# СЕКЦІЯ 5: АВТОМАТИЗАЦІЯ ЕЛЕКТРОМЕХАНІЧНИХ СИСТЕМ ТА ЕЛЕКТРОПРИВОД

## СИСТЕМИ АВТОМАТИЗАЦІЇ ІЗ ЗАХИЩЕНИМ КАНАЛОМ ЗВ'ЯЗКУ

**Кривошея І.В., студент, Король С.В., к.т.н., доц.**
*КПІ ім. Ігоря Сікорського, кафедра автоматизації електромеханічних систем та електроприводу*

**Вступ.** В останні десятиліття багато регіональних компаній виросли до світових масштабів, тому постає проблема як встановити швидкий та надійний зв'язок всередині компанії. До появи віртуальної приватної мережі VPN (Virtual Private Network), зв'язок налагоджувався за допомогою глобальної мережі WAN (Wide Area Network). Це дуже безпечний спосіб комунікації, проте, має один суттєвий недолік: висока вартість, яка тим більша, чим віддаленіші точки сполучення. Зі зростанням мережі Інтернет, глобальна комунікація стає набагато легшою. Багато компаній використовують його, проте, основна проблема Інтернету те, що він є публічним, а, отже, не захищений від кібератак.

Безпечна передача інформації через загальнодоступні мережі можлива через закритий для сторонніх вузлів канал обміну інформацією із шифруванням, який реалізується технологією VPN. Такий підхід дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних незахищених каналів. VPN складається з сервера та клієнта. Клієнт – це об'єкт, що бажає приєднатися до захищеної мережі; а сервер керує доступом до мережі та надає клієнту IP-адресу.

В даній статті розглядається методика вивчення принципів побудови систем автоматизації на основі промислового комп'ютера з графічним інтерфейсом XV100 компанії EATON при використанні VPN для підключення до віддаленої корпоративної мережі. Таким чином, знання принципів побудови глобальних мереж є вагомою перевагою фахівця в області автоматизації, що обумовлює необхідність вивчення даного питання.

**Мета роботи.** Метою роботи є розробка концепції стенду для вивчення принципів побудови глобальних систем автоматизації з використанням VPN.

**Матеріали і результати досліджень.**

Структура лабораторного стенду для вивчення принципів глобальної комунікації між елементами системи автоматизації представлено на рис.1. Стенд складається з чотирьох ПК та промислового комп'ютера з графічним інтерфейсом XV100.

XV100 – промисловий комп'ютер для розподілених систем автоматизації з операційною системою Windows CE. Комп'ютер інтегрований з кольоровим TFT-дисплеєм з тач-скріном, та має наступні інтерфейси передачі даних: Ethernet, CAN, Profibus, RS232, RS485. Для реалізації функцій промислової

автоматизації на XV100 встановлено програмний ПЛК і середовище для реалізації графічного інтерфейсу Galileo.

Один із стандартних ПК буде виконувати функцію сервера, другий – використовуватись для перевірки можливості несанкціонованого доступу до створеної мережі, а ще два будуть членами захищеної корпоративної мережі.

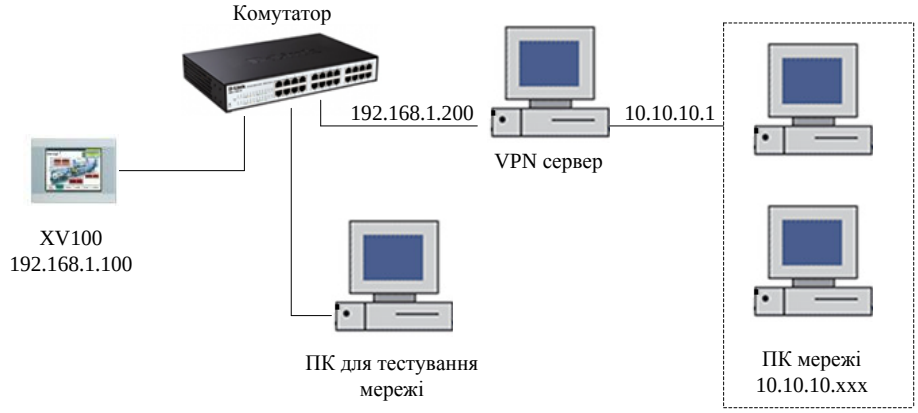


Рисунок 1 – Структура VPN з ПЛК XV100

*Налаштування клієнта.* На XV100 потрібно завантажити операційну систему Windows CE 2.26 і також налаштувати параметри локальної мережі.

Встановлення VPN клієнта відбувається наступним чином: спочатку обирається “Start/Settings/Network and Dialup connections” в операційній системі Windows CE. Далі у вікні необхідно обрати тип з’єднання VPN і задати всі параметри VPN з’єднання.

Далі в програмі Galileo необхідно обрати “Config/CE Configuration” та додати в файл autoexec.bat запис в реєстрі “import VPNconnection.reg –q”, і завантажити будь-який проекту Galileo до панелі після чого VPN клієнт може підключатися до VPN серверу.

*Налаштування сервера.* На комп’ютері, який використовується для налаштування XV100 необхідно встановити Galileo 8.1.1, і налаштувати параметри локальної мережі. На ПК, що працює під ОС Windows, перейти до «Панелі керування», далі до «Мережі та Інтернет», і обрати «Змінити налаштування адаптера». У вкладі «Файл» натиснути на «Нове підключення», знайти панель XV100, вибрати необхідні налаштування та натиснути «Дозволити доступ».

*Перевірка роботи мережі.* На завершальному етапі необхідно перевірити можливість передачі інформації між клієнтом та сервером і перевірити можливість несанкціонованого доступу до мережі з іншого ПК.

**Висновок.** Розроблена концепція буде використана для створення лабораторної установка, яка буде використовуватись в дисципліні «Інтегровані системи» для практичного вивчення принципів налаштування захищеного з’єднання між віддаленими елементами системи автоматизації.

**Перелік посилань**

1. Application Note AP050001EN 1000 Eaton Boulevard Cleveland, -Rev. June 2013
2. Quick Start Guideline [Text]/: manual. Eaton Automation AG, CH-9008 St. Gallen