УДК 004.04

Копійка О. В., к.т.н., (Державний університет телекомунікацій. +380442492923. okopiyka@gmail.com)

АРХІТЕКТУРА МЕРЕЖІ В СУЧАСНИХ ДАТА-ЦЕНТРАХ

Копійка О. В. Архітектура мережі в сучасних дата-центах. У статті розглядаються основні вимоги до проектування архітектури мережі IT інфраструктури корпорації. Архітектура мережі призначена для забезпечення надійним, масштабованим і доступним зв'язком на фізичному і логічному рівнях. Для того, щоб гарантувати додаткам належний рівень мережевої служби, архітектура мережі повинна проектуватися з урахуванням архітектури системи безпеки, яка встановлює певні вимоги на структурному (пристрої) і логічному рівнях (конфігурації). При проектуванні архітектури мережі були забезпечені наступні вимоги: доступність; безпека; масштабованість; керованість; підтримка; консолідація; інтероперабельність.

Ключові слова: IT інфраструктура, дата-центр, архітектура мережі, IT сервіси,система безпеки

Копейка О. В. Архитектура сети в современных дата-центрах. В статье рассматриваются основные требования к проектированию архитектуры сети ИТ инфраструктуры корпорации. Архитектура сети предназначена для обеспечания надежной, масштабируемой и доступной связью на физическом и логическом уровнях. Для того, чтобы гарантировать приложениям должный уровень сетевой службы, архитектура сети должна проектироваться с учетом архитектуры системы безопасности, которая устанавливает определенные требования на структурном (устройства) и логическом уровнях (конфигурации). При проектировании архитектуры сети были обеспечены следующие требования: доступность; безопасность; масштабируемость; управляемость; поддержка; консолидация; интероперабельность.

Ключевые слова: ИТ инфраструктура, дата-центр, архитектура сети, ИТ сервисы,система безопасности

Kopiyka O.V. Network architecture in the modern data centers. The article deals with the matters related to the main requirements to corporate IT infrastructure network architecture projecting. Network architecture is designed for reliable, scalable and available communication supply on physical and logical levels. In order to guarantee applications adequate level of network service, network architecture should be projected taking into account architecture security system which arranges certain requirements on structural (device) and logical levels (configurations). While projecting network architecture certain requirements were provided: accessibility, security, scalability, controllability, support, consolidation, interoperability.

Key words: IT infrastructure, data centers, network architecture, IT services, security system

1. Вступ і постановка завдання. В Україні вже 85 % підприємств малого та середнього бізнесу використовують той чи інший "хмаровий сервіс". І ця кількість буде зростати, так як сьогодні "хмарові технології" пропонують практично безлімітні ресурси бізнесу будь-якого розміру при вартості, яка непорівняння з капітальними інвестиціями у власну інфраструктуру. При реалізації концепції "хмарових сервісів" виникає завдання побудови Дата - центрів з сучасною архітектурою і наявністю повного обсягу сервісів.

У даній статті розглядається розвиток системної архітектури IT інфраструктури Корпорації, яка розвивається за рахунок створення власного дата-центру. Метою дослідження є вироблення стратегії розвитку системної архітектури IT інфраструктури на основі застосування передових методологій і концепцій провідних виробників апаратного і програмного забезпечення (HP , SUN , EMC , CISCO , Microsoft , ORACLE , Veritas) .

Основним завданням при цьому є розробка архітектур IT інфраструктури, які визначають фундаментальні принципи побудови IT сервісів і їх взаємозв'язок. Також на базі архітектур формуються вимоги до створення IT сервісів. Ми виділяємо наступні архітектури: управління; зберігання даних; додатків; мережі; безпеки.

Однією з найважливіших є архітектура мережі.

2. Взаємозв'язки між архітектурами. Призначення архітектури мережі – забезпечувати надійний, масштабований та доступний зв'язок з мережею на фізичному й логічному рівнях відповідно до вимог підприємства. Щоб гарантувати прикладним програмам належний рівень мережної служби, архітектура мережі має проектуватися з урахуванням архітектури системи безпеки, яка встановлює певні вимоги на структурному (пристрої) та логічному рівнях (конфігурації). У деяких випадках архітектура мережі може залежати від архітектури

системи керування. Наприклад, якщо система керування вимагає виділення окремої мережі для передачі даних для керування.

При проектуванні архітектури мережі слід забезпечити наступні вимоги:

2.1. Доступність. Необхідний рівень доступності мережі визначається вимогами прикладних програм, які нею користуються. Неможливо та навіть економічно не вигідно забезпечувати 100-відсотковий рівень доступності мережі. Краще визначити рівень доступності кожного пристрою мережі, спираючись при цьому на вимоги прикладних програм, які він має обслуговувати.

Зазвичай надлишковість, за допомогою якої підтримується високий рівень доступності мережі, досягається за рахунок використання таких елементів:

- *Надлишкові компоненти.* Самі пристрої можна розробляти так, щоб досягти надлишковості завдяки дублюванню їх внутрішніх компонентів.
- *Кластеризація "активний-активний" або "активний-пасивний".* Коли застосовуються механізми кластеризації, в архітектурі можна запровадити по два мережних пристрої кожного типу для підтримки високого рівня доступності мережі.
- *Пристрої або сервери "гарячого" резерву.* У мережі можна запровадити надлишкові маршрутизатори, комутатори та брандмауери. Таким чином, у мережі не буде жодного пристрою, який зможе спричинити глобальний перебій. Коли перебій станеться в роботі брандмауеру, вручну буде введений в дію резервний брандмауер. Якщо перестане працювати комутатор (а він використовується спільно з групою мережних адаптерів, як описується нижче), інший комутатор візьме на себе повне навантаження, допоки перший не буде відремонтовано або замінено.
- *Групи мережних адаптерів на хостах.* За допомогою групи мережних адаптерів на одному хості створюють два мережних порти. Кожен порт фізично зв'язаний з окремим комутатором, а комутатори застосовують протокол резервного копіювання (протокол залежить від обладнання постачальника, яке використовується). Окрім того, драйвер мережного адаптера хоста забезпечує керування портами як одним логічним пристроєм. Коли один порт мережного адаптера виходить з ладу, хост продовжує підтримувати зв'язок через функціонуючий порт, а якщо припиняє працювати комутатор, усі хости продовжують обмінюватися даними через мережний адаптер, з'єднаний з функціонуючим комутатором.

2.2. Безпека. Як зазначалося в попередньому розділі, при проектуванні мережі треба брати до уваги вимоги до безпеки і продуктивності. Працівники організації, котрі відповідають за безпеку, повинні визначити зони безпеки, яких слід дотримуватися при проектуванні мережі.

- *Множинна адресація (Multihoming).* Сервери підприємства можуть оснащатися кількома мережними адаптерами. Це робиться, зокрема, для того, щоб відділити потоки даних, які йдуть до інтернет-клієнтів, від внутрішніх потоків даних, а також для підтримки відповідного рівня продуктивності (два потоки даних можуть перевантажити один мережний адаптер, а два адаптери добре з ними упораються) або захисту. Множинна адресація серверів передбачає застосування на одному сервері кількох мережних адаптерів або кількох IP-адрес (в останньому випадку сервер може мати один або кілька адаптерів). Ми розглядатиметься тільки застосування кількох мережних адаптерів (що, в свою чергу, передбачає використання багатьох IP-адрес).
- *Обмеження безпеки.* Оскільки обладнання мережі контролює передачу інформації в межах організації та до Інтернету, воно має підтримувати функції, призначені для впровадження обмежень безпеки. Пристрої, що складають мережу, повинні надавати такі можливості: щонайменше *автентифікацію* та перевірку паролю користувача для віддалених адміністраторів; в оптимальному варіанті – *шифрування даних*, що передаються з метою адміністрування та моніторингу.
- *Списки контролю доступу.* Списки контролю доступу (Access Control List — ACL) можна застосовувати для хостів або сегментів мережі. Застосування їх до мережних

пристроїв дозволяє контролювати, які дані можуть передаватися до певних локальних та віртуальних локальних мереж.

• *Облікові записи служб.* Коли для забезпечення функціональності мережі використовуються сервери, всі облікові записи служб (service accounts) мають бути локальними, а не доменними. Імена та паролі в облікових записах повинні відповідати рекомендаціям про присвоєння паролів, визначеним політикою безпеки організації.

• *Мережна автентифікація.* Автентифікація в мережі проводиться з метою перевірки того, що користувачі, які намагаються підключитися до мережі, є саме тими, за кого себе видають. Ця функція зазвичай використовується в мережах, де: *важко* контролювати фізичний доступ до точок мережі; *клієнти* отримують віддалений доступ за допомогою служб віддаленого доступу (наприклад, у віртуальних приватних мережах); *застосовується* безпровідний зв'язок. Для автентифікації застосовують такі засоби, як смарт-карти, біометричні данні, протокол IPSec і сервер Internet Authentication Server (IAS), а у випадку безпровідного зв'язку – автентифікацію 802.x.

• *Шифрування даних у мережі.* Шифрування потоків даних у мережі забезпечує захист проти зловмисного перехоплення та декодування кадрів даних. До традиційних методів шифрування належать стандарти DES (Data Encryption Standard) та 3DES, що входять до пакету IPSec, а також стандарт MPPE (Microsoft Point-to-Point Encryption — двоточкове шифрування Microsoft) для протоколу PPTP (Point-to-point Tunneling Protocol — протокол тунелювання типу точка-точка).

2.3. Масштабованість. При реалізації мережі потрібно застосовувати інтелектуальні мережні пристрої, щоб адміністратори мережі могли її масштабувати в разі зростання вимог до пропускної здатності дата-центру та мережі. Складні мережні пристрої можуть виконувати інтелектуальну маршрутизацію та фільтрування пакетів, завдяки чому здійснюється ефективне переміщення пакетів, часто майже зі швидкістю мережі (wire speed). Мережні пристрої та сервери мають бути здатними підтримувати швидкості роботи портів від 10 Мбіт/с до 10 Гбіт/с, як визначається вимогами до пропускної здатності середовища. Для збільшення кількості портів для підключення пристроїв і серверів, що додаватимуться до середовища, можна застосовувати модульні комутатори.

2.4. Керованість. Важливість питань, пов'язаних з керованістю, привела до посилення і поглиблення зв'язків між бізнес-потребами та мережними операціями. Провідна мета менеджерів мережі — здійснити розподіл компонентів мережні між бізнес-процесами та змістити в бік бізнес-потреб фокус розробки метрик керування і правил обробки подій, призначених для виконання угод про рівень сервісу.

До основних завдань керування мережею належать: *поліпшення* якості служб; *зниження* вартості володіння; *зниження* загрози безпеці.

Для керування середовищем організації потрібні добре побудовані, гнучкі процеси, спрямовані на вирішення бізнес-завдань. Керування середовищем передбачає адміністрування, вирішення проблем та превентивну розробку інфраструктури з метою скорочення до мінімуму кількості проблем. Керування також передбачає визначення угод про рівень сервісу та перевірку дотримання належної якості служб.

• *Служби керування мережею.* Основними засобами, які використовують служби керування, є інструменти керування серверами, що дають можливість визначати продуктивність роботи мережі, збирати дані про події, складати звіти та поширювати повідомлення в мережі.

• *Системне адміністрування.* Необхідно забезпечити можливість віддаленого та безпечного керування через мережу кожним мережним пристроєм і сервером. Запроваджені в організації політики безпеки можуть передбачати лише локальне адміністрування. Проте взагалі рекомендується передбачити можливість безпечного віддаленого адміністрування.

Керування мережею має бути безпечним. Захист консолей керування передбачає фізичний захист пристроїв, застосування складних і довгих паролів та захист мережних

маршрутів, що застосовуються для керування. Вирішити проблему безпечного керування допомагають такі технології, як RADIUS або Secure Shell (SSH). Інші заходи з вирішення цієї проблеми передбачають запровадження шифрованих сеансів та застосування ізольованої мережі для керування. Ізольоване керування може передбачати фізичне виділення інтерфейсів для керування пристроями з усіх інших загальних маршрутизованих потоків даних у мережі та обмеження керівних потоків даних між хостами мережі. Якщо для керування застосовуються загальні мережні маршрути, наполегливо рекомендуємо вдаватися до шифрування керівних потоків даних.

Варіанти керування різняться залежно від пристроїв, обраних організацією. На певному етапі проектування треба прийняти рішення про те, чи потрібно проводити стандартизацію за якимось із протоколів керування. Зазвичай мережні пристрої підтримують такі протоколи керування: Telnet; Secure Shell (SSH); HTTP (Hypertext Transfer Protocol – протокол передачі гіпертексту) або HTTPS (Secure Hypertext Transfer Protocol – протокол захищеної передачі гіпертексту); FTP (File Transfer Protocol – протокол передачі файлів) або TFTP (Trivial File Transfer Protocol – найпростіший протокол передачі файлів); Syslog; SNMP (Simple Network Management Protocol — простий протокол керування мережею).

• *Інтегровані або виділені мережі керування.* Як зазначалося, проектування мережі передбачає також розробку політик безпеки організації. Часто механізм контролю за доступом діє між Інтернетом та внутрішніми користувачами. На рівні 3 та нижче він, як правило, реалізується у вигляді брандмауера з фільтрами портів TCP та/або UDP. Хоча такий підхід і дає можливість досягти вищих рівнів безпеки, тому що забезпечує контроль за проходженням потоків даних у мережі, він часто спричинює проблеми, коли потрібно виконати типові завдання з керування, наприклад віддалене адміністрування, резервне копіювання або відновлення. Багато організацій створюють окремі, або виділені, мережі для керування, що обслуговують операції, пов'язані із керуванням. Проте задля безпеки для такої мережі теж необхідні засоби контролю.

2.5. Продуктивність. Для того щоб спроектувати мережу з найвищою можливою продуктивністю, потрібно врахувати такі показники:

• *Швидкість роботи пристроїв.* Швидкість роботи пристрою залежно від його функції (як швидко він може виконувати маршрутизацію або фільтрування пакетів).

• *Швидкість мережі.* Швидкість мережних інтерфейсів та пристроїв зв'язку або серверних портів (наприклад 100 Мбіт/с або 1 Гбіт/с).

• *Фільтрування.* Тип фільтрування пакетів (перевірка пакетів вище рівня 3 моделі ОБІ) визначає необхідну потужність процесору. Чим вище рівень, на якому здійснюється фільтрування, тим ймовірніше погіршення продуктивності. У разі необхідності для відновлення рівнів продуктивності треба вводити додаткові центральні процесори.

• *Шифрування.* Застосування шифрування, наприклад у віртуальних приватних мережах, призводить до зниження продуктивності. Якщо навантаження, викликане шифруванням, виявляється надто відчутним і продуктивність стала нижчою за потрібну, пристроям, що виконують шифрування, необхідно виділити додаткові ресурси центральних процесорів, і продуктивність повернеться на належний рівень.

• *Кількість пристроїв.* Затримка в роботі мережі в цілому збільшується при зростанні в ній кількості пристроїв.

2.6. Підтримка. Основний аспект архітектури мережі, про який часто забувають, – це підтримка. Кожен пристрій, що вводиться в мережне середовище, спричиняє додаткові витрати, тобто збільшує повну вартість придбання та експлуатації мережі. Щоб знизити повну вартість придбання та експлуатації, необхідно визначити та придбати пристрої, конструкція яких передбачає мінімальні витрати, пов'язані з їх роботою.

Можливості підтримки можна розширити за допомогою: *інструментів* віддаленого адміністрування; *централізованої* віддаленої модернізації програмно-апаратного

забезпечення; *високого рівня* підтримки промислових стандартів; *інтеграції* із системою керування підприємства.

2.7. Консолідація. В організації, що постійно зростає, швидко збільшується кількість пристроїв. На кожному поверсі та в кожній серверній з'являються нові комутатори; керування одними з них здійснюється, а іншими – ні, одні забезпечують швидкість передачі 10 Мбіт/с, тоді як інші – більшу. Багато організацій спрямовують зусилля на стандартизацію та консолідацію, щоб уникнути хаосу в інфраструктурі мережі. У результаті цей процес може закінчитися вибором конкретного способу консолідації, два з них розглянемо нижче.

• ***Консолідація однакових ролей.*** Такий тип консолідації передбачає скорочення загальної кількості пристроїв з метою впровадження меншої кількості більш потужних пристроїв, які здатні виконувати певну роль за меншої кількості точок перебоїв. Комутатор – це ймовірний кандидат на такого роду консолідацію. Малопотужні некеровані комутатори можна видалити, замінивши їх більш потужним керованим комутатором. З появою потужних процесорів та мережних адаптерів з великою швидкістю передачі даних з'явилася можливість консолідувати складні мережні пристрої, такі як маршрутизатори, брандмауери і пристрої віртуальних приватних мереж (сервери віддаленого доступу).

• ***Консолідація різних ролей***. Межа між різними мережними пристроями або типами серверів поступово зникає. Наприклад, багато маршрутизаторів та комутаторів може виконувати функції брандмауерів або підтримувати служби віртуальних приватних мереж. Консолідація кількох компонентів у таких багатофункціональних пристроях або серверах допомагає знизити число пристроїв, якими потрібно керувати в середовищі, завдяки чому скорочуються загальні витрати на придбання та експлуатацію. Компанії можуть вдатися до застосування цього підходу, зваживши на такі міркування:

– *Адміністрування.* Контроль за роботою різних пристроїв або серверів можуть здійснювати декілька людей. Не завжди вдається розділити функції контролю за роботою багатофункціональних пристроїв так, щоб це відповідало структурі організації.

– *Більший фронт для нападу.* Коли функціональність багатьох «кінцевих» пристроїв (пристроїв, з'єднаних безпосередньо з Інтернетом) об'єднується, зростає загроза безпеці, оскільки такий пристрій більш вразливий для атак різного роду.

– *Менше варіантів оптимізації.* Наприклад, якщо функціональність віртуальної приватної мережі об'єднується з функціями маршрутизатора, втрачається можливість незалежного масштабування служб. Для функціональності віртуальної приватної мережі потрібне шифрування, виконання якого потребує ресурсів центрального процесора, і це може призвести до зменшення продуктивності маршрутизації. Якщо ж ці дві функції виконують окремі пристрої, продуктивність цих функцій можна оптимізувати окремо.

2.8. Інтероперабельність. Елементи архітектури мережі мають взаємодіяти між собою та з іншими компонентами інфраструктури. Необхідно забезпечити взаємодію на таких рівнях:

• *Фізичний.* Апаратура мережі має працювати з іншим мережним обладнанням; наприклад, вона має підходити до стандартних апаратурних стояків. Потрібно також враховувати вимоги до електричної напруги.

• *З'єднання.* Апаратне забезпечення мережі має забезпечувати відповідний рівень зв'язку, щоб відповідати іншим елементам мережі. Наприклад, воно повинно підтримувати з'єднання з використанням витої пари або волоконно-оптичного кабелю.

• *Протоколи.* Необхідна підтримка як протоколів рівня 2, так і протоколів рівня 3. Можливості взаємодії, які забезпечують виробники мережних пристроїв зазвичай досить значні. Майже всі виробники маршрутизаторів і комутаторів класу підприємства дотримуються опублікованих Робочою групою IETF (Internet Engineering Task Force) промислових стандартів. Мова йде, зокрема, про інформацію щодо конфігурації та протокол маршрутизації RIP (Routing Information Protocol). Багато опублікованих документів з серії RFC прийняті як стандарти виробниками апаратного та програмного забезпечення.

• *Керування.* Апаратне і програмне забезпечення мережі має взаємодіяти на рівні керування, щоб його можна було контролювати, настроювати на відстані та забезпечувати його якомога більш економну роботу. Якщо порівняти можливості керування в разі придбання обладнання від різних виробників та придбання цілої інфраструктури маршрутизації від одного виробника, то зазвичай переваги, які надає використання невеликих уніфікованих наборів інструментів і методик керування, спонукають підприємства користуватися послугами одного виробника, коли це можливо.

3. Приклад мережі передачі даних Корпорації в Україні. Для формування корпоративної мережі (інтранет), взаємодії з мережами партнерів (екстранет), а також підключення до Інтернет використовується технологія побудови VPN в IP/MPLS (Рис. 1).

Центри обробки даних (ЦОД) корпорації розміщуються в тих же містах , що і центральний і регіонально-транзитні вузли мережі передачі даних корпорації , і відповідно до них підключаються.

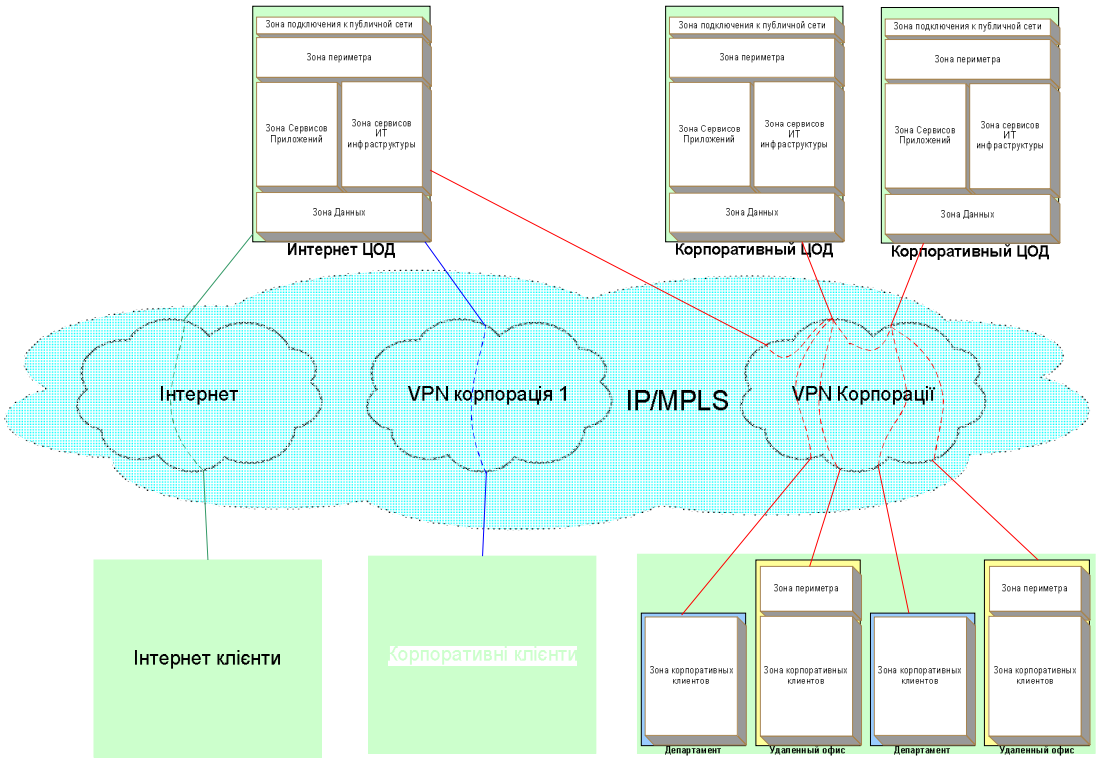

Рис. 1. Віртуальні приватні мережі в IP / MPLS мережі Корпорації

Мережі віддалених офісів і департаментів отримують доступ до ЦОД за допомогою Регіональних вузлів мережі передачі даних.

Мережа корпорації складається з 6-ти ЦОД, 2-х Інтернет ЦОД та 20-400 віддалених офісів з типовим набором автономного обладнання та систем. 1100-1400 мереж будуть включати тільки користувальницькі робочі станції.

Мережа корпорації логічно поділяється на зони безпеки за допомогою сервісу захисту периметра. У корпорації формується сім основних зон безпеки (Рис. 2). Центри обробки даних включають в себе наступні зони: *мережі* даних, *сервіс*ів ІТ інфраструктури, *сервісів* додатків, *периметра*.

Усі підрозділи корпорації, на території яких знаходяться робочі місця співробітників (апарати управління, центри інформаційних технологій та технічного обслуговування (ЦІТТО), цехи і інш.) і які знаходяться усередині корпоративної мережі корпорації включають в себе зони *корпоративних* користувачів і *підключення* до публічної мережі.

ЦОД підключений безпосередньо до центрального вузлу мережі передачі даних. Регіональні ЦІТТО не є опорними. Деякі центри електрозв'язку , які визначені як віддалені офіси, включають в себе *зону* периметра та *зону* сервісів ІТ інфраструктури.

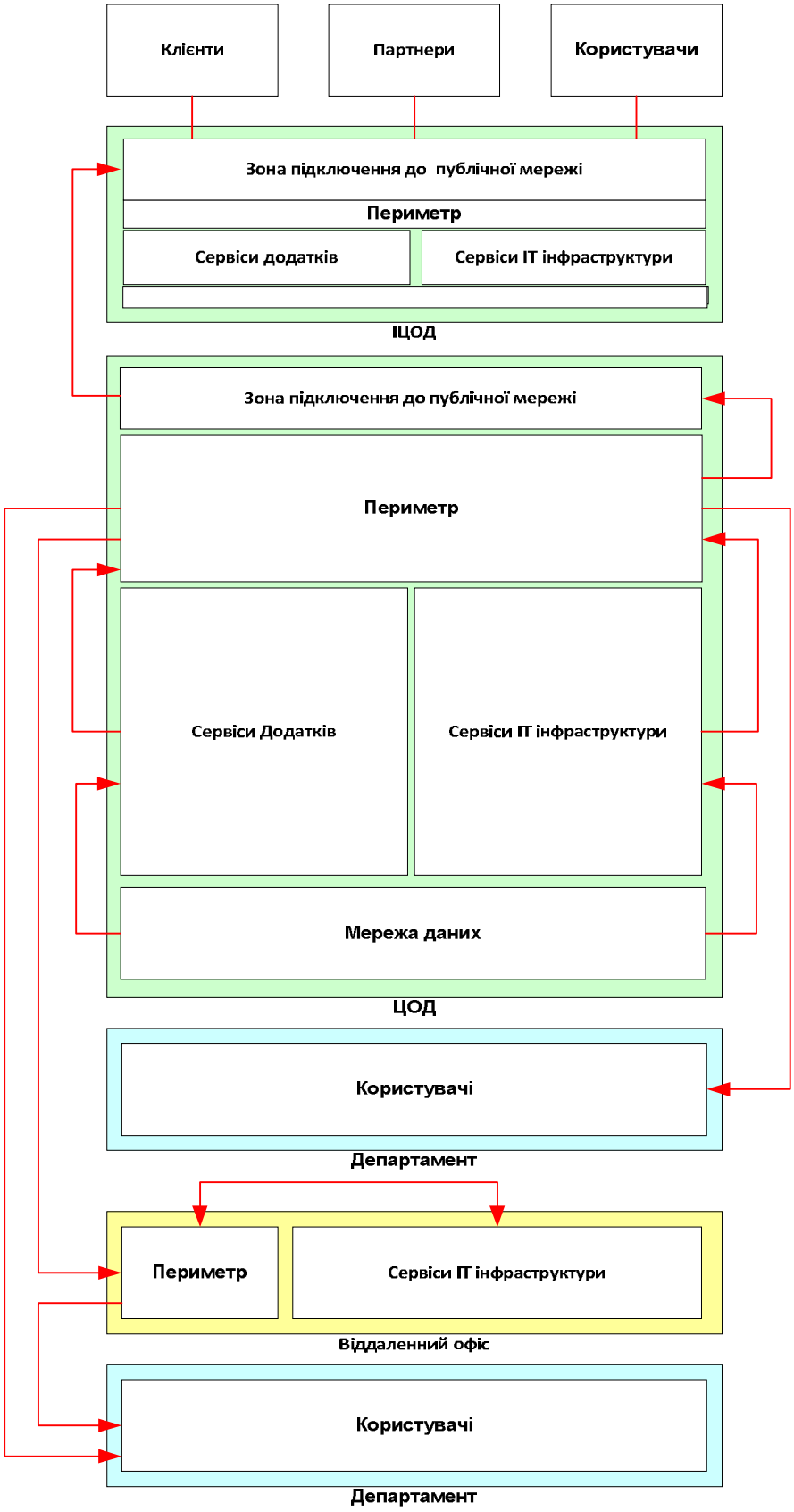

Рис. 2. Зони безпеки корпоративної мережі корпорації

4. Висновки. В статті розглядається архітектура мережі ІТ інфраструктури дата-центру Корпорації, яка призначена забезпечувати надійний, масштабований та доступний зв'язок з мережею на фізичному й логічному рівнях відповідно до вимог підприємства.

Щоб гарантувати прикладним програмам належний рівень мережних служб, архітектура мережі має проектуватися з урахуванням архітектури системи безпеки, яка встановлює певні вимоги на структурному (пристрої) та логічному рівнях (конфігурації).

При проектуванні архітектури мережі були забезпечені наступні вимоги: доступність; безпека; масштабованість; керованість; підтримка; консолідація; інтероперабельність.

У деяких випадках архітектура мережі може залежати від архітектури системи керування. Наприклад, якщо система керування вимагає виділення окремої мережі для передачі даних для керування.

Література

1. Информационные технологии – практические правила управления информационной безопасностью // ISO/IEC 17799. – [Первое издание]. – 2000. –87 с.

2. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група BHN, 2005. – 352 с.

3. Копейка О. В. Архитектура системы управления ИТ-инфраструктурой в современных Дата-центрах / О.В.Копейка// Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 1(29). – С.29-37.

4. Oleg Kopiyka Telecommunication Systems Architectures Structural Synthesis with Modern Servises Providing / Oleg Kopiyka, Alexander Drobyk, Iurii Kovalchuk// XII International Conference Modern Problems of Radio Engineering TCSET 2014. – 2014. – P. 527-528.

5. Копейка О. В. Архитектура системы безопасности ИТ-инфраструктуры в дата-центрах/ Копейка О. В.// Сучасний захист інформації. – 2014. – №1. – С.48-57.

6. Копейка О. В. Сетевые службы и службы сетевых устройств в дата-центрах / О. В. Копейка // Системи управління, навігації та зв'язку: наукове періодичне видання. – 2013. – №4(28). – С. 98-104.

7. Засади регіональної інформатизації / Довгий С. О., Копійка О. В., Черепін Ю. Т. – К.:ВПЦ «ТИРАЖ», 2004. – 304с.

8. Довгий С. А. Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития / С. А. Довгий, О. В. Копейка, С. П. Поленок. – К.:Укртелеком, 2001. – 281 с.

9. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / [Довгий С. О., Савченко О. Я., Копійка О. В. та ін..] ; за ред. С. О. Довгого. –К.: Український видавничий центр, 2002. – 502 с.

10. O. Kopeika O., I. Tarasenko, A. Kisselevskiy, A. Karichenskiy, T. Valiulin. Softline applies TMF standards as a guide when building Resource Inventory solution for nation-wide carrier Ukraine Telecom// TM Forum Case Study Handbook, Volume 3, May 2007. – P. 27.

11. Jew, Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010. – P. 28.

12. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // Schneider Electric, 2011. – P. 4.

13. Telecommunications Infrastructure Standard for Data Centers//TIA STANDARD TIA-942. Telecommunications industry association. – April 2005. – P. 135.

14. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices// Committee Approval. – January 2011. First Published: March 2011. – P. 367.