УДК 004.415.3
Міскевич О.І., Сичов Д.І., Христинець А.О.
Луцький національний технічний університет

ПРО МОДЕРНІЗАЦІЮ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ НА ПрАТ яВОЛИНЬОБЛЕНЕРГО" НА ОСНОВІ GRE-TUNNEL З ВИКОРИСТАННЯМ ШИФРУВАННЯ IPSEC

Міскевич О.І., Сичов Д.І., Христинець А.О. Про модернізацію локально-обчислювальної мережі на ПрАТ "Волиньобленерго" на основі GRE-tunnel з використанням шифрування IPSec. Створено нову мережу та модернізовано вже існуючу локально-обчислювальну мережу на основі обладнання MikroTik.
Ключові слова: мережа, локально-обчислювальна мережа, MikroTik, IPSec, комутатор, модернізація.

Мискевич О.И., Сычев Д.И., Христинец А.О. О модернизации локально-вычислительной сети на ЧАО "Волыньоблэнерго" на основании GRE-tunnel с использованием шифрование IPSec. Создано новую сеть и модернизировано уже существующую локально-вычислительную сеть используя оборудование MikroTik.
Ключевые слова: сеть, локально-вычислительная сеть, MikroTik, IPSec, комутатор, модернизация.

Miskevych O. I., Sychov D. I., Khrystinets A.O. On modernization of the local-computer network at PrAT "Volynoblenergo" on the basis of the GRE-tunnel using IPSec encryption. New network has been created and an existing locally-based computer network based on MikroTik equipment has been upgraded.
Keywords: network, local-computer network, MikroTik, IPSec, switch, modernization.

Вступ. На сьогодні у світі існує безліч комп'ютерів і понад 80% із них об'єднані в різні інформаційно-обчислювальні мережі, від малих локальних мереж у офісах, до глобальних мереж, типу Internet. ПрАТ «Волиньобленерго» - це підприємство, основними видами діяльності якого є передача електричної енергії місцевими (локальними) мережами та постачання електроенергії за регульованим тарифом. Енергопостачання споживачів забезпечується лініями та обладнанням із напругою 0,4-110кВ.

Постановка проблеми. ПрАТ «Волиньобленерго» обслуговує понад 353 тис. фізичних та 10 тисяч юридичних споживачів. У зв'язку зі створенням нового структурного підрозділу, виникла необхідність у розробці нового вирішення питання організації інформаційно-обчислювальної мережі на базі вже існуючого комп'ютерного парку та програмного комплексу, який відповідає сучасним науково-технічним вимогам та з урахуванням зростаючих потреб і з можливістю подальшого поступового розвитку мережі (у зв'язку з появою нових технічних і програмних рішень). Тому було вирішено модернізувати вже існуючу мережу, шляхом переходу на нове обладнання MikroTik із вбудованим програмним забезпеченням та створити нову локально-обчислювальну мережу.

Аналіз існуючих рішень. На ПрАТ «Волиньобленерго» використовується топологія «Зірка». В цьому випадку кожен комп'ютер підключається окремим кабелем до загального пристрою, який називають концентратором і який знаходиться в центрі мережі. У функції концентратора входить прийом і передача комп'ютером інформації одному або решті комп'ютерів із мережі. Головна перевага цієї топології перед загальною шиною - це істотно велика надійність. Будь-які неприємності з кабелем стосуються лише того комп'ютера до якого цей кабель приєднаний і лише несправність концентратора може вивести з ладу всю мережу. Крім того, концентратор може грати роль інтелектуального фільтру інформації, яка поступає від вузлів в мережу і, при необхідності, блокує заборонені адміністратором передачі. Проте, існує ряд недоліків, зокрема, вища вартість мережевого устаткування через необхідність придбання концентратора. Крім того, можливості із накопичення кількості вузлів в мережі обмежуються кількістю портів концентратора. Іноді має сенс будувати мережу з використанням декількох концентраторів ієрархічно сполучених між собою зв'язками типу зірка. В даний час ієрархічна зірка є найпоширенішим типом топології зв'язків як в локальних так і глобальних мережах. На рисунку 1 зображена детальна будова нинішньої мережі на одній із філій ПрАТ «Волиньобленерго».

У власній модернізації було використано обладнання компанії MikroTik, зокрема комутатори CRS125-24G-1S-in, тому що вони відповідають багатьом критеріям: досить низька ціна [2], вони

мають 24 порти Gigabyte Ethernet та володіють прекрасною пропускною спроможністю. На цих комутаторах встановлена операційна система Mikrotik RouterOS L 5, через яку зручно налаштовувати повністю весь комутатор під себе [4]. З проведеного аналізу MikroTik CRS125-24G-1S-RM виявився не просто комутатором, а 24-портовим маршрутизатором з необмеженим функціоналом [3]. Крім того, слід зауважити, що таке обладнання використовують у провідних інтернет-компаніях світу [1].

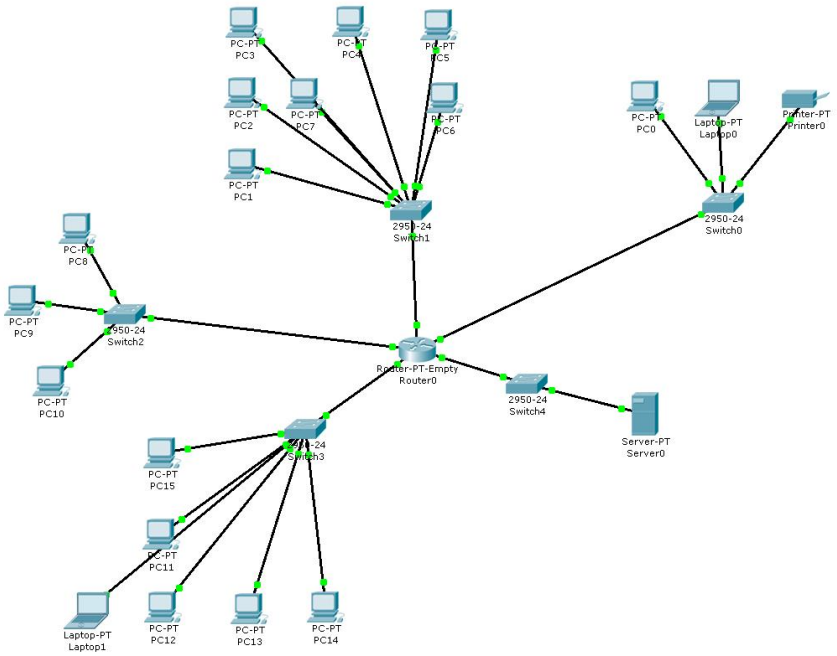

Рисунок 1 - Схема мережевого обладнання на ПрАТ "Волиньобленерго"

Виклад основного матеріалу роботи Вся маршрутизація мережі побудована на обладнанні MicroTik CRS125-24G-1S- in та на протоколі OSPF. Потрібно зазначити, що протокол OSPF (Open Shortest Path First) належить до класу протоколів стану каналів (Link State Protocol). Дослівний переклад — першим обирається найкоротший шлях. «Open»-специфікація протоколу вільно поширюється, на відміну, наприклад, від специфікації протоколу EIGRP. RFC 2328 — основний діючий документ по OSPF. Окрім того, протокол OSPF дозволяє визначити для будь-якої мережі значення метрики, залежно від типу послуги TOS (Type of Service). В OSPF підтримуються метрики пропускної здатності та затримки. Метрика, що оцінює пропускну здатність каналу, визначається, наприклад, компанією Cisco, як кількість секунд, необхідних для передачі 100 Мбіт. Метрика затримки — час у мікросекундах, необхідний маршрутизатору для обробки, постановки в чергу та передачі пакетів. Для кожної з метрик протокол OSPF будує окрему таблицю маршрутизації. Стандартний порядок розрахунку метрики, що оцінює показники надійності, затримки й вартості, поки не визначений. Цей порядок визначається адміністратором.

У цьому протоколі також закладено можливість балансування навантаження на шляхах як з однаковою вартістю, так і з різною. Розподіл трафіку відбувається пропорційно метриці шляху.

Generic Routing Encapsulation (GRE-tunnel) - простий протокол тунелювання. Це означає, що можна взяти початкові дані разом зі службовими заголовками (як правило, це IP, але може бути і Ethernet і ATM), запакувати в пакет і передати до публічної мережі, немов машина їде в тунелі через гори. На кінцевому вузлі заголовки нового пакету знімаються, а ваші дані в початковому вигляді продовжують свою подорож. GRE-тунелі є односпрямованим, і зазвичай мається на увазі наявність зворотного тунелю на іншій стороні, хоча взагалі кажучи, це необов'язково. Але в нашому випадку, коли посередині Інтернет, і завдання - організувати приватну мережу, зі зворотного боку повинне бути симетричне налаштування.

IPsec (скорочення від IP Security) — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжньості та/або шифрування IP-пакетів. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет.

Протоколи IPsec, на відміну від інших добре відомих протоколів SSL та TLS, працюють на мережевому рівні (рівень 3 моделі OSI). Це робить IPsec гнучкішим, так що він може використовуватися для захисту будь-яких протоколів, що базуються на TCP та UPD. IPsec може використовуватися для забезпечення безпеки між двома IP-вузлами, між двома шлюзами безпеки або між IP-вузлом і шлюзом безпеки. Протокол є "надбудовою" над IP-протоколом, і обробляє сформовані IP-пакети. IPsec може забезпечувати цілісність та / або конфіденційність даних переданих по мережі [6].

Зробимо порівняльну характеристику нинішнього обладнання структурного підрозділу ПрАТ "Волиньобленерго" та обладнання, яке було встановлене до модернізації. Результати порівняння подані у таблиці 1.

Таблиця 1. Порівняльна характеристика обладнання D-Link DES-1210 та MIKROTIK CRS125-24G-1S-IN

Назва	D-Link DES-1210	MIKROTIK CRS125-24G-1S-IN
Тип	Комутатор керований рівня 2	Комутатор керований
Кількість портів Fast Ethernet (10/100)	24 (з грозозахистом)	1 (консоль)
Кількість портів Gigabit Ethernet (10/100/1000)	2x SFP + 2x комбо 1000Base-T / SFP (з грозозахистом)	24
Інші порти	консольний RJ-45	1x SFP, 1x USB, 1x micro-USB
Моніторинг та конфігурування	Web-інтерфейс, SNMP, RMON, Telnet, SSH, LLDP	Mikrotik RouterOS L 5
Живлення	100-240 В, 50-60 Гц	100-240 В, 50 / 60Гц
Розміри, мм	440x140x44	246x135x50
Особливості	802.1Q, Q-in-Q, ISM VLAN, 802.1p, IGMP Snooping, STP, LBD, LACP, ACL, 802.1x, IMPB, DHCP Snooping	Налаштування портів для комутації або для маршрутизації. LCD сенсорний екран.

Легко бачити, що обладнання із правого стовбця є на порядок кращим та має свою ОС, в якій можна розвинути власну мережу, включити та налаштувати власний VPN із використанням GRE-tunnel та ширфрування каналу з використанням протоколу IPSec без втрати швидкості передачі даних. Також, є можливість розгорнути декілька мереж із використанням одночасно декількох провайдерів із надійними налаштуваннями безпеки. На завершення, слід зауважити, що цією системою можна керувати не виходячи з дому.

Після проведеної модернізації локально-обчислювальна мережа на структурному підрозділі ПрАТ "Волиньобленерго" матиме наступний вигляд (рисунок 2):

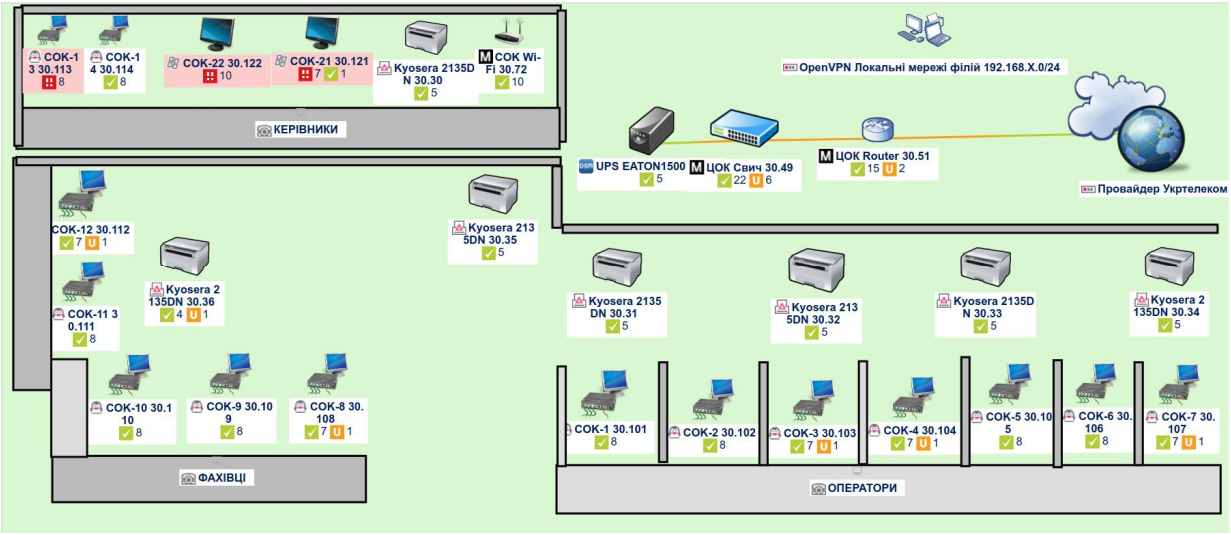

Рисунок 2 - Локально-обчислювальна мережа на основі обладнання MikroTik

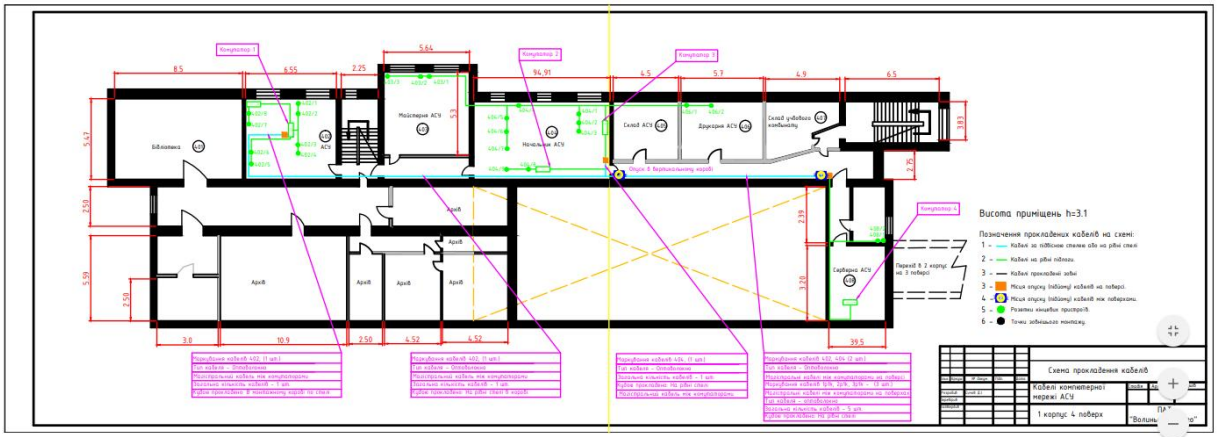

Рисунок 3 - Розташування комутаторів при модернізації вже існуючої мережі на підприємстві ПрАТ "Волиньобленерго"

Висновки В ході проведеної роботи відбулося дослідження об'єкта на ПрАТ "Волиньобленерго", його структури та функцій, наявного апаратного та програмного забезпечення і комплексу задач, що вирішується ним. На основі аналізу існуючих апаратних та програмних засобів були виявленні недоліки побудови існуючого комплексу апаратно-програмних засобів та реалізовані шляхи виправлення даної ситуації. Щодо подальшої реалізації проекту, то пізніше можна реалізувати модернізацію за аналогічною схемою повної мережі філій ПрАТ "Волиньобленерго".

1. https://weblance.com.ua/336-amazon-ispolzuet-v-svoih-datacentrah-i-oblachnyh-servisah-oborudovanie-mikrotik.html
2. https://rozetka.com.ua/routers/c80193/producer=cisco-sb,mikrotik/
3. https://mikrotik.com/aboutus
4. https://habrahabr.ru/post/265387/
5. https://habrahabr.ru/post/271707/
6. https://uk.wikipedia.org/wiki/IPsec