Герасимчук Є. С., магістр,
Єфіменко А.А., к.т.н., завідувач кафедри,
Житомирський державний технологічний університет

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ ЖИТТЄЗАБЕЗПЕЧЕННЯ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ «INTERNETOFTHINGS»

На сьогоднішній день технологія Інтернет речей (IP) (англ. Internet of Things, IoT) набула великої популярності. Основною концепцією IP є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль. Всі ці об'єкти (речі) повинні бути оснащені вбудованими давачами або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації.

Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, а в разі спекотної погоди будинок має механізми відкривання і закривання вікон, завдяки чому провітрюється будинок, і все це відбувається без втручання людини.

Що стосується об'єктів критичної інфраструктури – це підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення

До системи життєзабезпечення об'єктів критичної інфраструктури входить: водопостачання, електроживлення, теплопостачання, освітлення, вентиляція, протипожежна система. В цілому є три головні вимоги систем життєзабезпечення: простота використання, достатня захищеність та стабільність роботи.

Розглянемо приклад системи управління життєзабезпеченням об'єкту критичної інфраструктури для нафтогазової галузі. Поставлені завдання покладаються на єдину автоматизовану систему контролю та безпеки. В комплексну автоматизовану систему управління, контролю та безпеки повинні входити: 1) система захисту магістральних трубопроводів; 2) система безпеки локальних об'єктів; 3) система захисту інформації; 4) сучасний диспетчерський центр; 5) програмна платформа комплексної безпеки.

Система захисту локальних об'єктів, що складається з комплексу технічних засобів безпеки та включає в себе підсистеми: 1) система охоронного відеоспостереження; 2) система технологічного відеоспостереження; 3) система контролю та управління доступом; 4) система охоронної сигналізації; 5) система охорони периметра.

Для фізичної реалізації такої мережі доцільно застосовувати обладнання та програмне забезпечення компанії Cisco. Зокрема, використовуючи програмний симулятор Cisco Packet Tracer можливо створити програмну модель майбутньої мережі та у режимі реального часу протестувати систему на дію різних факторів, зовнішніх або внутрішніх, відповідно корегуючи налаштування програми-симулятора.

У конкретному випадку це вибір протоколів передачі даних, налаштування мережевого обладнання, спосіб підключення пристроїв між собою, сегментування мережі, застосування групових політик безпеки тощо.

Для ідентифікації кожного об'єкту потрібна проста, компактна технологія. Тільки при наявності системи унікальної ідентифікації можна збирати та накопичувати інформацію про певний предмет. Такий функціонал можна забезпечити за допомогою мікросхем RFID (Radio-Frequency IDentification). Як альтернатива до даної технології для ідентифікації об'єктів можуть використовуватись QR-коди. Для визначення точного місця знаходження речі можливо використати технологію GPS.

Для відслідковування змін у стані елементу чи оточуючого середовища об'єкти повинні оснащуватися сенсорами. Для обробки та накопичення даних з сенсорів повинен використовуватися вбудований комп'ютер (наприклад Raspberry Pi, Intel Edison). Для обміну інформацією між пристроями можуть бути використані технології бездротових мереж (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN).

Таким чином при побудові системи життєзабезпечення об'єкту критичної інфраструктури потрібно враховувати застосування технології IoT та взаємодії між пристроями мережі.

Встановлено, що основною перевагою даної технології є використання стандартних протоколів передачі даних для обміну інформацією між пристроями та надійність системи у цілому.