УДК 004.72

**Є.В.Кузьмінов**
**М.Г.Тарновський**

# АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Вінницький національний технічний університет.

***Анотація***

*Проаналізовані основні підходи до побудови високопродуктивної корпоративної мережі з використанням сучасних технологій, новітнього обладнання та урахування всіх особливостей функціонування підприємства.*

**Ключові слова:** ISDN, Internet, з'єднання за запитом, локальний порт, VLAN.

***Abstract***

*The basic approaches to the construction of a high-performance corporate network using modern technologies, the latest equipment and taking into account all features of functioning of the enterprise are analyzed.*

**Keywords**: ISDN, Internet, dial-on-demand, local port, VLAN.

## Вступ

Надійна мережева інфраструктура є фундаментом для успішного розвитку бізнесу сучасного підприємства, незалежно від масштабу і роду діяльності. Для багатьох підприємств надійність і захищеність бізнесу нероздільні з функціонуванням інформаційних систем; збої в роботі мережі призводять до прямих матеріальних втрат.

Основною тенденцією розвитку сучасних корпоративних інформаційних систем є централізація обчислювальних ресурсів з можливістю доступу до них з будь-якої територіально-віддаленої точки. Для реалізації даної архітектури, необхідно побудувати надійну, безпечну та продуктивну мережу, що охоплює всі віддалені філії.

У процесі функціонування підприємства та експлуатації мережі відбуваються зміни зовнішніх умов ведення бізнесу, розширення або зменшення обсягів виробництва, зміни і вдосконалення технологій і технічних засобів, удосконалення технічних параметрів і програмного забезпечення комп'ютерних систем. Відповідно до цього повинна розвиватися і змінюватися корпоративна мережа. Періодично її основні характеристики повинні переглядатися і корегуватися відповідно до поточних потреб підприємства. Таким чином, життєвий цикл комп'ютерної мережі передбачає її формування, супроводження та розвиток.

## Основні підходи до побудови корпоративної мережі підприємства

Для підключення віддалених користувачів до корпоративної мережі найпростішим і доступнішим варіантом є використання телефонного зв'язку. Там, де це можливо, можуть використовуватися мережі ISDN. Для об'єднання вузлів мережі в більшості випадків використовуються глобальні мережі передачі даних.

Підключення корпоративної мережі до Internet виправдане, якщо потрібен доступ до відповідних послуг. Використовувати Internet як середовище передачі даних доцільно тільки тоді, коли інші способи недоступні, фінансові витрати переважують вимоги надійності і безпеки. Якщо Internet використовується лише для отримання інформації, краще користуватися технологією "з'єднання за запитом" (dial-on-demand), тобто у такий спосіб підключення, коли з'єднання з вузлом Internet встановлюється тільки за ініціативою користувача і на потрібний йому час. Це дозволяє суттєво знизити ризик несанкціонованого проникнення у мережу компанії ззовні.

В основі системи управління корпоративної мережі повинні лежати такі принципи:

- суміщення адміністрування окремих функціональних підсистем (питання ефективності не може вирішуватися поза розгляду питання живучості мережі, а питання безпеки без обліку ефективності та живучості;
- централізоване/розподілене адміністрування, припускає, що основні завдання адміністрування повинні вирішуватися з центру, вторинні завдання засобами управління окремих

підсистем;

− в рамках керуючої системи повинні бути реалізовані функції системи автоматичного управління. З метою підвищення оперативності реакції системи управління на особливо важливі події, в системі повинна реалізуватися автоматична обробка особливо важливих впливів;

− в рамках системи безпеки повинен бути реалізоване адаптивне управління безпекою адекватною зміною відповідних подій (наприклад, система виявлення атак може блокувати локальний порт в разі атаки типу «відмова в обслуговуванні»).

При цьому слід зазначити, що спрощення структури мережі полягає в частині зменшення складності віддалених фрагментів, з перенесенням відповідних функцій на елементи основного фрагмента, (відповідно з його ускладненням), що, перш за все, має місце для наступних елементів:

− інформаційні сервери (з точки зору забезпечення безпеки мережі має сенс сконцентрувати всі інформаційні сервери, забезпечуючи для них необхідний захист організаційними і технічними заходами);

− адміністрування всіма функціональними підсистемами для корпоративних мереж, що використовують обмежену кількість додаткових засобів реалізації функціональних підсистем (наприклад, маршрутизаторів) може бути сконцентровано в основному фрагменті;

− підключення до загальнодоступних сервісів (мережа Інтернет) здійснюється з виділених робочих місць основного фрагмента (тут використовуються відповідні засоби захисту, підключення до глобальних мереж у загальному випадку відмінні від інших).

Система забезпечення безпеки інформації повинна мати багаторівневу структуру і включати наступні рівні:

− рівень захисту автоматизованих робочих місць (АРМ);

− рівень захисту локальних мереж та інформаційних серверів;

− рівень захисту корпоративної автоматизованої системи (КАС).

На рівні захисту автоматизованих робочих місць повинна здійснюватися ідентифікація та аутентифікація користувачів операційної системи. Повинно здійснюватися управління доступом: надання доступу суб'єктів до об'єктів відповідно до матрицею доступу, виконання реєстрації та обліку всіх дій суб'єкта доступу в журналах реєстрації. Повинна бути забезпечена цілісність програмного середовища, періодичне тестування засобів захисту інформації. Такі засоби захисту повинні володіти гнучкими засобами налаштування і можливістю віддаленого адміністрування.

Механізми захисту повинні бути здатні створювати, обслуговувати (підтримувати) і захищати від модифікації або неправомірного доступу або руйнування аутентифікаційні інформацію і матрицю доступу до об'єктів. При цьому повинна здійснюватися реєстрація дії користувачів з критичними об'єктами, дій, вжитих операторами та адміністраторами системи та інше.

Засоби захисту інформації повинні мати модульну структуру, кожен модуль повинен підтримувати область пам'яті для власного виконання. Для кожного модуля системи захисту інформації, повинна забезпечуватися ізоляція ресурсів, що потребують захисту так, щоб вони підкорялися контролю доступу і вимогам ревізії.

Для створення логічної топології корпоративної мережі, яка ніяк не буде залежати від фізичної топології, може бути використана технологія VLAN, що дозволяє на одному фізичному мережевому інтерфейсі створити кілька віртуальних локальних мереж. Це надасть змогу реалізувати гнучкий поділ пристроїв на групи, оскільки зазвичай, одному VLAN відповідає одна мережа. Комп'ютери, що знаходяться в різних VLAN, будуть ізольовані один від одного, що сприятимемо підвищенню рівня безпеки. Крім того, у результаті такого підходу отримується можливість об'єднати в одну віртуальну мережу комп'ютери, підключені до різних комутаторів.

Для забезпечення підключення до глобальної мережі пропонується використати технологію NAT, яка дозволяє різним комп'ютерам локальної мережі спільно використовувати один IP адрес для виходу у глобальну мережу. Це дає можливість передавати дані з локальної мережі у глобальну, приховуючи IP-адреса локальної мережі.

**Висновки**

Висвітлено класифікаційні ознаки корпоративних мереж, проведено їх аналіз та класифікацію розглянуто основні концепції створення корпоративної інформаційної мережі. Визначено основні підходи до управління безпекою мережі, описано основні вимоги до неї та виділено поняття корпоративної інформаційної системи. Було розроблено трирівневу ієрархічну модель корпоративної

мережі підприємства, що призведе до спрощення керування та адміністрування мережі що створюється. На основі проведеного аналізу, було прийнято рішення створити мережу на основі технологій Fast Ethernet, Gigabit Ethernet з використанням кабелю на основі витої пари.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Максимов Н.В., Попов И.И. Компьютерные сети. – 3-е изд., испр. и доп. – М.: ФОРУМ, 2008. – 448 с.: ил.

2. В.Г. Олифер, Н.А. Олифер – Компьютерные сети. Принципы, технологии, протоколы. 3-е издание – СПб.: Питер, 2006 – 958 ст.: ил.

3. Новиков Ю.В., Кондратенко С.В. – Локальные сети: архитектура, алгоритмы, проектирование. М.: ЭКОМ, 2000, 312 стр.

***Кузьмінов Євгеній Валерійович*** — студент групи КІ-18м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yevhnii.kuzminov@gmail.com

***Тарновський Микола Геннадійович***— кандидат технічних наук, доцент кафедри Лазерної та оптоелектронної техніки, Вінницький національний технічний університет

Науковий керівник: ***Тарновський Микола Геннадійович*** — кандидат технічних наук, доцент кафедри Лазерної та оптоелектронної техніки, Вінницький національний технічний університет, м. Вінниця

***Kuzminov Yevhenii V.*** — student of KI-18m group, Faculty of Information Technology and Computer Engineering, Vinnitsa National Technical University, Vinnitsa, e-mail: yevhenii.kuzminov@gmail.com

***Tarnovskiy Mykola G.*** — Candidate of Technical Sciences, Associate Professor, Laser and Optoelectronic Engineering Department, Vinnitsa National Technical University

Supervisor: ***Tarnovskiy Mykola G.*** — Candidate of Technical Sciences, Associate Professor, Laser and Optoelectronic Engineering Department, Vinnitsa National Technical University.