

operating costs for each stage of processing and qualitative indicators of the flow of processed raw materials.

References

1. Novytsky I. Automatic optimization of ore self-grinding processes in drum mills. *System Technologies*, 2000.
2. Nebatov, K, Shevchenko, Y. System analysis as a direction in the study of control processes. *Dnipro University of Technology*, WIDENING OUR HORIZONS: the 18th International Forum for Students and Young Researchers, 2023: 162-164. <https://ir.nmu.org.ua/handle/123456789/164332>
3. Novitskyi I, Sliesariiev V, Shevchenko Y. System approach in optimal management problems for two-stage technological lines, *Collection of Research Papers of the National Mining University*, №71; 2022: 211-216. doi: <https://doi.org/10.33271/crpnmu/71.222>
4. Novytskyi, I, Shevchenko, Y. Distribution of resources in the system of decentralized management. *Collection of Research Papers of the National Mining University*, 75, 2023.

УДК 004.7(07)

РОЗРОБКА ГЕТЕРОГЕННОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ІЗ ВИКОРИСТАННЯМ ДОДАТКОВИХ МЕТОДІВ РЕЗЕРВНОГО КОПІЮВАННЯ І ВІДДАЛЕНОГО ДОСТУПУ

Багнюк Н.В., к.т.н., доцент, bagnyuknata@gmail.com, ЛНТУ

Хвищун О.В., магістр, khvyshchun.o2410@lntu.edu.ua, ЛНТУ

Для створення надійної і захищеної комп'ютерної мережі підприємства необхідно використовувати комплекс інструментів і технологій, які ускладнюють зловмисникам доступ до комп'ютерів і обладнання підприємства, також забезпечують збереження даних і швидке відновлення у випадку збоїв як в програмному так і в апаратному забезпеченні. Одним з таких варіантів є використання гетерогенної мережі з використанням VPN-з'єднання.

Unix подібні операційні системи досить успішно можливо використовувати для роботи в якості робочих станцій, файлових серверів і пристроїв резервного копіювання NAS (англ. Network Attached Storage). [2]

Розробка такої системи складається з декількох етапів.

- аналіз структури підприємства;
- визначення схеми роботи;

- розробка системи захисту і технологій роботи;
- оцінка існуючого обладнання;
- побудова комплексного проекту мережі.

Аналіз структури підприємства дає можливість оцінити масштаб проекту, топологію локальної мережі, наявність віддалених офісів і працівників. Це потрібно для оцінки ризиків можливих загроз і розробки захищеної системи. На цьому етапі визначається тип роботи віддалених офісів, їх кількість. Також визначається кількість працівників, які працюють на віддалених офісах самостійно і в локальній мережі. Це суттєво впливає на вибір потужності обладнання, яке планується використовувати. [1]

Схема роботи індивідуальна для кожного підприємства. Сюди входять методи і програмні засоби ведення виробництва, обліку, ведення бухгалтерії і податкової звітності, використання спеціального обладнання, визначення пікового інтервалу завантаження структури для правильного планування часу резервного копіювання і відкриття доступу до мережі.

На схему захисту впливають:

- операційні системи на клієнтських ПК;
- наявність і кількість WI-FI точок доступу;
- кількість серверів, ресурси, які вони надають для спільного використання, і програмне забезпечення, яке використовується;
- мережеве обладнання, яке комутує внутрішню роботу і забезпечує віддалений доступ.

В оцінку існуючого обладнання входять:

- визначення можливостей підключення наявної та майбутньої кількості користувачів;
- визначення пропускнув можливості обладнання з врахуванням поставлених задач.

Враховавши описане вище, починається етап побудови і впровадження локальної мережі. Програмне забезпечення, яке розробляється за технічним завданням, повинно вирішувати ряд актуальних завдань:

- реалізація алгоритмів для аналізу трафіку мережі;
- виявляти кореляційні, структурні і інші ознаки, характерні для нормального функціонування мережі та виявлення можливих загроз;
- розробка і використання архітектури програмного забезпечення, що дозволяє легко інтегрувати нові компоненти для моніторингу та аналізу різних аспектів функціонування мережі;
- розробка системи резервного копіювання забезпечення надійності зберігання даних і налаштувань для можливості швидкого відновлення функціональності системи без втрат інформації;
- розробка типів віддаленого доступу.

На підприємстві, яке займається реалізацією металопрокатної продукції, постало питання зв'язку віддалених філій і працівників з центральним офісом з метою використання доступу до серверів і даних. Ці питання постають перед більшістю існуючих підприємств в зв'язку з розширенням, впровадженням нових технологій і ін. Через що був пророблений вищеперерахований комплекс заходів. Як результат, впроваджені необхідні рішення для забезпечення функціонування і безпеки підприємства. В результаті чого підприємство почало використовувати такі нові інструменти:

- переведено мережу на Gigabit Ethernet;
- віддалені офіси було зв'язано з центральним по протоколу L2TP VPN і користувачі отримали можливість працювати з серверами на офісі, підключаючись по протоколу PPTP VPN;
- запроваджено сервер резервного копіювання і файл обмінник на основі операційної системи DEBIAN;
- серверну частину розділено на дві частини: перша на основі Windows Server 2022 (для функціонування сервера баз даних), друга на основі Windows Server 2019 (було налаштовано контролер домену). Ці заходи дозволили застосувати на контролері домена Group Policy, що дало можливість значно підвищити захист, контролювати доступ до ресурсів сервера і включити детальний контроль роботи сервера.

В роботі розроблено порядок побудови і модернізації ІТ структури підприємства з метою досягнення надійності, захищеності, відмовостійкості і можливості відновлення функціонування в найкоротші терміни.

Список використаних джерел

1. Хомуляк М.О. Адміністрування комп'ютерних систем і мереж. Магнолія, 2023. 154 с.
2. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Львівська політехніка, 2022. 228 с.