але з невеликими швидкостями передачі даних та досить високими ймовірностями втрати пакетів у разі великої щільності пристроїв. За допомогою LoRaWAN можна в режимі online виконувати моніторинг віддалених промислових об'єктів та керувати інфраструктурою у «розумних містах».

LoRaWAN хоча і найбільш поширений, але не єдиний метод передачі даних в IoT-мережі. Крім LoRaWAN, також розробляються стандарти 802.15.4 (на основі Wi-Fi). Це компанія SigFox , яка одночасно є оператором та виробником обладнання, а також стандарт NB-IoT ( NarrowBand Internet of Things ), що просувається консорціумом по мобільній телефонії 3 GPP. З точки зору швидкості передачі даних NB-IoT має більшу швидкість, ніж LoRaWAN , але не на багато. SigFox має найповільніший канал зв'язку, і до того ж односторонній. З погляду архітектури, кожна з конкуруючих технологій використовує або шлюз, або БС як точку бездротового інтерфейсу. SigFox і LoRaWAN використовують діапазони частот, що не ліцензуються, що є їх перевагою в порівнянні з NB-IoT .

Кожна технологія має свою нішу, де її застосування є найбільш обґрунтованим. SigFox та LoRaWAN найкраще підійдуть там, де потрібно передавати кілька коротких повідомлень кілька разів на день. З іншого боку, NB-IoT буде доцільніше використовувати там, де необхідно забезпечити невеликі затримки та часту передачу повідомлень. Кожна IoT-технологія має свої унікальні переваги, але всі вони виконують одне завдання – передати мінімум даних за мінімального енергоспоживання на максимальну відстань.

Також можлива передача даних з використанням 3G, 4G, 5G, LTE, Wi-Fi та дротових технологій. Найчастіше наданням послуг для забезпечення Інтернетом речей займаються великі оператори зв'язку, але з LoRaWAN це стає доступно будь-кому, тому що альянс LoRaWAN є відкритим.

За допомогою LoRaWAN можна виконувати моніторинг віддалених промислових об'єктів, наприклад, контроль температури або тиску в паливних баках, виявлення витоку, контроль вібрації, оптимізацію споживання енергії і т.д. д., так як термін служби датчика може доходити до 10 років, а кількість інформації, що передається, невелика і відбувається досить рідко. Перспективним вважається застосування LoRaWAN в «розумних містах», де керування значною частиною інфраструктури відбувається online. Ще одне перспективне застосування – це розумне освітлення, яке керуватиметься датчиками LoRaWAN.

У специфікації LoRaWAN1.1 підтримується визначення місцезнаходження за допомогою тріангуляції, тобто за БС, що дасть можливість визначати місцезнаходження датчика з точністю 10–20 м. За допомогою датчиків LoRaWAN можна створити єдину мережу, яка передаватиме інформацію про показання температури в будівлях і будинках будь-яких розмірів. Перевагою буде те, що датчики можна буде розмістити у важкодоступних місцях. Застосування LoRaWAN у датчиках диму має добрі перспективи у зв'язку з тривалим терміном автономної роботи. Датчики вологості зможуть застосовуватись у великих приміщеннях, теплицях тощо.

Контроль вібрації (сейсмодатчики) – ще одне дуже перспективне використання LoRaWAN, оскільки до такого роду датчиків пред'являються особливі вимоги щодо часу автономної роботи та радіусу дії, з чим добре справляється LoRaWAN.

Незважаючи на те, що існує ще низка невирішених питань, у тому числі пов'язаних із забезпеченням належного рівня безпеки, як одна з перспективних технологій Інтернету речей може бути розглянута LoRaWAN – як рішення останньої милі для низькошвидкісних автономних пристроїв. У даній технології є свої переваги та недоліки, але, враховуючи велику кількість організацій, що входять до LoRa Alliance і збільшення кількості комерційних проектів на основі LoRaWAN можна сподіватися на її затребуваність у новому цифровому суспільстві.

### 6.3. Технології Інтернету речей

Використання технології Інтернету речей у повсякденному житті дозволить її спростити та зробити більш комфортною та безпечною [90]. Архітектура IoT-мережі досить проста і включає чотири основних компоненти (рис.6.2):

- сенсор із передавачем;
- БС;
- мережевий сервер/систему управління;
- сервер додатків.

*Сенсори та передавачі.* Сенсор збирає інформацію із зовнішнього середовища та з певною періодичністю передає через радіомодуль дані на БС. Радіомодулі, або, в зарубіжній термінології, транспондери виконують

функцію прийому сигналу від сенсора і передачі його далі в мережу, а метод передачі даних не має значення. Відмінною рисою технології Інтернету речей є використання бездротових сенсорів разом із передавачами із дуже низьким енергоспоживанням, термін роботи яких вимірюється роками. Саме низьке енергоспоживання уможливило впровадження технології Інтернету речей.

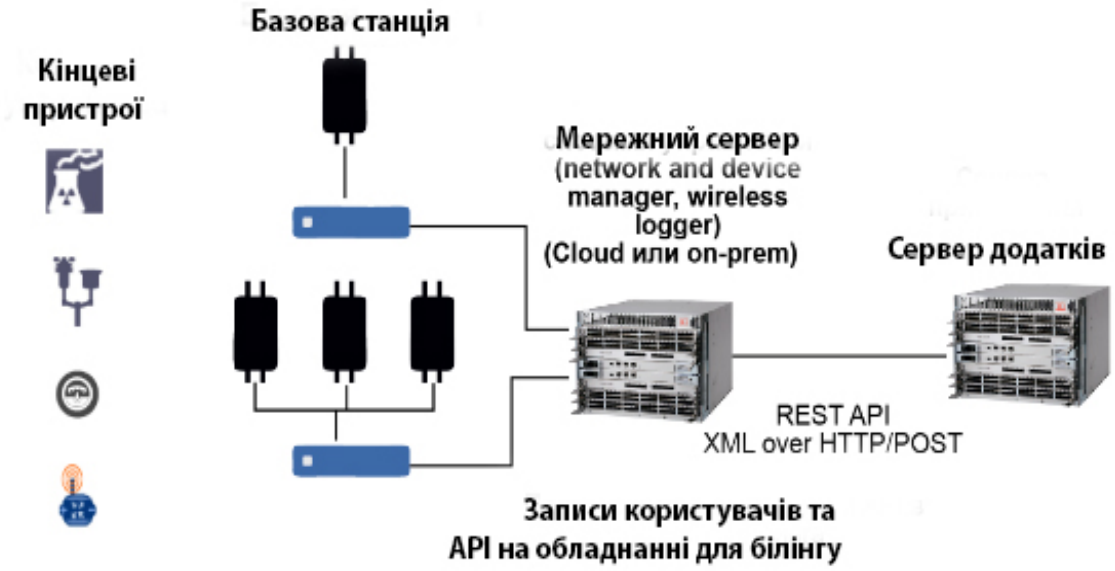



Рис. 6.2. Архітектура IoT-мережі

У випадках, коли необхідно підключити більшу кількість IoT-пристроїв і на більшій території, можна використовувати існуючі мережі або зробити це за допомогою LPWAN – глобальної мережі малої потужності.

*Базова станція.* Виконує завдання отримання радіосигналу та передачі даних через мережну інфраструктуру на мережевий сервер. Оскільки IoT-технологій немає значення спосіб транспортування даних від датчика до сервера додатків, то БС пред'являється лише вимога підтримувати той самий тип передачі, як і передавач. БС відрізняються один від одного радіусом покриття (від 10 до 15 км) та обсягом інформації, що приймається від датчиків.

*Мережеві сервери.* Агрегує сигнали від сенсорів, «витягує» корисні дані та передає їх на сервер додатків. Завдання мережевого сервера – отримати сигнал від БС, «витягти» корисні дані та передати для подальшої обробки спеціалізовані системи, а також здійснювати моніторинг та управління пристроями IoT-мережі.

*Сервер програм.* Програмно-апаратний комплекс, що дозволяє інтерпретувати дані, отримані від датчиків, та надати їх користувачу у зручному для нього вигляді.

Відмінність сервера додатків від мережевого сервера в тому, що сервер додатків нічого не знає про сенсори, тому що оперує даними, отриманими з мережі, а мережевий сервер керує пристроями та агрегує сигнали від мережі сенсорів в одній точці. Саме сервер додатків є аналітичним центром, який

інтерпретує дані для кінцевого користувача. А оскільки кінцеві користувачі можуть отримувати показники, що їх цікавлять від ПК, мобільних пристроїв або використовуючи автоматизовані програмні засоби через API, то розгортання сервера додатків буде найбільш трудомістким процесом при впровадженні IoT-мережі. А основні трудові витрати будуть пов'язані з розробкою програмного забезпечення, API та логіки роботи сервера додатків.

На сьогоднішній день вже існують хмарні послуги, що надають функції сервера додатків. Архітектура таких IoT-мереж досить проста – БС, отримавши сигнал від сенсора, відразу ж передає його на сервер у хмарі (рис.6.3).

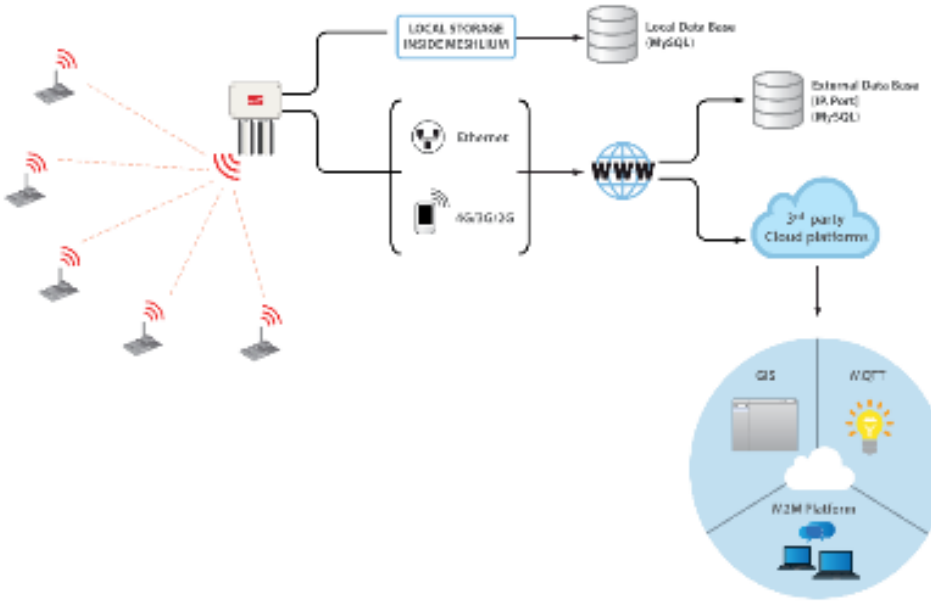



Рис. 6.3. Архітектура IoT-мережі з підключенням до хмарного сервісу

У хмарі і відбувається подальша обробка та аналіз даних, розмежування прав користувачів, надання даних у потрібному форматі.

Хмарні сервіси для Інтернету речей надають уже десятки компаній: Simfony, Amazon web services, Sofia, Cumulocity, sensorup, Smart. Так, наприклад, компанія Amazone надає сервіс AWS IoT, що дозволяє підключати пристрої мережі до хмарного сервісу для подальшого аналізу та обробки даних. А хмарний сервіс Cumulocity надає функціонал управління пристроями, SDK для розробки плагінів та додатків, обстеження даних, безпеку, розмежування прав користувачів, інтеграцію з програмними продуктами третіх компаній-виробників (SAP, Astea, Zapier), аналіз даних, управління даними, аналітику та прогнозування, настроювання правил обробки даних та ін.

Отже, Інтернет речей – це не технологія передачі даних через бездротову мережу, це технологія збору даних з множини сенсорів, обробка, аналіз та надання даних користувачеві. Ця технологія вже добре зарекомендувала себе в США та розвинених європейських країнах.

# РОЗДІЛ 7
# СИСТЕМИ ПІДТРИМКИ ОПЕРАЦІЙНИХ ПРОЦЕСІВ

Однією з основних особливостей сучасного етапу розвитку телекомунікаційного ринку є зосередження зусиль операторів зв'язку на підвищенні якості обслуговування клієнтів та зменьшення операційних витрат, що визначає величезний інтерес до систем підтримки операційних процесів операторів зв'язку – Operation Support Syste m (OSS) в усьому світі.

Системи підтримки діяльності операторів зв'язку дозволяють автоматизувати процеси експлуатаційної діяльності та доповнити існуючу мережну інфраструктуру засобами управління, інтегруючи різноманітні додатки до єдиного інформаційного та операційного простору.

Впровадження OSS дозволяє на базі систем управління та моніторингу, зосередити інформацію про роботу мережі в єдиному центрі управління, багаторазово збільшити віддачу від наявних ресурсів та вийти на новий якісний рівень розвитку.

## 7.1. Розвиток систем підтримки операційних процесів операторів зв'язку

Історія розвитку систем підтримки операційних процесів чи, як їх ще називають, систем автоматизації операційної діяльності, що тісно пов'язана з розвитком світового телекомунікаційного ринку, який пройшов значний еволюційний шлях і зазнав істотних трансформацій [93]. Приблизно з середини 80-х років минулого століття для вирішення проблеми управління мережами провідні міжнародні організації в галузі стандартизації ISO (International Organization for Standardization), ITU (International Telecommunication Union), ETSI (European Telecommunications Standards Institute) та ін розробили ряд стандартів для систем управління (СУ) мережами зв'язку. В результаті в рекомендаціях ITU-T (сектор стандартизації ITU) M.3010 було викладено загальні принципи планування, функціонування та технічного обслуговування системи керування електрозв'язком (Telecommunications Management Network – TMN) з використанням

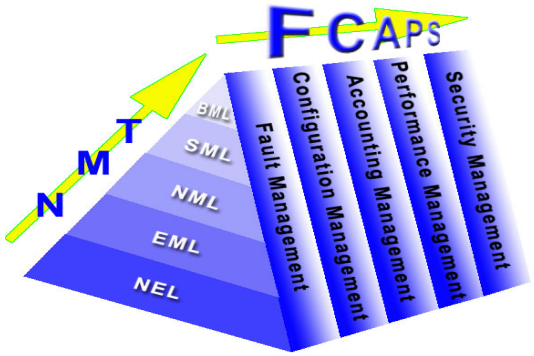



Рис. 7.1. TMN-модель

стандартних протоколів та інтерфейсів. Запропонована у рекомендаціях TMN -модель СУ (рис.7.1) охоплювала п'ять рівнів управління мережами зв'язку:

- управління бізнесом (Business Management – BM);
- управління сервісами (Service Management – SM);
- управління мережею (Network Management – NM);
- управління елементами (Element Management – EM);
- елементи мережі (Network Element – NE).

У свою чергу, для прикладних функцій управління мережею TMN виділено п'ять функціональних областей (так звана модель FCAPS):

- управління усуненням відмов ( Fault Management – FM);
- керування конфігурацією мережі (Configuration Management – CM);
- управління розрахунками з користувачами та постачальниками послуг (Accounting Management – AM);
- контроль продуктивності мережі (Performance Management – PM);
- забезпечення безпеки роботи мережі (Security Management – SM).

Виявилося, що представлені моделі FCAPS та TMN взаємно доповнюють одна одну. Така модель у певний період сприяла значному розвитку систем OSS, які відповідали вимогам свого часу. При цьому велика кількість OSS систем були самописними або замовними, і кожна з них була налаштована на «свої» архітектуру мережі, обладнання та послуги, що надаються. Але згодом вимоги клієнтів до послуг зв'язку значно зросли, і виявилося, що системи OSS періоду технологічного зростання слабко відповідають новим бізнес-вимогам, а саме: мають, з одного боку, дублювання, з іншого, – фрагментарне покриття функцій і, крім того , їх складно та дорого модернізувати. Ці недоліки були наслідком того, що основною метою концепції TMN було підвищення ефективності роботи мережі, а не операторської компанії як підприємства загалом.

Вирішенню проблем, що виникли у розвитку телекомунікаційного бізнесу взагалі і OSS-систем, зокрема, посприяла розпочата в 1995 р. робота міжнародної неурядової організації TeleManagement Forum (TM Forum) з розробки способів управління телекомунікаціями за принципом від бізнес-завдання надання послуг до управління обладнанням. Розвиваючи ідеї управління мережами, закладені в документах ISO, ITU, та на основі узагальнення досвіду багатьох телекомунікаційних компаній TM Forum розробила для оператора зв'язку типову структуру бізнес-процесів з управління наданням послуг – TOM (Telecommunication Operations Map). Згідно з TM Forum, для ефективного впровадження системи OSS необхідно насамперед використовувати відповідну сучасним вимогам модель бізнес-процесів оператора зв'язку, у створенні якої операторам має допомогти типова структура бізнес-процесів TOM. Рішення для OSS-систем мають будуватися відповідно до загальної структури бізнес-процесів оператора. Модель бізнес-процесів дозволяє правильно визначити вимоги до системи OSS, які відповідають за досягнення бізнес-цілей. Тому структура процесів TOM стала для багатьох розробників OSS-систем, телекомунікаційних

компаній та системних інтеграторів відправною точкою при впровадженні систем OSS і дозволила більшою мірою узгодити технологічний та бізнес-підхід.

Надалі TM Forum, аналізуючи фактичний розвиток та тенденції телекомунікаційного ринку, постійно вдосконалює розширену карту процесів телекомунікаційного оператора (enhanced Telecommunications Operations Map – eTOM), яка прийшла на зміну TOM і розробляє рекомендації щодо її практичного використання [101]. Структурна модель бізнес-процесів eTOM націлена на створення загального уявлення про бізнес-процеси надання послуг зв'язку та орієнтована на задоволення запитів клієнтів з високою ефективністю для оператора.

Основна відмінність eTOM від TOM – це більш повна та детальна структурна модель бізнес-процесів, що має чотири рівні деталізації. Фактично в ній описані типові бізнес-процеси оператора зв'язку, декомпозовані до 4-го рівня, що не вимагає для їх розгляду обліку технологічних особливостей оператора. Відповідальності OSS-систем на структурі бізнес-процесів eTOM відповідають бізнес-процеси в області Операційні процеси для горизонтальних рівнів Управління сервісами та Управління ресурсами.

З 2004 р. eTOM як типова структура бізнес-процесів оператора зв'язку набула статусу офіційного стандарту ITU. Для України в цей період більш характерним є екстенсивний розвиток ринку телекомунікацій, коли практично єдиним аргументом у боротьбі за клієнта були «цінові війни», тому розуміння необхідності побудови моделей бізнес-процесів для управління бізнесом, тобто застосування процесного управління на додаток до структурно-функціонального, не було приділено належної уваги. Це період обережного знайомства з eTOM та іншими рекомендаціями TM Forum. На наш погляд, недостатня увага до процесного підходу не дозволила операторам досягти очікуваних результатів від впровадження OSS-систем. Адже, на думку експертів, саме бізнес-логіка є при впровадженні систем OSS тією основою, яка дозволяє правильно визначити послідовність впровадження ключових додатків та, як наслідок, необхідний обсяг інвестицій та очікування віддачі від них.

Але у зв'язку з тим, що в цей період мережі операторів досягають масштабів усієї країни, і для надання послуг все більше використовуються мережеве обладнання та системи управління (NMS, Element Management System – EMS) різних виробників, зростає роль централізованих OSS-систем, що дозволяють створювати і використовувати єдині взаємодіючі між собою інформаційні моделі ресурсів мережі (Inventory Management System – IMS), її продуктивності (Performance Management System – PMS) та подій, що відбуваються (Fault Management System – FMS). Такі OSS-системи стають одним із найважливіших елементів централізованих систем експлуатації і дозволяють операторам значно підвищити ефективність використання ресурсів мережі, відстежувати її продуктивність, суттєво спростити і зробити

більш ефективною обробку багатьох подій мережі для скорочення часу на виявлення аварійних ситуацій та їх відпрацювання [95]. Ці системи вимагають серйозних капіталовкладень, але, незважаючи на це, при їх створенні більша перевага надається використанню промислових та апробованих рішень.

Значно вичерпавши можливості екстенсивного розвитку, оператори зв'язку для збереження та посилення своїх позицій у конкурентній боротьбі змушені пропонувати ринку нові послуги, скорочувати час їх виведення та приділяти велику увагу якості цих послуг відповідно до зростаючих запитів клієнтів. Ринок телекомунікацій стає дедалі клієнт-орієнтованим. Для того, щоб відповідати новим вимогам ринку, операторам потрібно було вдосконалити свої підходи до управління телекомунікаційними мережами, що призвело до необхідності значного розширення функціональної відповідальності систем OSS. Тому вищезазначені компоненти OSS-систем (IMS, FMS, PMS) доповнились такими:

- TT (Trouble Ticketing) – система контролю за усуненням несправності;
- WOM (Work Order Management) – система керування виконанням робіт на мережі;
- SC (Service Catalog) – модель послуг мережі ;
- AS (Activation System) – системи активації ресурсів та сервісів;
- SLM (Service Level Monitoring) – системи моніторингу рівня сервісу;
- SLA – система керування рівнем послуги клієнта.

Необхідність управління повним циклом надання послуги зажадала більш тісної інтеграції із системами бізнес-підтримки (Business Support System – BSS). Інший важливою особливістю цього періоду є те, що для надання послуг все більше використовуються IT-сервіси. Це накладає свої особливості на використання OSS-систем:

- необхідність інтеграції систем OSS з IT-ресурсами, що використовуються для надання послуг (централізований моніторинг та інвентаризація IT-ресурсів з боку OSS-систем, обмін даними з IT-додатками та ін.);
- необхідність комбінованого використання підходів, що визначаються різними стандартами (наприклад, забезпечення взаємодії eTOM-процесів та ITIL-процесів (Information Technology Infrastructure Library – ITIL), тобто бізнес-процесів, що належать до служби експлуатації мережі та IT-процесів).

Ця особливість знайшла своє відображення у рішеннях TM Forum. Почавши кілька років тому з рекомендацій щодо комбінованого використання ITIL і eTOM, TM Forum в eTOM версії 8.0 запропонував карту процесів, яка включає і ITIL-процеси [96].

Таким чином, системи OSS складаються з різних компонентів, які взаємопов'язані в єдину інтегровану систему, метою якої є забезпечення функціонування основних процесів постачальника послуг із заданим рівнем

якості надання сервісу. Використання OSS-систем дозволяє отримати істотні переваги за рахунок:

- централізації інформації про роботу мережі та мережевого обладнання в єдиному центрі управління, що дозволяє підвищити ефективність експлуатації мережі та підвищити якість управління;
- актуалізації стану систем у реальному часі, що дозволяє службам технічної підтримки суттєво підвищити ефективність своєї роботи та знизити час реакції на позаштатну ситуацію;
- збирання даних для подальшого аналізу системами BSS;
- зменшення вимог до спеціалізації обслуговуючого персоналу та кількості унікальних фахівців;
- підвищення якості обслуговування клієнта;
- зниження часу на організацію нових послуг.

Цим пояснюється значний попит на OSS-системи, що забезпечують автоматизацію основних бізнес-процесів оператора зв'язку, пов'язаних з матеріально-технічним забезпеченням, управлінням мережею, наданням послуг та підтримкою клієнтів.

## 7.2. Особливості систем підтримки операційних процесів для мереж нового покоління

Черговим етапом розвитку телекомунікаційних технологій стала поява мереж NGN (Next Generation Networks), які покликані забезпечити широкий асортимент та високу якість послуг, при цьому скоротити витрати оператора і підвищити прибутковість надання послуг. Розвиток ринку зв'язку призвело до нових передумов появи мереж NGN:

- масового впровадження сучасних систем та засобів зв'язку, характерні риси яких – мультисервісність та мультипротокольність;
- суттєву зміну мережевих архітектур: відмову від жорсткої ієрархії, характерної для класичних ТфЗК, під впливом впровадження нових засобів зв'язку, принципів передачі та обробки інформації;
- функціональному поділу рівня транспортної мережі і рівня формування послуг, що виник у результаті впровадження інтелектуальних мереж (IN) і закріпленому в NGN (завдяки Інтернету, оператору необов'язково мати власну транспортну мережу, а спектр послуг вийшов за рамки традиційних послуг зв'язку; розмитим виявилося і поняття-концепція «телематичні служби»);
- загострення конкуренції у динамічних секторах ринку, таких як мобільний зв'язок, Інтернет, послуги для корпоративних користувачів;
- поділу бізнес-моделі оператора нових послуг на дві частини: інфраструктурну (створення та обслуговування мережі) та сервісну (пов'язану з маркетингом);

- наявності проміжних ланок – віртуальних операторів, які формують та реалізують пакети послуг із доданою вартістю, як це роблять системні інтегратори в IT;
- зміни статусу інфокомунікаційних послуг: власне мережа втрачає свою цінність, її набувають послуг;
- зменшення ролі/частки голосових послуг у сучасних пакетах Triple Play (TP) та Quadruple Play (QP);
- використання умовно безкоштовних послуг, що базуються на експлуатації мережі Інтернет (наприклад, послуга, що надається по Skype);
- зниження інвестиційної привабливості, конкурентоспроможності та рентабельності традиційних систем зв'язку.

Концепція NGN передбачає підтримку необмеженого набору послуг з гнучкими можливостями щодо їх управління, реалізацію універсальної транспортної мультипротокольної мережі з розподіленою комутацією, інтеграцію з традиційними мережами зв'язку. Базовим принципом NGN є поділ функцій перенесення та комутації, керування викликом та керування послугами. Замість прийнятого традиційних мережах управління каналами для з'єднання між абонентами за принципом «точка–точка» в NGN реалізується перехід до ідеології віртуальних приватних мереж, здійснюють доставку сервісів кінцевому користувачеві поверх протоколу IP.

Для побудови мережі, яка задовольняє концепції NGN, у функціональній моделі NGN ITU виділяє три категорії об'єктів: функції, послуги, ресурси. Сервіси реалізуються різними функціями за допомогою доступних ресурсів. Один і той ж сервіс може реалізовуватися різним набором функцій і навпаки, одна функція можна використовувати реалізації різних сервісів. Їх взаємозв'язок показано на рис.7.2.

Технології NGN пред'являють до OSS-систем нові вимоги, що змінюються разом із розвитком NGN [97]. Головна відмінність полягає в тому, що OSS-система в мережах нового покоління відповідає не тільки за керування мережею, а й має забезпечити якісне функціонування користувацьких послуг та технологічних служб (сервісів). Тобто акценти все більше зміщуються у бік обслуговування абонентів, тому OSS-система має вміти використовувати інформацію про користувачів, накопичувати її, класифікувати та інтелектуально обробляти. Функції NGN показано на рис.7.3.

Тому рішення, що забезпечують заданий рівень послуги клієнта (SLA) та її якість (QoS), мають бути невід'ємною частиною OSS-систем. Дедалі більше затребуваними стають рішення для управління сприйняттям послуги користувачем (CEM – Customer Experience Management).

Мережі наступного покоління та послуги, що надаються на базі, на порядок складніші та динамічніші, ніж існуюче мережеве середовище, реагувати на будь-які, в тому числі й можливі негативні зміни, необхідно буде дуже швидко, тому в більшості випадків доведеться використовувати «проактивне» (превентивне) управління замість «реактивного».

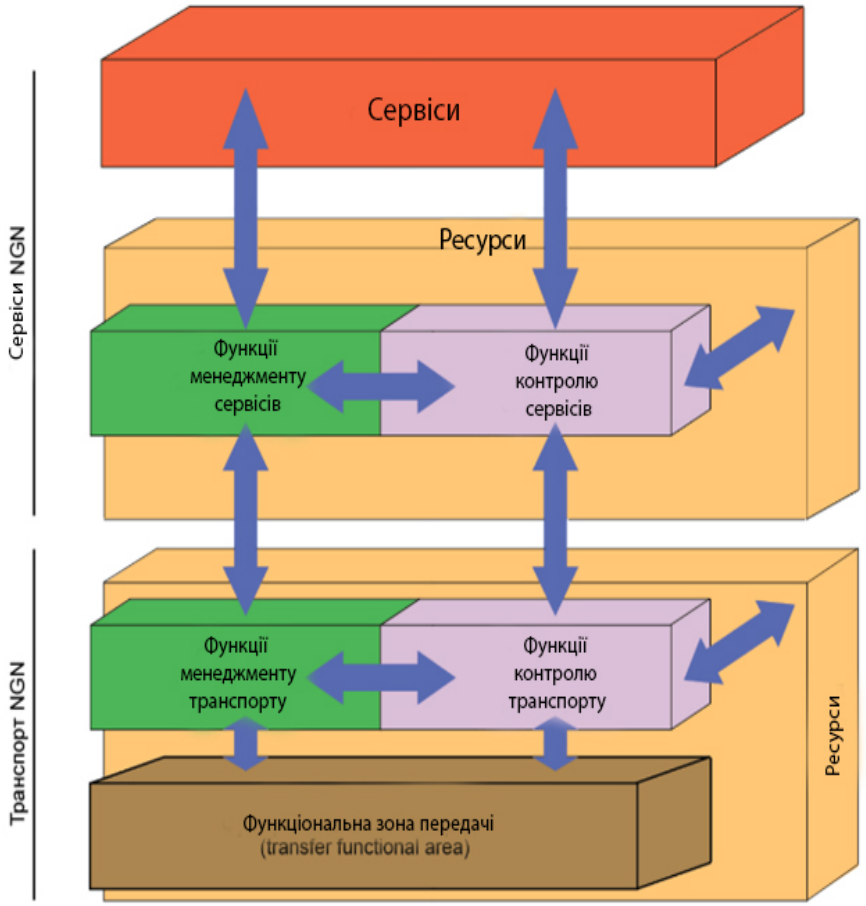



Рис. 7.2. Узагальнена функціональна модель NGN

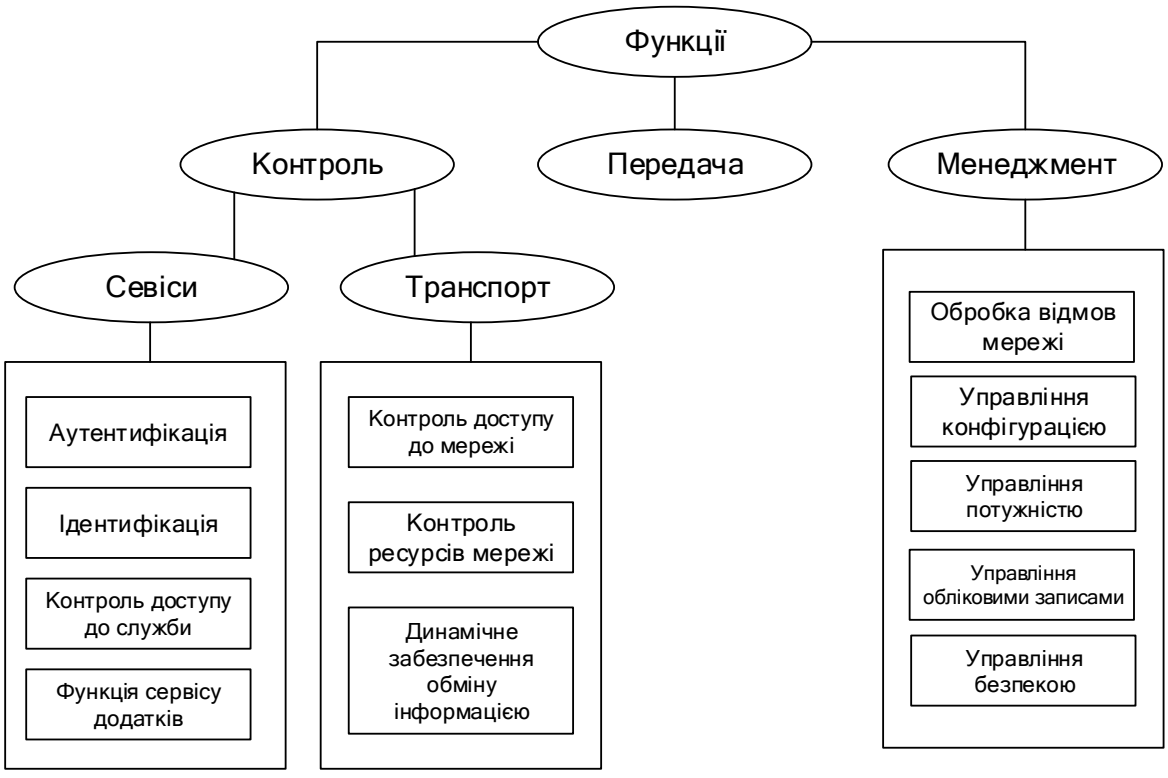



Рис. 7.3. Функції NGN

Послуги у цих мережах безперервно активуються та дезактивуються. Це супроводжується інтенсивним додаванням, видаленням і конфігуруванням пристроїв, що призводить до значного збільшення кількості подій, що при цьому генеруються. Більше того, конвергентна природа NGN означає, що кожна подія може бути пов'язана з помилкою, що зачіпає якусь послугу, при цьому не впливаючи на неї самостійно. Оператор у цих випадках повинен у режимі реального часу ідентифікувати, яка подія, пов'язана з помилкою в роботі обладнання, впливає на надання послуг.

Недостатньо розвинені технології управління проблемами призведуть до великих експлуатаційних витрат або навіть неможливості надання послуг, тому що NGN-мережі більш критичні до можливих простоїв. Тому відповідні засоби OSS-систем необхідно доопрацювати або замінити на нові, щоб вони змогли забезпечити необхідний рівень обробки вхідних подій, а саме:

- автоматичне фільтрування, дедуплікація та агрегація, щоб показувати лише пов'язані з першопричиною події; виявлення критичних подій;
- високий рівень автоматизації ізоляції проблеми шляхом застосування складного кореляційного аналізу та ефективних правил пошуку подій, пов'язаних із першопричиною проблеми (Root Cause Analysis – RCA);
- збагачення подій, пов'язаних з першопричиною проблеми, для автоматизованого/автоматичного виявлення їх впливу на користувачів та послуги (Impact Analysis – IA);
- автоматизована кореляція проблем мережі та проблем користувача;
- автоматичний пошук на основі моделей першопричини проблеми (RCA) та виявлення впливу (IA), що буде дуже актуальним для мереж наступного покоління, оскільки методи на основі правил не завжди дозволяють ефективно вирішувати зазначені завдання в мережах NGN.

Для швидкого усунення проблем OSS-система повинна мати у своєму складі кошти для своєчасного і гарантованого автоматичного оповіщення всіх зацікавлених і залучених до усунення можливої проблеми осіб при виявленні критичних подій ще до передачі події в систему контролю за усуненням несправності (Trouble Ticketing System). Також система контролю за усуненням несправності в NGN повинна мати деякі відмінності, наприклад, всю повну і детальну інформацію про проблему, що виникла, а також містити не тільки дані про статус картки контролю, а й дані про поточний стан вирішуваної проблеми в необхідної деталізації.

Існуючі підходи планування ґрунтуються на припущенні того, що мережі розвиваються повільно, циклічно, без різких раптових змін, і кожна послуга будується на базі конкретної технології. Планування починається зі створення плану розвитку мережі на основі ринкових прогнозів та тенденцій зміни ємності мережі. Після цього виконується поступове планування необхідних ресурсів кожного окремого шару технології, типу SDH/WDM чи IP/MPLS. Для такого підходу до планування характерно:

• планування виконується не автоматизованим способом або у різних незв'язаних (слабозв'язаних) системах;

• цикли планування тривалі, тому не можуть враховувати поточні зміни, внаслідок цього планування доводиться виконувати із «запасом», який знижує ефективність використання ресурсів для надання послуг;

• брак фактичних даних для розрахунків або неможливість їх використання, навіть якщо вони перебувають у суміжних автономних системах, які виробляють свої «оптимальні» плани.

В умовах NGN такі підходи малозастосовні, оскільки це дуже гнучка мережа, що швидко конфігурується і безперервно змінюється, яка призначена для надання багатьох різних видів послуг з використанням різноманітних різних технологій і механізмів.

Тому для NGN необхідна інтегрована система планування, здатна безперервно виконувати в єдиному замкнутому циклі довготривале, тактичне та поточне планування мережі для потреб управління ресурсами (Inventory Management), надання послуг (Fulfilment) та забезпечення (Assurance). У цих умовах для операторів особливо важливим стає правильно передбачити впровадження відповідних компонентів OSS-систем вже на етапі розробки концепції побудови мережі з використанням технологій NGN.

ETSI у своїх стандартах для мереж NGN визначив ділові та операційні, а також функціональні та архітектурні вимоги до OSS-системи та її компонентів, тим самим описавши основні проблеми, що стоять на шляху впровадження OSS для NGN та заклавши основу для їх вирішення. Дуже важливим є те, що впровадження нових NGN-послуг вимагає впровадження не лише нових телекомунікаційних технологій, а й серйозного реінженірингу експлуатаційних процесів. Виходячи з цього, ETSI розглядає методологію TM Forum New Generation Operations Systems and Software (NGOSS) як найбільш ймовірну основу, яка може забезпечити успішну реалізацію OSS-систем для NGN-мереж [98].

TM Forum, починаючи з 2001 р., у рамках методології NGOSS розробляє для мереж нового покоління багато рекомендацій щодо ефективного управління в процесі надання послуг, визначаючи технологічні напрями та підходи розвитку OSS/BSS. В основі методології NGOSS – перехресне використання двох підходів, що лежать в основі управління життєвим циклом NGOSS:

• «Plug and play» – компонентна архітектура, яка є специфічною формою SOA, в результаті дозволяє дуже швидко створювати нові сервіси шляхом динамічного комбінування компонентів, що повторно використовуються. Це має забезпечити скорочення часу на розробку, а також зниження витрат на впровадження та тестування нових послуг.

• архітектура MDA (Model Driven Architecture), що керується моделлю, що дозволяє специфікувати рішення у вигляді абстрактної моделі з можливістю подальшої автоматизації генерації програмного коду.

Дана методологія реалізована у вигляді пакета загальноприйнятих у телекомунікаційній індустрії специфікацій та рекомендацій, що спирається на чотири взаємопов'язані між собою компоненти:

- eTOM – мапа бізнес-процесів;
- SID – пов'язана з eTOM бізнес-процесами корпоративна інформаційна модель;
- TAM (Telecommunications Applications Map) – пов'язана з eTOM бізнес-процесами карта додатків;
- набір рішень щодо інтеграції та впровадження мережевих рішень – TNA (Technology Neutral Architecture), SOA та ін.

Ключовий елемент цієї методології-eTOM, тому що він є стартовою точкою для оператора зв'язку при проведенні робіт з реінженірингу його бізнес-процесів та створення структурної моделі бізнес-процесів. Створення, а потім уважний аналіз цієї моделі дозволить оператору визначити найбільш критичні зони, з яких потрібно починати будувати власну систему OSS. Створена структурна модель буде використана і для визначення бізнес-вимог до системи OSS, що будується.

У більшості випадків оператори розглядають та оцінюють лише функціональну частину OSS-додатків. При цьому не береться до уваги, що ПЗ постачальника OSS-додатків, як правило, значною мірою не відповідає моделі бізнес-процесів конкретного оператора. Тому саме додаток, що впроваджується, повинен мати серйозні можливості з адаптації до бізнес-процесів оператора. При цьому необхідно уникнути й іншої крайності, коли реалізована у додатку модель бізнес-процесів має бути повністю змінена відповідно до вимог оператора. Вирішенню цих суперечностей допомагає те, що зараз більшість провідних виробників систем OSS/BSS беруть участь у розробках TMF і в будь-якому випадку хоча б декларують відповідність свого ПО eTOM.

Аналогічні аргументи можна навести і на користь використання загальної інформаційної моделі SID, яка має безпосередній зв'язок зі структурною моделлю eTOM. Використання моделі SID дозволить більш легко і правильно визначити функціональні та інтеграційні вимоги до створюваного рішення і на цій основі створити необхідні моделі даних для програм, що впроваджуються.

Важливим фактором для інтеграції додатків, що використовуються для побудови OSS-системи, а також для керування взаємодією цих додатків для автоматизації конкретних бізнес-процесів, є відповідна архітектура OSS-системи. Тут найперспективнішим підходом є використання архітектури SOA. Ця архітектура використовує кілька технологій (інтеграційна шина, шина повідомлень, сервісна шина, шина даних та ін) і дозволяє виконувати обмін повідомленнями, перетворення даних, маршрутизацію та узгодження сервісів. При цьому з'являється можливість гнучкого управління користувальницькими послугами за рахунок повторного використання

сервісів та зміни бізнес-процесів їх надання переважно шляхом конфігурування замість програмування.

Після того, як на зміну інтеграційній шині (Enterprise Application Integration – EAI) прийшла технологія сервісної шини (Enterprise Service Bus – ESB), архітектура SOA отримала на ринку систем OSS значне визнання. SOA на основі інтеграційного програмного забезпечення з однорідним інтеграційним середовищем (на базі сервера додатків) вже використовується провідними постачальниками для об'єднання своїх OSS-додатків у єдину OSS-систему. Але операторам доводиться при побудові своїх OSS-систем використовувати з тих чи інших причин OSS-продукти різних постачальників, а також інтегрувати програми, що вже працюють, з новими. Тому доводиться будувати архітектуру SOA для інтеграції різноманітних інтегрованих додатків з використанням іншого інтеграційного ПЗ. Крім того, виявилося, що суто синтаксичної сумісності даних (сумісність форматів) для успішного використання переваг архітектури SOA недостатньо, що також необхідна сумісність на семантичному рівні, тобто однакове розуміння всіма сторонами елементів даних, якими вони обмінюються. Так з'явилося поняття сервісів даних та шини даних (Enterprise Data Bus – EDB), через які вони взаємодіють. Для перетворення потоків даних EDB може імпортувати та використовувати загальну інформаційну модель, наприклад, SID. Розвитку EDB зараз приділяється першочергова увага. Вважається, що EDB допоможе SOA стати високоефективною та загальнодоступною технологією.

Таким чином, з'явившись як засіб підвищення ефективності управління телекомунікаційними ресурсами, сучасні OSS-системи стають засобом, без якого в мережах нового покоління неможливе надання послуг. Для реалізації повнофункціональної OSS-системи потрібний значний набір компонентів від різних виробників та виконання великого обсягу інтеграційних робіт. Для успішного вирішення цих завдань необхідно спиратися на стандарти, рекомендації та методології в галузі створення, управління та підтримки експлуатації телекомунікаційних мереж (TMF, ITU-T, TISPAN та ін.), від початку закладати можливості інтеграції, віддаючи перевагу рішенням, що відповідають міжнародним стандартам і підтримує відкриті інтерфейси. Такий підхід також має бути основою для створення передінтегрованих рішень або їх складових частин, оскільки це впливає на тривалість проекту і пов'язані з ним витрати.

### 7.3. Система моніторингу та автоматизація обробки інциндентів

IT-інфраструктура постійно ускладнюється. Весь цей динамічно змінний і зростаючий комплекс обчислювальних систем, мереж зв'язку та систем життєзабезпечення необхідно підтримувати та обслуговувати. І це завдання без засобів автоматизації вирішити неможливо. Засобом автоматизації ручної праці у разі є OSS-системы. Ця абревіатура поєднує кілька класів систем і, як правило, взаємодіє з різного роду аналітичними системами класу BI для

отримання зведеної картини того, як функціонування IT-інфраструктури впливає на конкретні бізнес-процеси підприємства. Ці аналітичні системи показують, що саме необхідно змінити IT-інфраструктуру, щоб оптимізувати діяльність підприємства, і допомагають оцінити, наскільки якісні послуги надаються кінцевому споживачеві.

Одним з важливих класів систем для OSS є Fault Management & Trouble Ticketing – реєстрація та управління несправностями [99,100]. Вони дають змогу ефективно управляти планами робіт, а також оптимізувати роботу персоналу. Скорочення термінів ремонтних робіт, що досягається при його впровадженні, дозволяє компанії працювати значно оперативніше. Принцип дії Trouble Ticketing – це збирання та систематизація інформації про всі проблеми і неполадки, що виникають, крім того, збереження даних про спосіб їх усунення та поточний стан робіт. За допомогою систем класу Fault Management створюються системи для управління телекомунікаційними ресурсами. Нерідко Fault Management інтегрується із Help Desk [101]. За оцінками експертів, впровадження систем такого класу дозволяє суттєво зменшити їх повну вартість володіння (Total Cost Ownership – TCO).

Крім перерахованих класів, до сучасної OSS-системи входить безліч інших модулів. Це управління інвентаризацією (Inventory Management), що дозволяє автоматизувати планування поповнення запасів і забезпечити наочність, суворий контроль та облік однойменних ресурсів телекомунікаційного оператора, і навіть управління продуктивністю (Performance Management), призначений оптимізації роботи телекомунікаційної мережі. Ще в OSS-системах є модулі для управління замовленнями (Order Management), а також аналітичні модулі для планування та розвитку послуг (Network & Service Provisioning Management) та WorkFlow-системи, призначені для управління територіально-розподіленими командами співробітників. Кошти WorkFlow Management забезпечують також моніторинг та складання аналітичних звітів у режимі реального часу.

Аналітики розрізняють кілька можливих варіантів побудови OSS-системи для підприємства. Але так чи інакше, кожен варіант передбачає інтеграцію різних класів систем з іншими інформаційними системами та/або класами. Наприклад, це може бути Fault management & Trouble ticketing + SLA management + CRM, або Fault management + Inventory + Help Desk + контакт-центр + CRM, а також інші варіанти. Кожна комбінація забезпечує вирішення завдань певного класу, найбільш критичного для бізнесу замовника. Вибір робиться з урахуванням комплексного аналізу всіх бізнес-процесів підприємства.

### 7.3.1. Автоматизація обробки критичних аварій службою моніторингу

Телекомунікаційні оператори та Інтернет-провайдери керують IT-інфраструктурою, яка складається з тисяч та десятків тисяч пристроїв. Це мережні маршрутизатори, комутатори, МСЕ, сервери, СЗД, елементи

віртуальної інфраструктури, БС, точки доступу, кондиціонери, дизель-генератори, блоки безперебійного живлення та інше спеціалізоване технологічне обладнання.

Моніторинг та управління такою інфраструктурою – досить складне завдання та вимагає від служб технічної підтримки та обслуговування професійної та злагодженої роботи. Одне з основних завдань служби моніторингу – оперативне виявлення збоїв у роботі обладнання та якнайшвидше залучення профільних фахівців для відновлення штатного режиму роботи обладнання та систем [102].

Для автоматизації цього досить трудомісткого процесу потрібний відповідний інструментарій [103]. Як такий інструментальний засіб і пропонується Orion CRL, який інтегрується з системами моніторингу, управління інцидентами, управління мережею, інвентаризації, CRM, Service Desk, IVR (Interactive Voice Response), контакт-центром та прискорює обробку критичних аварій, що дає додаткові можливості для проведення базової діагностики та підвищує ефективність роботи служби моніторингу (рис.7.4.).

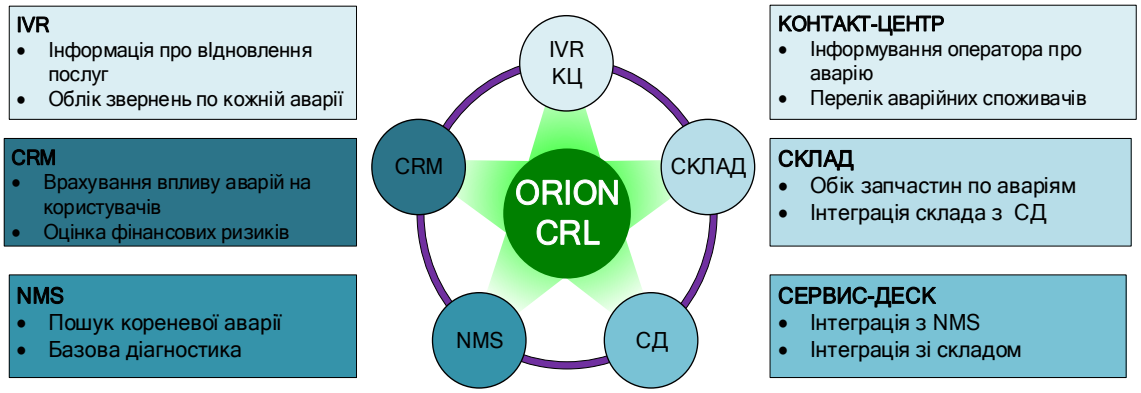



Рис. 7.4. Інтеграція Orion CRL із системами різних класів

### 7.3.2. Інтеграція з сервіс-деск та системою інвентаризації

Для реєстрації наряду на роботи оператор служби моніторингу використовує інформацію із системи моніторингу (код аварії, опис, hostname). Роботи з усунення аварії передбачають збір інформації про адресу розташування збійного елемента, артикулу та серійний номер обладнання та обладнання, що вийшло з ладу на заміну, контакти фахівців задіяних підрозділів (рис.7.5). Звичайно виникає необхідність вести облік використаного обладнання при відновлювальних роботах за тим чи іншим інцидентом. Коректна інформація з деталями аварії значно прискорює роботу внутрішніх служб, а автоматизація процесу підготовки таких даних підвищує ефективність задіяних підрозділів.

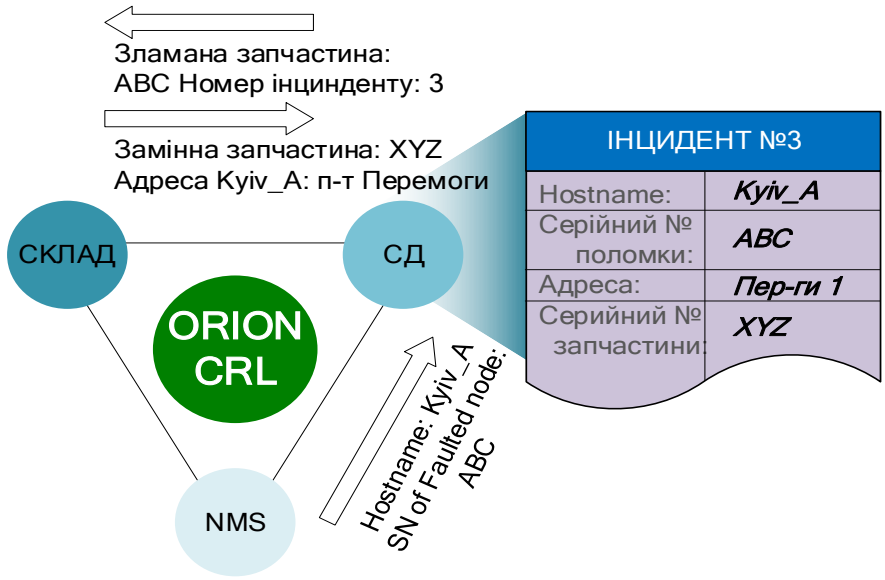



Рис. 7.5. Інтеграція Orion CRL з сервіс-деск та системою інвентаризації

Інтеграція Orion CRL із системою сервіс-деск автоматизує збір та перенесення інформації із системи моніторингу у форму реєстрації інциденту та розширює контекстне меню системи моніторингу додатковими можливостями з реєстрації інциденту. Оператор із контекстного меню системи моніторингу може зареєструвати інцидент та автоматично перенести в реєстраційну форму код аварії, опис, назву елемента та іншу інформацію із системи моніторингу.

Інтеграція Orion CRL із системою інвентаризації доповнює інцидент інвентарними даними, адресою об'єкта інсталяції та супутньою інформацією.

### 7.3.3. Інтеграція з IVR та контакт-центром

Окремим складним завданням при обробці аварій у мережі є обслуговування споживачів. У контексті обслуговування клієнтів завданням технічних підрозділів є забезпечення операторів контакт-центру, необхідної для обслуговування споживачів інформації. Насамперед – це інформація про наявність проблеми та орієнтовні терміни її усунення. Інтеграція з Orion CRL створює механізм передачі даних із системи сервіс-деск у контакт-центр, де оператор володітиме інформацією щодо впливу аварій на надання послуги споживачеві.

Наступним завданням є облік користувачів, які звернулися зі скаргами. Облік та диференціація звернень щодо аварій дозволяє точніше оцінити фінансові та репутаційні ризики для кожної аварії. Також перелік аварійних звернень може бути використаний для інформування споживачів про відновлення надання послуг.

Orion CRL виконує контроль та облік звернень споживачів по кожній аварії, а інтеграція Orion CRL з сервіс-деск, IVR та контакт-центром дає додаткові можливості для обслуговування споживачів та аналізу якості послуг (рис.7.6).

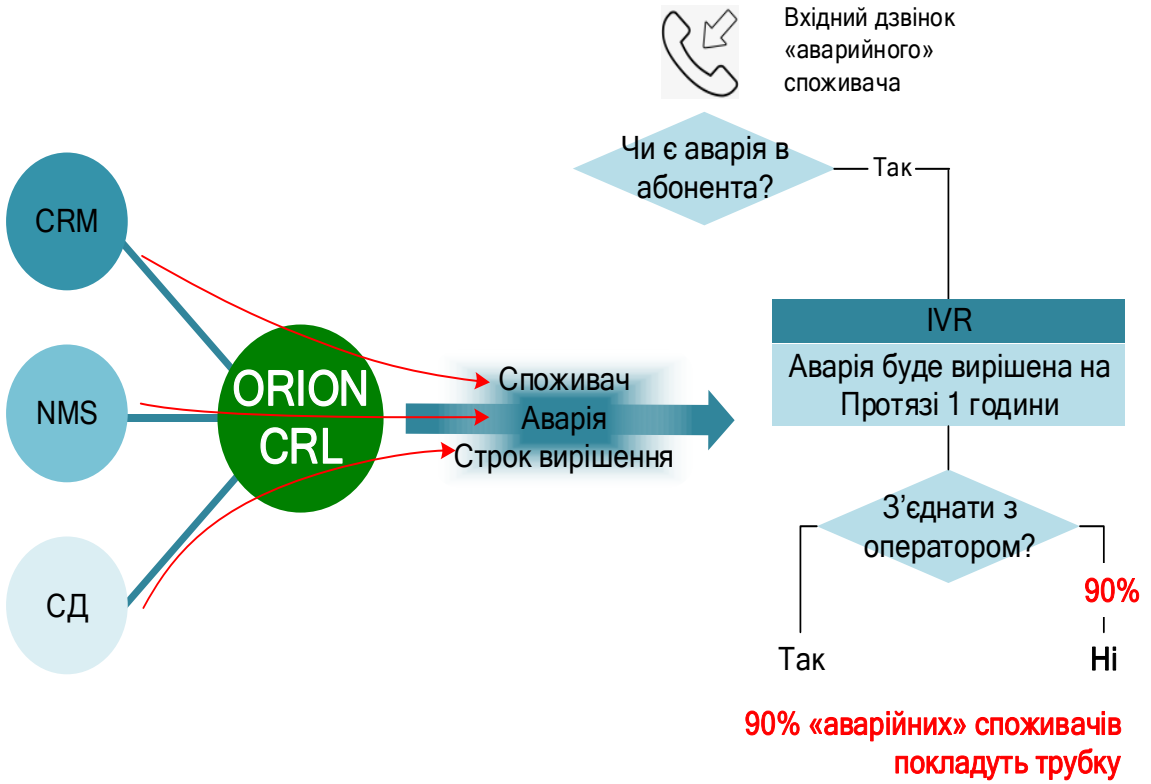



Рис. 7.6. Інтеграція Orion SRL з сервіс-деск, IVR та контакт-центром

Оцінка Orion CRL впливу інциденту на споживачів дозволяє відокремити вхідні дзвінки «аварійних» споживачів, а інтегрувавшись із сервіс-деск, Orion CRL передасть у IVR інформацію про плановий час усунення аварії. Це дозволяє автоматично обробляти «аварійні» звернення за окремим сценарієм IVR, зменшити навантаження на операторів контакт-центру, зберегти лояльність споживачів, інформуючи їх про актуальний стан відновлення послуги.

Orion CRL формує список «аварійних» споживачів, надає IVR очікуваний час усунення аварії, розвантажує операторів контакт-центру і, як наслідок:

- можливість аналітики критичності аварій;
- підвищення точності оцінки фінансових та репутаційних ризиків;
- облік та аналіз звернень споживачів щодо інцидентів;
- інформування оператора контакт-центру про інциденти споживача;
- автоматизація сценаріїв IVR для обробки звернень під час активного збою.

### 7.3.4. Автоматизація базової діагностики та пошук кореневої аварії

Одиничний збій в інфраструктурі з десятками тисяч пристроїв призводить до одночасної сигналізації про збій кількома системами та супроводжується численними повідомленнями про аварію (рис.7.7).

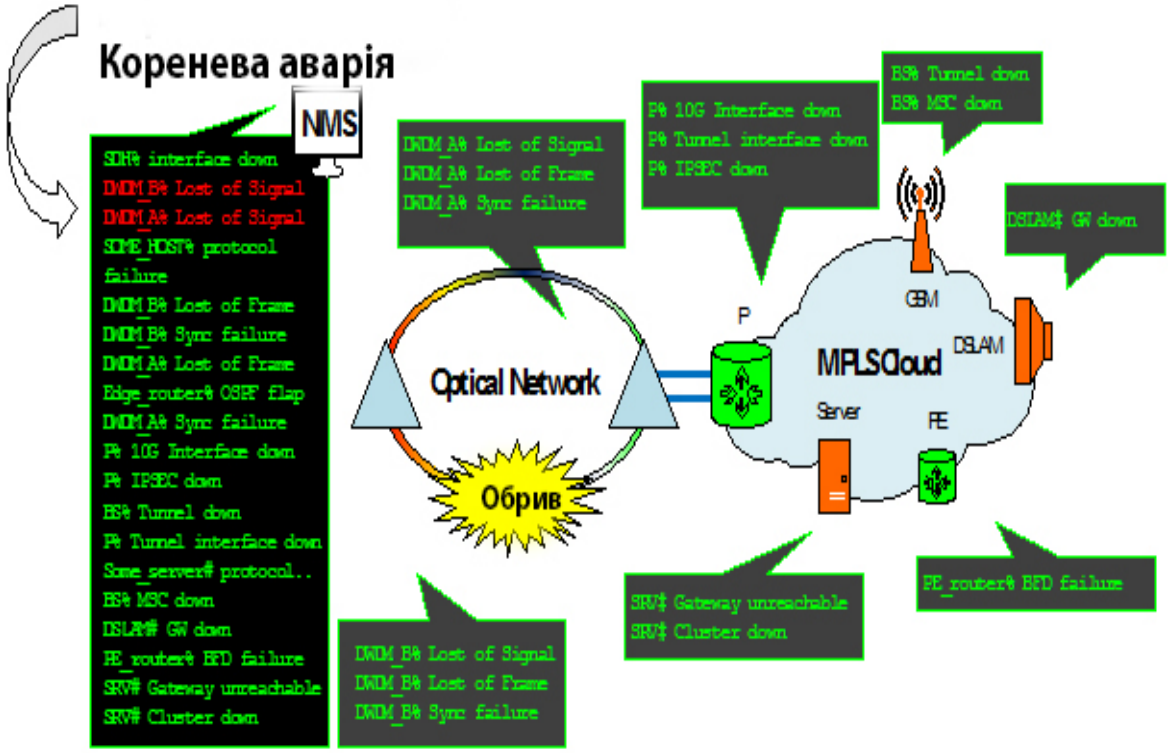



Рис. 7.7. Індикація повідомлень про аварію в системі моніторингу

Наприклад, при пошкодженні оптичної лінії зв'язку в системі моніторингу буде створено аварійну подію . Failure та Host Down для кожного елемента мережі в аварійному сегменті мережі. Ці аварії супроводжуються численними аваріями-симптомами типу BGP Neighbor Loss, OSPF Link Failure, Network/Node Unreachable та інші. Кількість аварійних повідомлень може налічувати від десятків до кількох сотень повідомлень на кожний інцидент.

Завданням служби моніторингу є оперативне виявлення з потоку аварійних повідомлень, що стосуються кореневої аварії, та залучення відповідної технічної служби для її усунення.

Хибна діагностика чи помилкова реєстрація інцидентів призводить до втрат часу, затягує вирішення проблеми та відволікає фахівців від вирішення інших актуальних питань та завдань. Для підвищення ефективності діагностики розроблено оригінальний алгоритм аналізу та пошуку кореневої аварії – RCA. Робота алгоритму базується на аналізі топології мережі та отриманих системою моніторингу аварій типу Host Down, Host Up, Link Down .

Алгоритм передбачає проведення базової діагностики, виконання типових операцій перевірки аварії на типових для IT-інфраструктури організації процедур відновлення. Завдяки інтеграції із системою моніторингу RCA визначає ключову подію та події-симптоми, а Orion CRL маскує аварії-симптоми та підсвічує кореневу аварію в системі моніторингу.

Orion CRL звертає увагу оператора служби моніторингу на подію, визначену як кореневу, пройшла базову перевірку та надає оператору додаткову інформацію для прискорення залучення профільних технічних підрозділів. Оператору служби моніторингу залишається візуально переконатися у правильності аналізу та розпочати реєстрацію наряду на роботи.

Таким чином, Orion CRL надає такі можливості:

- інтеграція з сервіс-деск та системою інвентаризації для прискорення реєстрації інциденту в системі сервіс-деск;
- інтеграція сервіс-деск із системою моніторингу та складським обліком для автоматизованого обміну інформацією;
- інтеграція з IVR та контакт-центром для формування бази «аварійних» споживачів та обліку звернень споживачів щодо кожного інциденту;
- автоматизація базової діагностики та пошук кореневої аварії за допомогою алгоритму RCA для прискорення діагностики та оптимізації роботи системи моніторингу.

Отже, час виявлення точки збою чи відмови, визначення відповідального технічного підрозділу та підготовка необхідної інформації для подальшої роботи щодо усунення аварії – ключові показники ефективності роботи служби моніторингу. А автоматизація типових операцій базової діагностики та перевірки аварій прискорює відновлення працездатності обладнання та економить робочий час операторів.

# ВИСНОВКИ

В результаті дослідження проблем аналізу інформації від різних джерел визначено, що основними серед них є проблеми, пов'язані з постійним розвитком та трансформацією об'єктів інтересу, обмеженістю можливостей кожного з видів інформаційних джерел, великим обсягом даних, обмеженим ресурсом, зростаючими вимогами до форм подання інформації, зростаючими вимогами до достовірності та повноти інформації. Зазначені проблеми постають на різних етапах виконання завдань, особливо під час узагальнення даних.

Доведено, що методологічна основа системного зведеного аналізу інформації від різнотипних джерел має базуватися на математичному інструментарію ТСДШ. Перетворення первинних даних і робота з гіпотезами за допомогою методів ТСДШ надають всі можливості забезпечити споживача обґрунтованими матеріалами для прийняття рішень.

Для впровадження в практику повсякденної діяльності нової методологічної схеми системного зведеного аналізу інформації від різнотипних джерел вирішена ціла низка наукових та науково-технічних завдань.

Розроблені та обґрунтувані схеми процесів формування і дослідження гіпотез на базі soft data & hard data, а також правила для зведеного аналізу даних. Розроблені архітектура та алгоритмічне забезпечення системного зведеного аналізу інформації. Запропоновано підходи до оцінки ефективності системи зведеному аналізі інформації від різнотипних джерел при вирішенні фахових завдань.

Система зведеного аналізу РІ має базування на відкритих стандартах і специфікаціях, принципах зрозумілості даних/сервісів для користувачів, можливості удосконалення ресурсів системи шляхом залучення до цього процесу всіх учасників системи; забезпечення своєчасного доступу до інформаційних ресурсів; захисту інформації; спільного підтримання системи користувачами в робочому стані в процесі її експлуатації; самоорганізація користувачів для внесення інформаційного вкладу в систему; мінімальні витрати на централізоване управління.

Для вирішення зазначених вище проблем запропановано створити систему зведення РІ на основі SOA-архітектури. Інтеграція здійснюється в декілька етапів на різних рівнях оброблення інформації, а безпосередній процес інтеграції описується з використанням однієї з відомих моделей інтеграції – JDL.

Для того щоб процес інтеграції був ефективним, алгоритми оброблення інформації мають оперувати наборами даних різнорідних джерел, крім того, результати роботи повинні у контрольних точках збігатися з еталонними значеннями та корелюватися. Для того щоб сформувати набір реалістичних

даних, визначених у контрольованому середовищі, вихідні дані слід збирати під час тренувальних вправ та навчань.

Сучасні методи інтеграції базуються на тому, що об'єктивна інформація описується в результаті розподілу ймовірностей, а суб'єктивна інформація інтерпретується як оцінка ймовірностей (у термінах ймовірнісної логіки). Проте багато видів СІ є непридатними для ймовірнісної інтерпретації. Інші види інформації з суб'єктивних джерел є суто якісними (експертне або нечітке оцінювання, міркування, здогадки), тому для них можуть бути застосовані методи нечіткої логіки, теорія свідчень, теорія парадоксальних суджень та інші.

Досліджені сучасні інформаційно-коммунікаційні технології і практичні питання їх застосування для розв'язання задач системного зведеного аналізу інформації від різнотипних джерел на основі сучасного математичного апарату.

Доведено, що використання даних з усіх можливих джерел, застосування інформаційно-телекомунікаційних технологій, а також запропонованої технології аналітичної обробки різнотипної інформації та інструментального засобу її автоматизації – дають змогу значно збільшити обсяг оброблюваної інформації, ефективність аналізу, покращити якість аналітичної обробки та як наслідок підвищити достовірність її результатів.

Розроблено оригінальний алгоритм аналізу та пошуку кореневої аварії (RCA), робота якого базується на аналізі топології мережі та отриманих системою моніторингу аварій типу Host Down, Host Up, Link Down для підвищення ефективності діагностики. А також інструментальній засіб моніторингу та автоматизації обробки інциндентів в IT-інфраструктурі, який дозволяє значно прискорити пошук кореневої аварії за допомогою алгоритму RCA та суттєво підвищити ефективність роботи системи моніторингу.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Іващенко О.І., Курдюк В.Ф., Огарок А.П. Концептуальні засади адаптації розвідки Збройних Сил України відповідно до стандартів НАТО. *Наука і техніка Повітряних сил Збройних сил України*. 2019. № 2 (35). С. 33–38.

2. Оборонна реформа: системний підхід до оборонного менеджменту: монографія / А. Павліковський, В. Фролов, Ф. Саганюк та ін.; за заг. ред. д.військ.н. А. Сиротенка. Київ: НУОУ, 2020. 274 с.

3. Орлова В. Розвідувальний процес за поглядами воєнних фахівців НАТО. *Авторський курс Віктора Гвоздя.* 2020. URL: https://bintel.org.ua/nukma/rozviduvalnij-proces-nato/ (дата звернення: 09.07.2023).

4. Зайцев О.В. Обґрунтування вимог до системи інтеграції даних від різнотипних джерел для інформаційного забезпечення збройних сил. *Перспективи розвитку озброєння та військової техніки Сухопутних військ*: зб. тез доп. Міжнар. наук.-техн. конф. (м. Львів, 14–15 травня 2015 р.). Львів: АСВ, 2015. С. 142.

5. Зайцев О.В. Аналіз і моделювання процесу інтеграції різнорідної інформації в умовах невизначеності. *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту*: матеріали міжнар. наук. конф. Херсон: Видавництво ХНТУ, 2015. С. 68–70.

6. Зайцев О.В., Новохатній Ю.В. Використання технологій BIG DATA в системах інтегрування різнорідної інформації. *Історія, сучасність та перспективи розвитку Державної прикордонної служби України та охорони державного кордону*: тези Міжнар. наук.-практ. конф. (м. Київ, 26 травня 2015 р.). Хмельницький: Видавництво НАДПСУ, 2015. С. 247–249.

7. Зайцев О.В. Структурно-функціональна модель системи інтегрування інформації на основі технологій BIG DATA. *Моделювання та інформаційні технології*: зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України. 2018. № 84. С. 169–176.

8. Зайцев О.В. Модель оцінювання нечіткості гіпотез щодо стану об’єкта на основі інтегрованої різнорідної інформації. *Моделювання та інформаційні технології*: зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України. 2018. № 85. С. 157–165.

9. Зайцев О.В., Савченко Т.В., Глухов С.І. Модель інтеграції даних від різних інформаційних джерел на основі теорії свідоцтв. *Зб. наук. пр. Військового інституту Київського національного університету імені Тараса Шевченка*. К.: ВІКНУ, 2013. Вип. 43. С. 142–145.

10. Зайцев О.В. Модель комплексування інформації отриманої від різних джерел на основі теорії свідчень Демпстера-Шейфера. *Системи управління, навігації та зв’язку*. Полтава: Полтавський національний технічний університет імені Юрія Кондратюка, 2015. Вип. 1 (33). С. 100–102.

11. Зайцев О.В. Математичне забезпечення інтеграції даних сенсорної мережі на основі теорії свідчень. *Проблеми телекомунікацій (ПТ-2015):* IX Міжнар. наук.-техн. конф.: зб. матеріалів конф. К.: НТУУ "КПІ", 2015. С. 369–371.

12. Зайцев О.В. Використання Байєсової моделі в задачах агрегування інформації від різних джерел. *Інформаційні технології в моделюванні*: матеріали всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених (м. Миколаїв, 24–25 березня 2016 р.). Миколаїв: МНУ ім. В.О. Сухомлинського, 2016. С. 71–72.

13. Зайцев О.В. Методичний підхід до комплексного оцінювання інформації технічних засобів розвідки в інтервальній формі. *Зб. тез доп. Міжнар. наук.-техн. конф.* (м. Львів, 16–17 травня 2019 р.). Львів: НАСВ, 2019. С. 68–69.

14. Зайцев О.В., Новохатній Ю.В., Попов М.О. Використання багатовимірної моделі даних для вирішення задач інтеграції новітніх ГІС в існуючі інформаційні системи військового призначення. *Застосування космічних та геоінформаційних систем в інтересах національної безпеки та оборони*: зб. тез доп. IV міжнар. наук.-практ. конф. (м. Київ, 10 квітня 2019 р.). Київ: Національний університет оборони України імені Івана Черняховського, 2019. С. 52–53.

15. Попов М.О., Стефанцев С.С., Зайцев О.В. Когнітивний підхід до калібрування номінальних суджень аналітика розвідувальної інформації. *Національна безпека і оборона: методичний аспект*. 2022. № 2. С. 37–42.

16. Gross G., Rakesh N., Sambhoos K., Schlegel D., Shapiro S., Tauer G. Towards hard+ soft data fusion. *Proc. architecture and implementation for the joint fusion and analysis of hard and soft intelligence data*. 2012. P. 955–962. URL: https://www.researchgate.net/publication/235220494_Towards_hard_soft_data_fusion_Processing_architecture_and_implementation_for_the_joint_fusion_and_analysis_of_hard_and_soft_intelligence_data (дата звернення: 09.07.2023).

17. Popov M., Zaitsev O., Piestova I. A Method for Determining Priorities Between Competing Interval-Valued Estimates of Experts IEEE Xplore. 2019. URL: https://ieeexplore.ieee.org/document/8813681 (дата звернення: 12.08.2023).

18. Popov M., Zaitsev O., Stambirska R. et al. A correlative method to ranking sensors via information reliability criterion: interval-valued numbers case. *The International Workshop on Reliability Engineering and Computational Intelligence RECI2020:* Book of Abstracts of the Intern. Workshop (Zilina, 27–29 October 2020). Slovakia, 2020. P. 16.

19. Popov M., Zaitsev O., Stambirska R. et al. A method to ranking reliability of sensors of multi sensor system: interval-valued number case. *IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*. Kyiv, Ukraine, 2020. P. 395–398.

20. Popov M., Zaitsev O., Andreiev A. A Method for Combination and Ranking Hypotheses Under Conditions of Partial Uncertainty. *Proc. 6th International Symposium on Microwaves, Radar and Remote Sensing (MRRS)*. Kharkiv, 2020. P. 333–338.

21. Popov M., Zaitsev O., Stambirska R. et al. A Correlative Method to Rank Sensors with Information Reliability: Interval-Valued Numbers Case. *Studies in Computational Intelligencethis link is disabled*. 2021. Vol. 976. P. 275–291.

22. Зайцев О.В. Підхід до інтегрування інформації, отриманої від різних джерел, з урахуванням мета-знань. *Перспективи розвитку озброєння та військової техніки Сухопутних військ*: зб. тез доп. Міжнар. наук.-техн. конф. (м. Львів, 18–20 травня 2016 р.). Львів: НАСВ, 2016. С. 183.

23. Зайцев О.В., Стамбірська Р.Г. Моделювання процесу інтеграції різнорідної інформації в умовах невизначеності з використанням мультиагентного підходу. *Новітні технології – для захисту повітряного простору*: XI наук. конф. Харківською університету Повітряних Сил імені Івана Кожедуба: тези доповідей, (м. Харків, 08–09 квітня 2015 р.). Х.: ХУПС ім. І. Кожедуба, 2015. С. 326–327.

24. Popov M.O., Zaitsev O.V., Stambirska R.G., Alpert S.I., Kondratov O.M. Chapter 17 A Correlative Method to Rank Sensors with Information Reliability: Interval-Valued Numbers Case. *Reliability Engineering and Computational Intelligence (Studies in Computational Intelligence book series)*. 2021. Vol. SCI-976) / C. van Gulijk, E. Zaitseva (eds.). Springer International Publishing, 2021. P. 275–291.

25. Korobchynskyi M., Rudenko M., Dereko V., Zaitsev O., Kovtun O. Optimization of Data Preprocessing Procedure in the Systems of High Dimensional Data Clustering. *Intellectual Systems of Decision-Making and Problems of Computational Intelligence, ISDMCI'2022*: the international scientific conf. (Kiev, May 23–27 2022). Springer, Cham. P. 1–13.

26. Valiente M.-C., Machín R., Barriocanal E., Sicilia M.-A. An Ontology-Based Integrated Approach to Situation Awareness for High-Level Information Fusion in C4ISR. *Lecture Notes in Business Information Processing*. 2011. N 83. P. 513–527.

27. Лисецький Ю.М., Короленко І.Г. Аналітична обробка неструктурованої інформації. *Підготовка фахівців в умовах широкомасштабної збройної агресії рф проти України: проблеми та перспективи:* матеріали XXII наук.-метод. конф. (м. Київ, 23 листопада 2023 р.). Київ, 2023. С. 64.

28. Лисецький Ю.М. Концепція побудови системи комплексної аналітичної обробки різнотипної інформації. *Вісник воєнної розвідки*. 2023. № 77. С. 26–31.

29. Лисецкий Ю.М. Корпоративные системы хранения данных. Построение. *Управляющие системы и машины*. 2013. № 6. С. 68–71.

30. Лисецкий Ю.М., Козаченко С.В. Резервное копирование как инструмент защиты информации. *Математичні машини і системи*. 2019. № 2. С. 80–87.

31. Лисецкий Ю.М. Защита информации: системы резервного копирования. *System Analysis and Information Technologies SAIT-2014:* 20-th International conf. (м. Київ, 21–24 May 2018). Kyiv, 2018. P. 236–237.

32. Лисецкий Ю.М. Информационные технологии в обработке и хранении экономической информации. *Інформаційні технології, системний аналіз і моделювання соціоекологоекономічних систем:* зб. тез п'ятої міжнар. наук.-практ. конф. (м. Київ, 19–20 березня 2014 р.). Київ: Національний авіаційний університет, 2014. С. 79–81.

33. Лисецкий Ю.М., Середович Е.П. Software-Defined Storages as a Tool of Lower IT Infrastructure Costs. *Управляющие системы и машины*. 2019. № 4. С. 42–48.

34. GlusterFS Documentation. URL: http://gluster.readthedocs.io/en/latest/ (дата звернення 10.02.2024).

35. Лисецкий Ю.М., Бобров А.И. Опыт построения корпоративного центра обработки данных национального масштаба. *Математичні машини і системи*. 2008. № 6. С. 82–88.

36. Лисецкий Ю.М. Модели проектирования центров обработки данных. *Математичне та імітаційне моделювання систем. МОДС'2019*: Чотирнадцята міжнар. наук.-практ. конф. (м. Чернігів, 24–26 червня 2019 р.). Чернігів, 2019. С. 160–163.

37. Лисецький Ю.М. Інформаційні технології в управлінні та обробці інформації: монографія. Київ: ЛАТ&К, 2018. 268 с.

38. Лисецкий Ю.М. Комплексный подход к управлению данными. *Математичні машини і системи*. 2019. № 4. С. 93–99.

39. Подройко Е.В., Лисецкий Ю.М. Сетевые технологии: эволюция и особенности. *Математичні машини і системи*. 2020. № 2. С. 14–29.

40. Лисецкий Ю.М. Новые тенденции в построении корпоративной сетевой инфраструктуры. *Информационные процессы и технологии. Информатика-2014*: Седьмая междунар. науч.-практ. конф. (г. Севастополь, 22–26 апреля 2014 г.). Севастополь, 2014. С. 63–64.

41. Ульянов А.В. Мультиплексоры сетей OTN/DWDM. *Информационные технологии и телекоммуникации*. 2016. Т. 4, № 3. С. 85–94.

42. Лисецкий Ю.М., Бобров С.И. Исследование технологий широкополосного беспроводного доступа. *Informatics and computer technics problems. PICT-2014*: Proc. of the Third International conf. (Chernivtsi, 27–30 May 2014). Chernivtsi, 2014. P. 188–190.

43. Лисецкий Ю. М. Каналы связи как средство интеграции территориально распределенных структур. *Управляющие системы и машины*. 2014. № 4. С. 68–72.

44. Что такое WiMAX? Принципы работы WiMAX. URL: http://www.broadband.org.ua/tekhnologii-bystrogo-interneta/1311-chto-takoe-wimax-printsipy-raboty-wimax (дата звернення: 15.09.2023).
45. Лисецкий Ю.М., Бобров С.И. WiMAX – высокоэффективная беспроводная «последняя миля». *Моделювання та інформаційні технології. Спецвипуск. Інформаційні технології в енергетиці*: зб. наук. пр. Київ: Національна академія наук України, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2007. С. 21–29.
46. OFDMA. URL: http://www.gridcomm-plc.com/rus/ofdma.htm (дата звернення: 15.09.2023).
47. Scalable Orthogonal Frequency Division Multiple Access (SOFDMA or S-OFDMA). URL: https://www.techopedia.com/definition/9246/scalable-orthogonal-frequency-division-multiple-access-sofdma-or-s-ofdma (дата звернення: 15.09.2023).
48. Adaptive antenna systems. URL: https://ieeexplore.ieee.org/document/1448022 (дата звернення: 15.09.2023).
49. Non-Line of Sight (NLOS). URL: https://www.techopedia.com/definition/5077/non-line-of-sight-nlos (дата звернення: 15.09.2023).
50. Бобров С.И. Принципы проектирования корпоративных сетей. *Информационные технологии в энергетике*: материалы третьей научн.-практ. конф.: сб. науч. тр. К.: НАН Украины, Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, 2004. С. 34–37.
51. SmartPass Connect. URL: https://apkpure.com/smartpass-connect/com. junipernetworks.smartpassconnect (дата звернення: 15.09.2023).
52. Application Tracking. URL: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-application-tracking.html (дата звернення: 15.09.2023).
53. Configure Unified Access Control in Junos OS.URL: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-uac.html (дата звернення: 15.09.2023).
54. SSID – Service Set Identifier. URL: https://nettech.ua/news/ssid-angl-service-set-identifier (дата звернення: 15.09.2023).
55. Introduction to Software Defined Networks (SDN). URL: https://www.researchgate.net/publication/311479628_Introduction_to_Software_Defined_Networks_SDN (дата звернення: 15.09.2023).
56. Overview of RFC7426: SDN Layers and Architecture Terminology. URL: https://sdn.ieee.org/newsletter/september-2017/overview-of-rfc7426-sdn-layers-and-architecture-terminology (дата звернення: 15.09.2023).
57. Control and Data Planes. URL: https://networkdirection.net/articles/network-theory/controlanddataplane/ (дата звернення: 15.09.2023).
58. OpenFlow. URL: http://flowgrammable.org/sdn/openflow/ (дата звернення: 15.09.2023).

59. Open Networking Foundation (ONF). URL: https://www.sdxcentral.com/ listings/open-networking-foundation/ (дата звернення: 15.09.2023).
60. OPFLEX. URL: https://ipwithease.com/opflex/ (дата звернення: 15.09.2023).
61. Cisco ACI vs Cisco SD-Access. URL: https://www.trustradius.com/compare-products/cisco-application-centric-infrastructure-aci-vs-cisco-software-defined-access-sd-access (дата звернення: 15.09.2023).
62. Introduction to LISP and VXLAN – Scalable Technology Overlays for Switching. URL: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2016/pdf/ BRKRST-3045.pdf (дата звернення: 15.09.2023).
63. IS-IS vs OSPF. URL: http://prosto-seti.blogspot.com/2016/08/is-is-vs-ospf.html (дата звернення: 15.09.2023).
64. Cisco TrustSec. URL: https://www.cisco.com/c/dam/en/us/products/collateral/ security/identity-services-engine/at_a_glance_c45-726831.pdf (дата звернення: 15.09.2023).
65. Security Group Tagging Basics. URL: https://www.networkworld.com/ article/2224825/security-group-tagging-basics.html (дата звернення: 15.09.2023).
66. Cisco ISE Configuration for Cisco DNA Center. URL: http://www.unifiedguru.com/cisco-ise-configuration-for-cisco-dna-center/ (дата звернення: 15.09.2023).
67. What Is a WLAN Controller? URL: https://www.cisco.com/c/en/us/products/ wireless/wireless-lan-controller/what-is-wlan-controller.html (дата звернення: 15.09.2023).
68. Сравнение SD-WAN и традиционной архитектуры WAN. URL: http://blog.sedicomm.com/2017/07/18/sravnenie-sd-wan-i-traditsionnoj-arhitektury-wan/ (дата звернення: 15.09.2023).
69. OMP. URL: https://sdwan-docs.cisco.com/Product_Documentation/ vManage_Help/Release_17.2/Configuration/Templates/OMP (дата звернення: 15.09.2023).
70. Zero-Touch Provisioning. URL: https://www.cisco.com/c/en/us/td/docs/ switches/lan/catalyst3850/software/release/16-5/configuration_guide/prog/ b_165_prog_3850_cg/zero_touch_provisioning.pdf (дата звернення: 15.09.2023).
71. Лисецкий Ю.М. Особенности информационно-технологической инфраструктуры территориально распределенных организаций. «Інформаційні управляючі системи та технології: зб. тез 7-ї міжнар. наук.-практ. конф. (м. Одеса, 20–22 вересня 2017 р.). Одеса: Одеський національний морський університет, 2017. С. 143–45.

72. Немного о конвергентной (и гиперконвергентной) ИТ-инфраструктуре. URL: https://habr.com/company/it-grad/blog/281813/ (дата звернення: 15.09.2023).
73. Носкова А.И., Токранова М.В. Преимущество гиперконвергентных систем над облачными технологиями. *Интеллектуальные технологии на транспорте*. 2017. № 2. С. 47–51.
74. Введение в технологии FC и FCoE для сетевых инженеров. URL: https://www.slideshare.net/CiscoRu/fcfcoe (дата звернення: 15.09.2023).
75. Лисецкий Ю.М., Саблий Ю.В. Гиперконвергентная технология с открытым кодом. *Математичні машини і системи*. 2019. № 4. С. 49–55.
76. Mobile edge computing (MEC): What is mobile edge computing? URL: https://stlpartners.com/edge-computing/mobile-edge-computing/ (дата звернення: 17.09.2023).
77. Что такое Интернет вещей? URL: https://www.rbc.ru/trends/industry/ 5db96f769a7947561444f118 (дата звернення: 26.09.2023).
78. Анализ современных технологий виртуализации. URL: https://habr.com/company/southbridge/ blog/212985/ (дата звернення: 18.09.2023).
79. Детально про віртуалізацію: типи, переваги та рішення. URL https://onbiz.biz/about-virtualization/ (дата звернення: 18.09.2023).
80. Лисецкий Ю.М. Виртуализация: динамика развития и перспективы. *Information Control Systems and Technologies*: materials of the III International scientific-practical conf. (Odessa, 23–25 September 2014). Odessa, 2014. P. 271–273.
81. Лисецкий Ю.М., Татаренко М.А. Технологии виртуализации от Oracle. *Математичні машини і системи*. 2018. № 4. С. 34–43.
82. Что такое модель SaaS, ее преимущества и примеры. URL: https://www.kasper.by/blog/model-saas/ (дата звернення: 18.09.2023).
83. Лисецкий Ю.М. Облачная коммуникационная платформа по модели SaaS. *Informatio Control Systems and Technologies*: materials of the VIII International scientific-practical conf. (Odesa, 23–25 September, 2020). Odesa National Polytechnic University, 2020. С. 68–70.
84. Cisco Spark URL: https://www.cisco.com/c/dam/global/uk_ua/solutions/ spark/pdfs/CiscoSpark-service-aag.pdf (дата звернення: 18.09.2023).
85. Управляемые сервисы. URL: https://ko.com.ua/upravlyaemye_servisy_ 117807 (дата звернення: 18.09.2023).
86. Лисецкий Ю.М. Облачные технологии как основа виртуальных управляемых сервисов. Информационные управляющие системы и технологии. Проблемы и решения: монография / авт. кол.: В. Васянин, Г. Востров, В. Вычужанин [и др.]; под науч. ред. проф. В. Вычужанина. Одесса: Экология, 2019. 244 с.
87. Аналітичне моделювання SDN/NFV. URL: https://journals.nupp.edu.ua/ sunz/article/view/2324 (дата звернення: 18.09.2023).

88. What is the Internet of Things? WIRED explains. URL: https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot (дата звернення: 18.09.2023).

89. Лисецкий Ю.М., Калбазов Д.И. Технологии Internet of Things. *Математичні машини і системи*. 2019. № 2. С. 43–50.

90. Лисецький Ю.М. Глобальная сеть малой мощности для Интернета вещей. *Information Control Systems and Technologies*: materials of the VII International scientific-practical conf. (Odessa, 17–18 September 2018). Odessa, 2018. P. 96–98.

91. LPWA network technologies and standards: LPWAN wireless IoT guide. URL: https://www.i-scoop.eu/internet-of-things-guide/lpwan/ (дата звернення: 18.09.2023).

92. Лисецкий Ю.М. Развитие систем поддержки операционных процессов операторов связи. *Інфокомунікації – сучасність та майбутнє*: Третя міжнар. наук.-практ. конф. молодих вчених (м. Одеса, 17–18 жовтня 2013 р.). Одеса, 2013. С. 73–77.

93. Falge C. Präsentation: eTOM: Service Management & Operations. Hauptseminar: Neue Ansätze im IT-Service-Management-Prozessorientierung (ITIL/eTOM) / prof. Hegering, prof. Linnhoff-Popien. Munich, 2004. P. 9 –118.

94. Steinder M. A Survey of fault localization techniques in computer networks. *Science of Computer Programming*. 2004. N 53. P. 165–194.

95. Heller M. ITIL und eTOM-Konzepte im Vergleich. Hauptseminar: Neue Ansätze im IT-Service-Management-Prozessorientierung (ITIL/eTOM) / prof. Hegering, prof. Linnhoff-Popien. Munich, 2004. P. 132–154.

96. Лисецкий Ю.М., Куник А.А. Особенности систем поддержки операционных процессов для сетей нового поколения. *Інфокомунікації – сучасність та майбутнє*: Четверта міжнар. наук.-практ. конф. (м. Одеса, 30–31 жовтня 2014 р.). Одеса, 2014. С. 106–110.

97. NGOSS (New Generation Operations Systems and Software). URL: http://dpnm.postech.ac.kr/NGOSS/NGOSS.html (дата звернення: 18.09.2023).

98. Fault and Event Management. URL: https://www.nmsaas.com/solutions/fault/ (дата звернення: 18.09.2023).

99. What is a trouble ticketing system? URL: https://www.zoho.com/desk/trouble-ticketing-system.html (дата звернення: 18.09.2023).

100. Network fault management with an integrated helpdesk. URL: https://www.manageengine.com/network-monitoring/helpdesk-integration.html (дата звернення: 18.09.2023).

101. Steinder M. A Survey of fault localization techniques in computer networks. *Science of Computer Programming*. 2004. N 53. P. 165–194.

102. Лисецкий Ю.М., Калбазов Д.И., Тернавский В.О. Мониторинг и автоматизация работы с инцидентами. *Математичні машини і системи*. 2020. № 2. С. 80–86.

Наукове видання

Зайцев Олександр Вікторович, Попов Михайло Олексійович, Лисецький Юрій Михайлович.

**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМНОМУ ЗВЕДЕНОМУ АНАЛІЗІ ІНФОРМАЦІЇ ВІД РІЗНОТИПНИХ ДЖЕРЕЛ**

Монографія

Літературний редактор, коректор – Г.В. Галушкіна
Комп'ютерна верстка, макетування – А.О. Брем
Дизайн обкладинки – О.О. Старовойтенко
Технічний редактор – В.Ю. Бихун

Підп. до друку 01.03.2024. Формат 64x90/16.
Папір офсетн. Друк цифровий.
Ум. друк. арк. 14,98. Наклад 500 прим. Зам. № 25/12

Видавець Бихун В.Ю.
Видавництво «ЛАТ&К»
вул. Леонтовича, 9, к. 18, м. Київ, 01054
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
ДК № 5366 від 26.06.2017 р.
тел./факс: +38 044 235 000 9
моб.: +38 050 310 22 04
e-mail: lk@ukr.net