УДК 681.5

DEVELOPMENT OF REMOTE MONITORING SYSTEMS USING THE INTERNET

O. Pupena, V. Sidletsky
National University of Food Technologies

Key words:
Remote monitoring
Control system
Mobile Internet
Virtual private networks
OpenVPN

Article history:
Received 15.08.2014
Received in revised form 22.08.2014
Accepted 29.08.2014

Corresponding author:
O. Pupena
Email:
npnuht@ukr.net

ABSTRACT

The paper analyzes the approaches, methods and means of remote monitoring of control objects, and recommendations on how to use the Internet as a communication subsystem for dispatching station to the remote local management system.

РОЗРОБКА СИСТЕМ ВІДДАЛЕНОЇ ДИСПЕТЧЕРИЗАЦІЇ З ВИКОРИСТАННЯМ МЕРЕЖІ INTERNET

О.М. Пупена, В.М. Сідлецький
Національний університет харчових технологій

У статті проведено аналіз способів, засобів і підходів до віддаленої диспетчеризації об'єктів управління, надано рекомендації щодо використання мережі Internet як підсистеми зв'язку станції диспетчеризації з віддаленою локальною системою управління.

Ключові слова: *віддалена диспетчеризація, система управління, мобільний Internet, віртуальні приватні мережі, OpenVPN.*

Ряд об'єктів автоматизації потребують віддаленого диспетчерського контролю й управління. В основному це об'єкти житлово-комунального господарства, які можуть бути територіально розосереджені на великому просторі, а також котельні або теплопункти. Віддаленої диспетчеризації потребують також об'єкти енергетики — це різного роду розподільчі станції, до систем управління й телеметрії яких ставляться особливі вимоги, тому ці об'єкти не розглядаються в даній статті.

Необхідність у віддаленій диспетчеризації виникає, як правило, з таких причин:

1. Системи працюють в автоматичному режимі, однак необхідно забезпечити сигналізацію несправності з метою виїзду до об'єкта ремонтної бригади. Такими об'єктами диспетчеризації можуть бути ліфти, невеликі теплопункти тощо.

2. Системи переважний час працюють в автоматичному режимі, однак є необхідність в контролі за їх роботою та корегуванні заданих параметрів декілька раз за добу. У цьому випадку постійна присутність оператора на об'єкті економічно недоцільна. Для прикладу можна навести автоматизовані системи управління водонасосними станціями або котельними.

3. Необхідно централізовано збирати показники витрат, лічильників та інших параметрів для обліку, економічної звітності й аналізу. Це можуть бути будь-які територіально-розподілені об'єкти, в тому числі ті, в автоматизованій системі управління яких для операторського контролю передбачені локальні засоби людино-машинного інтерфейсу. Основна функція віддаленої диспетчеризації в цьому випадку — централізоване ведення архіву.

Функції системи віддаленої диспетчеризації

Складність об'єкта його призначення, реалізація локальної системи управління впливає на спосіб реалізації системи диспетчеризації й технології, які при цьому використовуються. Провівши аналіз потреб ринку і пропозицій [1—2], можна виділили такі функції системи диспетчеризації:

- реалізація підсистеми тривог: відображення активних тривог (технологічна, пожежна й охоронна сигналізація) з можливістю їх підтвердження;
- ведення архіву потрібних технологічних параметрів для можливості їх подальшого аналізу у вигляді трендів і звітів;
- ведення журналу повідомлень і тривог;
- формування звітів;
- відображення технологічних параметрів у м'якому реальному часі;
- управління станом обладнання, зміна уставок, корегування параметрів регуляторів тощо;
- діагностування роботи обладнання;
- віддалене конфігурування/програмування інтелектуальних засобів автоматизації й комунікації.

Наведені вище функції є класичними для засобів SCADA/HMI, які використовуються для побудови АСУТП. Суттєвою відмінністю систем віддаленої диспетчеризації є знаходження джерела даних на великій відстані від АРМ оператора, що вносить суттєві корективи в спосіб організації зв'язку й структури самої системи, тому як і у випадку необхідних функцій, так і при виборі структури й технологій чіткої однозначності немає.

Умовно в системі віддаленої диспетчеризації можна виділити такі функціональні підсистеми (рис.1).

Локальна система управління (ЛСУ). ЛСУ знаходиться безпосередньо в місці розташування об'єкта. Вона може працювати як в автоматичному, так і в автоматизованому режимі, має інтерфейс доступу до даних. ЛСУ може включати контролери, засоби зв'язку з об'єктом, засоби людино-машинного інтерфейсу (HMI). Система є функціонально закінченою, тому може працювати в автономному режимі. Для системи диспетчеризації ЛСУ є рівнем пристроїв зв'язку з об'єктом.

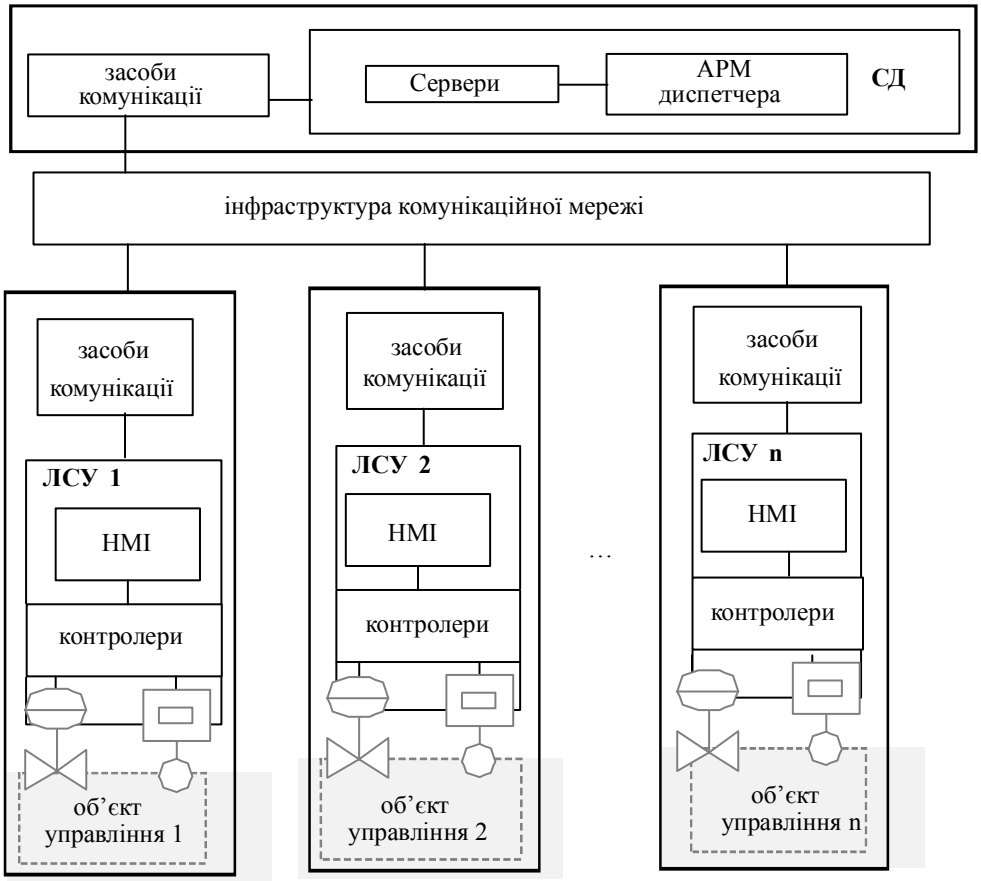

Рис.1. Функціональна структура системи віддаленої диспетчеризації

Підсистема віддаленого зв'язку. До цієї підсистеми можна віднести всі засоби комунікації та інфраструктури мережі, які беруть участь у створенні каналу зв'язку між ЛСУ й станцією диспетчеризації (СД).

Станція диспетчеризації (СД). Ця підсистема призначена для кінцевої реалізації всіх наведених вище функцій. Вона може включати сервери збору даних, архівування тривог і звітів, а також автоматизоване робоче місце (АРМ) диспетчера.

Слід зазначити, що функціональна структура, наведена на рис.1, є умовною і може відрізнятися залежно від об'єкта, реалізації ЛСУ і вимог до функцій системи віддаленої диспетчеризації.

Реалізації підсистеми віддаленого зв'язку

Для реалізації підсистем віддаленого зв'язку альтернативи використанню бездротових технологій, за винятком окремих випадків, немає. Це пов'язано насамперед зі значними затратами на побудову й обслуговування кабельної інфраструктури. Серед бездротових способів зв'язку у світі найбільш доступним є стільниковий. На сьогоднішній день на теренах України доступні технології декількох поколінь (G) стільникового зв'язку:

2G — технології зв'язку GSM з підтримкою голосових дзвінків, сервісів повідомлень SMS/MMS і передачі даних CSD;

2.5G — сервіси пакетної передачі GPRS, які функціонують на існуючих стільникових мережах GSM і краще пристосовані для обміну даними ніж CSD;

2.75G — сервіс пакетної передачі даних EDGE, які функціонують на існуючих стільникових мережах GSM; пропускна здатність EDGE збільшена порівняно з GPRS;

3G — технології зв'язку з підтримкою голосових дзвінків, сервісів повідомлень SMS/MMS і передачі даних на швидкостях більших, ніж 2/2.5/2.75G. В Україні доступні стандарт UMTS/W-CDMA, який підтримується Utel ("ОГО! Мобільний"); за відсутності зв'язку через канал UMTS стандарт UMTS/W-CDMA перемикається на роумінг GSM «Київстар"; стандарт CDMA2000, який підтримується PEOPLEnet, МТС Коннект тощо;

4G — технології забезпечують на високій швидкості передачу голосу, відео, даних, дозволяють організовувати IP-телефонію, корпоративні мережі та проводити якісну відео трансляцію. В Україні доступні WiMAX (базується на IEEE 802.16) та LTE, які підтримуються на обмежених територіях.

Слід зазначити, що серед наведених вище поколінь технологій 4G можуть бути задіяні тільки на дуже обмежених територіях.

Проаналізуємо, які сервіси можуть бути використані для обміну даними. Обмін даними CSD є повільним і малоефективним. Сервіс SMS використовується для передачі аварійних і службових повідомлень, а також команд управління переважно в системах з малою кількістю каналів, де до функцій віддаленої диспетчеризації входять тільки реалізація підсистеми тривог та управління станом обладнання. За необхідності реалізації інших із перерахованих вище функцій використання SMS може бути тільки додатковим каналом.

Основними технологіями для обміну даними є ті, які базуються на пакетній передачі (2.5G та вище), оскільки вони більше за SMS і CSD пристосовані до передачі даних в реальному часі. Ці технології надають можливість легко підключитися до Internet, а за вартістю послуг доступні не тільки організаціям, а й приватним особам. Internet, у свою чергу, загальнодоступний у будь-якій точці цивілізованого світу, що виключає необхідність у виділенні окремих каналів операторами зв'язку. Тобто провайдери зв'язку і технічна реалізація ЛСУ і СД можуть відрізнятися, тоді як TCP/IP пристосований для багатьох фізичних реалізацій мереж. На відміну від сервісу SMS, послуги мобільного Internet оцінюються в одиницях переданих даних або є безлімітними.

Програмні і апаратні засоби зв'язку

Для реалізації бездротового каналу зв'язку ЛСУ як засіб комунікації (рис.1) необхідно використовувати модем (GSM/GPRS/EDGE/3G), який може бути в складі одного з технічних засобів:

- інтегрованого в промисловий контролер модуля;
- апаратно-відокремленого від системи модему з одним з інтерфейсів RS-232, RS-485, USB;

- маршрутизатора (Router) або шлюзу(Gateway)

За останні декілька років номенклатура таких засобів розширилася, а їх функціональність значно зросла. У зв'язку з цим ринкова вартість знижується, що значно розширює можливості цільових систем і спрощує процес їх побудови.

До недавнього часу основними засобами для віддаленої диспетчеризації були GSM-модеми (без функцій мобільного Інтернету), а найбільш простим і популярним способом обміну — SMS-повідомлення. Побудова такої системи вимагає налагодження каналу зв'язку між GSM-модемом і промисловим контролером локальної системи управління по послідовному інтерфейсу (RS-232 або RS-485). У кращому випадку промисловий контролер може бути спеціально пристосований до такого зв'язку, у гіршому — його необхідно прописувати у вигляді додаткової функції програми контролеру. Відправка й отримання даних проходить з використанням символьного способу обміну AT-командами. Однак GSM-модеми надають можливість побудови модемного зв'язку з використанням CSD-каналу, що дозволяє налагодити зв'язок між модемом і контролером з використанням протоколів самого контролера. Такий спосіб зв'язку доцільний тільки в тому випадку, якщо контролер вміє накопичувати дані між викликами, а зв'язок відбувається періодично. Звісно, функціональність такого підходу значно обмежується, а вимоги до програмного забезпечення більш специфічні.

GPRS/EDGE/3G-модеми, окрім функцій GSM, надають можливість пакетного обміну GPRS, що, у свою чергу, дозволяє оптимальніше використовувати мобільний зв'язок для доступу до Internet. Проте зв'язок між модемом і промисловим контролером платформозалежний, здійснюється на основі AT-команд і, як правило, прописується індивідуально для кожного типу контролера.

Для автоматизації невеликих об'єктів житлово-комунального господарства на ринку існує ряд пропозицій промислових контролерів із вбудованими (інтегрованими) в них модемами. Прозорість обміну між пристроєм і модемом компенсується специфічністю використаних протоколів верхнього рівня, що призводить до обмеженого використання програмного забезпечення. Крім того, невеликий обсяг пропозицій на ринку обмежує вибір достойного пристрою такого класу.

Набагато більше можливостей для зв'язку з Internet є у маршрутизаторів. На відміну від модемів, маршрутизатори працюють на рівні протоколу IP і вище, що робить обмін між пристроями з підтримкою цього протоколу прозорим. Іншими словами, налаштування зв'язку між ЛСУ та СД через Internet проходить незалежно від способів підключення до глобальної мережі. Порт для виходу в Internet (позначений як WAN) через стільниковий зв'язок повинен бути одним із доступних GPRS/EDGE/3G, а інтерфейс інших портів вибирається з урахуванням структури системи управління на об'єкті: Ethernet, WiFi (IEEE 802.11), RS-232, RS-485, USB. Крім того, маршрутизатори мають стандартний для такого роду пристроїв набір функцій (NAT-трансляція, DHCP-сервер, переадресація, брандмауер, динамічний DNS, підтримка VPN-тунелів тощо).

Враховуючи, що пристрої локальної системи управління з наявними каналами RS-485 та RS-232 не підтримують IP-протокол, доповненням до маршрутизаторів є функції шлюзування. У цьому випадку, крім функцій маршрутизації, конфігуруються завдання збору даних за підтримуваним протоколом і передачі їх на верхній рівень. Однак велику гаму можливих промислових мереж не може задовольнити універсальний шлюз, тому найчастіше підтримуваним протоколом є Modbus або протокол вибирається як опція, що «прошивається» виробником шлюзів на замовлення.

Окремої уваги потребує питання перепрограмування шлюзів-маршрутизаторів. На сьогоднішній день програмна «прошивка» таких шлюзів базується на ОС сімейства LINUX. Це надає можливість розробляти власні скрипти (наприклад, на JAVA), записувати розроблені або придбані програми-демони (служби), робить діагностику й обслуговування шлюзу універсальною. Незважаючи на те, що для конфігурування й програмування таких пристроїв необхідна компетенція в галузі IT, такий підхід є досить функціональним. Загалом, шлюзи й маршрутизатори — це повноцінні комп'ютери, хоч і з обмеженими ресурсами.

Для зв'язку локальних систем управління об'єктів середньої та великої канальності (20 і більше датчиків та виконавчих механізмів) зі станцією диспетчеризації найбільш підходить використання шлюзів і маршрутизаторів, тому варто розглянути системи, побудовані на їхній основі. Для локальних контролерів з наявним Ethernet жодних додаткових засобів не потребується. Для інших типів інтерфейсів пристроїв рекомендується використовувати шлюзи з підтримкою стандартних протоколів (наприклад, Modbus/TCP) або використовувати/прописувати програми-демони в існуючих маршрутизаторах на базі LINUX.

Станції диспетчеризації необхідний доступ до Internet. Як альтернатива може бути використана налаштована провайдером зв'язку віртуальна приватна мережа (ця послуга додатково оплачується). Вимоги до апаратного за безпечення в більшості випадків визначають особливості реалізації підключення до провайдера Internet. Вибір програмного забезпечення для реалізації АРМ диспетчера та сервера станції диспетчеризації визначається такими ж вимогами, як і вибір локальних АРМів і серверів вводу/виводу, наприклад, на базі SCADA, власноруч розробленого ПО, браузера для доступу до WEB-серверів тощо.

Врахування особливостей реалізації

При виборі структури системи диспетчеризації необхідно враховувати особливості реалізації каналу.

Надійність. Менша надійність бездротового каналу зв'язку, порівняно з дротовими комп'ютерними чи промисловими мережами, потребує резервування каналу передачі і/або вибраного оператора мобільного зв'язку. При додаткових вимогах також можливо знадобиться архівування параметрів у локальному буфері за відсутності зв'язку з об'єктом. Резервування каналу досягається за рахунок використання послуг двох операторів, що вимагає від модемів маршрутизаторів підтримку двох SIM-карт. У сучасних промислових

маршрутизаторах такий функціонал, як правило, підтримується, а переключення проводиться автоматично.

У випадку відсутності доступу до всіх стільникових мереж дані в реальному часі передати неможливо. Однак для задачі ведення архіву їх можна зберігати в локальному буфері маршрутизатора, а після відновлення зв'язку — транспортувати на станцію диспетчеризації. Такий спосіб потребує додаткового програмування як з боку маршрутизатора-шлюзу, так і з боку станції диспетчеризації. Більш дорожчий, але класичний спосіб вирішення задачі локального архіву — використання розподілених архітектур SCADA, де сервери збору даних та архівування розміщуються як на ЛСУ, так і на станції диспетчеризації.

Послуги оператора. Необхідно заздалегідь продумати і вирішити всі економічні, юридичні й організаційні аспекти використання послуг оператора мобільного зв'язку, зокрема вибір оператора й тарифу, домовленість і відповідальність за надання послуг, замовлення додаткових послуг, порядок оплати тощо.

Дорогий, але надійний спосіб зв'язку — це організація віртуальної приватної мережі (VPN) самим оператором, без виходу в мережу Internet. До недоліків такого підходу можна віднести підвищену вартість обслуговування та залежність від одного оператора стільникового зв'язку.

Для доступу до серверних додатків пристроїв або маршрутизатора локальної системи управління необхідна виділена «біла» IP-адреса. Цей ресурс оплачується додатково, тому може значно збільшити вартість каналу зв'язку. Якщо кількість об'єктів диспетчеризації більше одного, доцільно виділити IP-адресу тільки для сервера диспетчеризації. Це, у свою чергу, вимагає клієнтських додатків для ЛСУ а не СД, оскільки ЛСУ знаходяться за NAT-трансляторами провайдерів і невидимі як окремі вузли.

З практичної точки зору наявність клієнтських додатків для ЛСУ означає, що більшість протоколів промислових мереж рівня контролерів є клієнт-серверними, де HMI/SCADA виступають як клієнт [3]. У даному випадку сторони клієнта і сервера повинні взаємно замінюватися, а це не завжди можливо. Наприклад, якщо використовується протокол Modbus/TCP, то на сервері диспетчеризації повинен бути використаний драйвер Modbus/TCP Server, а на контролері ЛСУ — Modbus/TCP Client. Проблеми, пов'язані з використанням IP-адреси, можуть бути вирішені шляхом створення VPN-тунелю.

Захист від несанкціонованого доступу. Слід мати на увазі, що Internet — це загальнодоступна глобальна мережа. Якщо підключення вузлів системи диспетчеризації реалізовувати через Internet, теоретично ресурсами може користуватися будь-який користувач. У даному випадку треба приділяти велику увагу питанням захисту підсистем від несанкціонованого доступу. На сьогоднішній день для цього використовують комплекс заходів, призначених для аутентифікації, авторизації та шифрування. Аутентифікація — це процедура перевірки автентичності, наприклад, перевірка користувача шляхом введення його пароля або перевірка достовірності доставлених даних порівнянням контрольної суми файлу тощо. Авторизація - надання корис-

тувачу певних прав для дозволу на виконання дій. Для авторизації необхідна процедура аутентифікації. Шифрування використовується для передачі даних у шифрованому форматі, що дає змогу захистити їх від перегляду та підміни сторонніми суб'єктами.

Огляд механізмів захисту від несанкціонованого доступу в мережевих системах виходить за межі статті. Однак треба врахувати той факт, що обмін даними відбувається без участі людини, тому процедура аутентифікації при створенні з'єднання повинна проходити автоматично. Найбільш ефективним способом захисту є використання захищених VPN-тунелів.

Функціональна безпека. Враховуючи велику відстань оператора від об'єкта, треба уникати можливості віддаленої зміни ним тих параметрів, які можуть привести до функціонально-небезпечних наслідків, або передбачити ЛСУ місцевим блокуванням. Якщо з переліку функцій виключити можливість зміни змінних і втручання в роботу обладнання чи програм, то система диспетчеризації жодним чином не впливає на роботу ЛСУ, і питання функціональної безпеки вирішується при роботі локальної системи управління.

Що стосується можливості зміни програмного забезпечення віддалено, то слід передбачити апаратне блокування (наприклад, перемиканням контролера в спеціальний режим). У будь-якому випадку, навіть якщо таке блокування не передбачено виробником обладнання, бажано проводити процедури переконфігурування тільки за наявності обслуговуючого персоналу ЛСУ.

Використання віртуальних приватних мереж (VPN)

Наведений вище аналіз вказує на доречність реалізації підсистеми віддаленого зв'язку з використанням VPN-тунелів. VPN — це віртуальна приватна мережа, тобто така, яка базується на іншій мережі, однак логічно відділяє її ресурси від базової. Якщо за базову мережу береться Internet, то окремі її вузли можна виділити таким чином, щоб тільки вони могли обмінюватися між собою. З точки зору Internet, вузли кожної VPN є звичайними вузлами, але вміст пакетів, якими вони обмінюються, зашифрований і доступний тільки в межах VPN.

Один із способів реалізації VPN — це використання тунелів. Тунель — це створене логічне з'єднання між двома вузлами в мережі (наприклад маршрутизаторами), призначене для передачі в полі даних упакованих мережних пакетів. У процесі обміну по тунелю проходить інкапсуляція одних пакетів (або сегментів) в інші. Для аналогії тунель можна порівняти з поромною переправою, по якій можна переправити інший транспорт, наприклад, автобус. Таким чином, з точки зору пасажирів, вони рухаються по маршруту в автобусі, хоч автобус знаходився на поромі. Якщо мережні пакети (або сегменти), які передаються по тунелю попередньо зашифрувати, то тунель забезпечить шифровану VPN-мережу, яка складається з двох вузлів. Для збільшення кількості вузлів VPN-мережі кількість тунелів теж збільшують.

Якщо тунелем з'єднати дві локальні мережі, то можна організувати інтермережу (рис.2). У цьому випадку subnet1 передає всі дані, адресовані за межі підмережі маршрутизатора Router1, а subnet2 — Router2. Трафіки в

середині підмереж нешифровані, тому що це зона закритого доступу. Маршрутизатори поєднані тунелем, по якому всі пакети, які передаються від subnet1 до subnet2 і навпаки, упаковуються в нові пакети і шифруються. Іншими словами, для вузлів підмереж взагалі нічого невідомо про наявність тунелю і тим більше про особливості його функціонування. Тобто обмін між вузлами subnet1 та subnet2 проходить так, ніби підмережі просто були об'єднані маршрутизаторами.

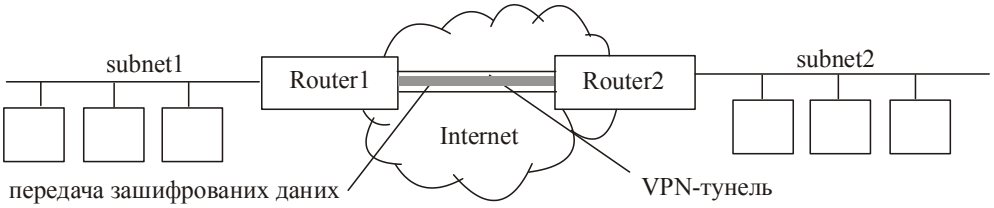

Рис.2. Об'єднання двох локальних мереж за допомогою тунелю

На сьогоднішній день є декілька технологій реалізації мереж шляхом VPN-тунелів. Найбільш ефективним для вирішення поставлених задач є OpenVPN [4]. Крім притаманних більшості технологій можливості захисту даних від несанкціонованого доступу, OpenVPN має низку переваг. Так, у тунельному режимі OpenVPN маршрутизатор упаковує всі пакети підмереж в UDP або TCP пакет, попередньо зашифрувавши їх одним із вибраних способів шифрування. Один із маршрутизаторів вибирається як OpenVPN-сервер, який буде очікувати підключення з боку іншого маршрутизатора - OpenVPN-клієнта. При цьому вибір сторони клієнта і сервера визначається зручностями й обмеженнями провайдерів Internet. Наприклад, за наявності тільки однієї «білої» адреси IP необхідно встановити OpenVPN-сервер саме на цьому маршрутизаторі. Слід зазначити, що розподіл ролей OpenVPN-клієнта та сервера жодним чином не впливає на обмін між вузлами в підмережах, тому розміщення клієнтських і серверних додатків в них не має значення.

Враховуючи, що тунель налаштовується на транспортному рівні в межах «дозволених» TCP/UDP-портів, на його функціональність не будуть впливати особливості реалізації каналу провайдера. Так, наприклад, NAT-транслятори не дають змоги реалізувати мережі VPN через протоколи L2TP/IPSec. Для вирішення цієї проблеми необхідна переадресування портів або попередня додаткова упаковка. На відміну від L2TP/IPSec, OpenVPN-пакети можуть передаватися через будь-який порт.

OpenVPN реалізований для більшості популярних платформ, зокрема для Windows і Linux. Біільшість маршрутизаторів підтримують цю технологію або можуть бути перепрошиті прошивкою DD-WRT [5], в якій реалізовані OpenVPN.

Приклад структури системи

Можливу структуру системи віддаленої диспетчеризації розглянемо на прикладі котельні (рис.3).

Часто для реалізації контурів управління ЛСУ котельних застосовують ПТК на базі конфігурованих контролерів, що надають доступ через мережу

LON. Для інтегрування їх у систему диспетчеризації можна використати шлюзи Modbus/TCP-LON, які підключаються до мережі Ethernet. Маршрутизатори Router1 та Router2 підтримують OpenVPN тунелі через канали WAN і GPRS. При цьому, один із маршрутизаторів буде мати виділену IP-адресу і буде сервером OpenVPN. RM — точка виходу в Internet оператора мобільного зв'язку, RI — провайдера Internet-станції диспетчеризації.

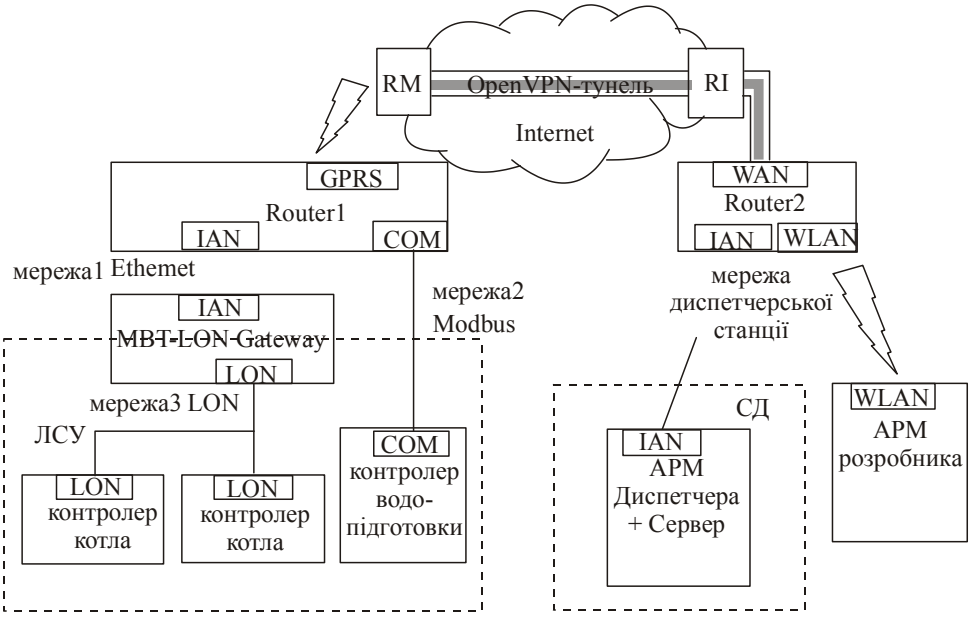

Рис.3. Приклад технічної структури системи віддаленої диспетчеризації

Маршрутизатори Router1 та Router2 налаштовані таким чином, щоб IP-пакети циркулювали між локальними мережами диспетчеризації та ЛСУ. На маршрутизаторі Router1 також запущена програма-демон Modbus/TCP—ModbusRTU шлюзу, яка надає можливість обмінюватися з контролером водопідготовки.

Висновки

На сьогоднішній день добре розвинута в Україні інфраструктура Internet і стільникового зв'язку дає змогу використовувати їх для систем віддаленої диспетчеризації. Особливості функціонування Internet і стільникового зв'язку пов'язані з вирішенням додаткових питань надійності, захисту інформації та реалізації прозорого обміну між вузлами системи диспетчеризації. Визначено, що для систем середньої та великої канальності доречним є використання стільникового Internet на базі технологій GPRS/EDGE/3G. Для систем такого класу замість модемів більш вигідно використовувати маршрутизатори та шлюзи. Для вирішення проблем захисту від несанкціонованого доступу доцільно використовувати шифровані віртуальні приватні мережі (VPN). Для універсальності і незалежності від операторів зв'язку та провайдерів Internet рекомендується використовувати технологію OpenVPN.

Враховуючи запропоновані підходи, всі інші частини задачі віддаленої диспетчеризації можна вирішувати з використанням традиційних програмних та апаратних засобів АСУТП.

Література

1. *Борисов Г.* Современные системы диспетчеризации // Коммунальный комплекс России. — 2009. — № 7—8. — С. 61—62.

2. *Диспетчеризация* территориально распределенных и удаленных пром.-шленных объектов и объектов ЖКХ с дистанционным управлением. Построение системы диспетчеризации [www.gammi-ltd.ru]

3. *Пупена О.М.* Промислові мережі та інтеграційні технології в автоматизованих системах: навч. посіб./ О.М. Пупена, І.В. Ельперін, Н.М. Луцька, А.П. Ладанюк. — К.: Вид-во «Ліра-К», 2011. — 552 с.

4. *Технологія* OpenVPN [Електронний ресурс, режим доступу www.openvpn.net]

5. *Прошивка* маршрутизаторів DD-WRT [Електронний ресурс, режим доступу www.dd-wrt.com]

РАЗРАБОТКА СИСТЕМ УДАЛЕННОЙ ДИСПЕТЧЕРИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ СЕТИ INTERNET

А.Н. Пупена, В.М. Сидлецкий
Национальный университет пищевых технологий

В статье проанализированы подходы, способы и средства для удаленной диспетчеризации объектов управления, разработаны рекомендации относительно использования Internet в качестве подсистемы связи станции диспетчеризации и удаленной локальной системы управления.

***Ключевые слова**: удаленная диспетчеризация, система управления, мобильный Internet, виртуальные частные сети, OpenVPN.*