***Пулеко І. В., канд. техн. наук, доцент кафедри КІтаКБ,***
***Росінський Ю. М., канд. техн. наук, доцент кафедри КІтаКБ***
*Державний університет «Житомирська політехніка»*

# РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ З'ЄДНАНЬ ІНТЕРНЕТУ РЕЧЕЙ

На сьогоднішній день фахівцями з кібербезпеки прийнято виділяти три основні рівні забезпечення безпеки Інтернету речей (англ. Internet of Things, IoT), які пов'язані з архітектурою: рівень сприйняття, мережевий рівень та прикладний рівень.

Рівень сприйняття повинен забезпечувати надійну ідентифікацію об'єктів та зчитування інформації з сенсорів.

Мережевий рівень повинен забезпечувати повсюдний доступ, передачу і зберігання інформації. У межах мережевого рівня виділяють ще два підрівні: підрівень доступу (мережі чи канали зв'язку, що надають доступ до мереж вищого рівня глобальності) і підрівень основного обміну (Інтернет).

Прикладний рівень повинен забезпечувати обробку і аналіз прийнятої інформації для прийняття оптимальних управлінських рішень та контролю за управлінням, додатками і послугами.

Більшість IoT систем на підрівні доступу використовують бездротові мережі зв'язку: персональні мережі (WPAN), локальні мережі (WLAN). Забезпечити безпеку бездротової мережі ще складніше, ніж захистити дротову мережу. В діапазоні дії точки доступу бездротова мережа відкрита для всіх, хто володіє відповідними обліковими даними.

Існує кілька форм загроз безпеці в бездротових мережах. Основні з них це:

Моніторинг трафіку. Відстеження пакетів даних в незахищеній бездротовій мережі, використовуючи відповідні програмні засоби за допомогою яких можна повністю розшифрувати вміст пакетів даних.

Неавторизований доступ. Здійснення моніторингу виконуваних в мережі програм та отримання доступу до бездротової мережі, знаходячись поза приміщенням, де вона функціонує. Навіть якщо в бездротовій мережі задіяні механізми захисту, істотною загрозою є під'єднання до підставної точки доступу (rogue access point).

Атака типу «людина всередині». Розміщення фіктивного пристрою між легальними користувачами і бездротовою мережею, який буде імітувати дійсний. В результаті чого можна отримати доступ до управління сеансами зв'язку користувача, отримати паролі, важливі дані і навіть доступ до корпоративних серверів.

Атака типу «Відмова в обслуговуванні» (denial of service, DoS) – це атака, в результаті якої бездротова мережа стає недоступною або її робота блокується. Серйозність DoS-атаки залежить від того, до яких наслідків може привести вихід з ладу бездротової мережі.

Іншим методом припинення роботи більшості бездротових мереж є використання сильного радіосигналу, що «глушить» всі інші.

Єдиної і повністю надійної системи захисту IoT систем, що застосовують бездротові мережі не існує. Однак, дотримання досить простих рекомендацій дозволить значно знизити ризики та ускладнити роботу зловмисника щодо зламу системи IoT чи несанкціонованого доступу до інформації.

Система безпеки бездротових мереж найбільш часто реалізується в точці доступу або в місці, де здійснюється бездротове підключення до мережі тому рекомендується здійснювати:

– зміна всіх налаштувань за замовчуванням;
– налаштування захисту адміністративного доступу;
– налаштування надійних протоколів аутентифікації зі стійкими паролями;
– включення шифрування;
– своєчасне оновлення мікропрограм.

Також не існує універсального способу протидії DoS-атакам всіх типів. Однак серед найбільш дієвих видів захисту дотримання таких правил безпеки:

– встановлення та оновлення брандмауерів;
– постійне оновлення антивірусних програмних засобів;
– встановлення останніх оновлень, за допомогою яких ліквідовують недоліки в системі безпеки операційної системи;
– використання довгих паролів;
– від'єднання мережевих пристроїв, які не використовуються.

Як засоби додаткового захисту бездротових мереж можна рекомендувати: фільтрацію за MAC адресою; приховування SSID; заборону доступу до налаштувань точки доступу чи роутера через бездротову мережу. Навіть незважаючи на застосування зазначених вище рекомендацій не можна гарантувати повної безпеки IoT системи. Тому, при виборі нових пристроїв з підтримкою бездротового зв'язку, що підключаються до всеосяжного Інтернету, слід особливу увагу звертати на появу нових функцій захисту бездротової мережі.