УДК 621.396.43

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В WI-FI МЕРЕЖІ СТАНДАРТУ 802.11

Єрмаков А.В., Постернак Б.С., Сарапулов С.В.
Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна
E-mail: yermak_antonio@ukr.net

Protecting personal data with 802.11 Wi-Fi network

Degree of protection off-wire networks. Methods of code mechanisms in the networks of Wi - Fi and code types.

Прилади стандарту 802.11 з'єднуються один з одним, використовуючи у якості переносника інформаційні сигнали, що передаються в спектрі радіочастот. Відомості переходять згідно радіомовлення відправником, який вважає, що радіоприймач крім того функціонує в обраному радіодіапазоні. Мінусом подібного пристосування вважається в цьому випадку, те, що будь-яка інша база, яка використовує даний спектр, також може здійснити ці відомості. У разі якщо не використовувати будь-який режим захисту, кожну базу вважаємо еталоною 802.11, яка взмозі обробити відомості, надіслані згідно з безпроводові місцеві мережі, в разі якщо тільки її радіоприймач функціонує в цьому ж радіодіапазоні. З метою надання хоча б одного мінімального ступеню захищеності потрібні наступні складові методи:

1. З метою прийняття постанови, що здатна застосовувати безпроводову LAN. Дана умова задовольняється за рахунок пристосування аутентифікації, яка забезпечує контролювання доступу до LAN.

2. Ресурси захисту даних, що подаються за допомогою безпроводової мережі. Дана умова задовольняється за рахунок використання алгоритмів кодування. У специфікації стандарту 802.11 регламентовано застосування механізму аутентифікації пристроїв з відкритим і до спільно використовуваним ключем та механізму WEP, що забезпечує захищеність даних.

Механізми кодування базуються в методах, які вважають за краще випадковим чином відомості. Застосовуються два типи шифрів: поточний та блочний шифри.

Шифри двох видів працюють, генеруючи першорядний потік (key stream). Ключовий потік змішується з відомостями, або не закритим словом, внаслідок чого ж утворюється кодований вихідний знак. Вище названі два типи шифрів розрізняються відповідно до розміру інформації, з якими вони можуть працювати в той же час.

Однопотоковий шифр виробляє безперервний проводовий потік, спираючись в значенні ключа. Наприклад, однопотоковий шифр здатний виробляти 15-розрядний ключовий потік з метою кодування однієї грані і 200-розрядним ключовим потоком з метою кодування другого. У рис. 1.1 проілюстрована діяльність поточного шифру. Більш популярним вважається однопотоковий шифр RC4, який і знаходиться в базі методу WEP. Блоковий шифр, навпаки, виробляє винятковий ключовий потік кодування зафіксованого обсягу. Розкритий документ ділиться в блоки чи будь-яке джерело, яке змішується з основним потоком незалежно. У разі якщо джерело прямого слова менш ніж джерело основного потоку, перший розширюється з вилученням блоку необхідного обсягу. У рис.1.2 проілюстрована діяльність блочного коду.

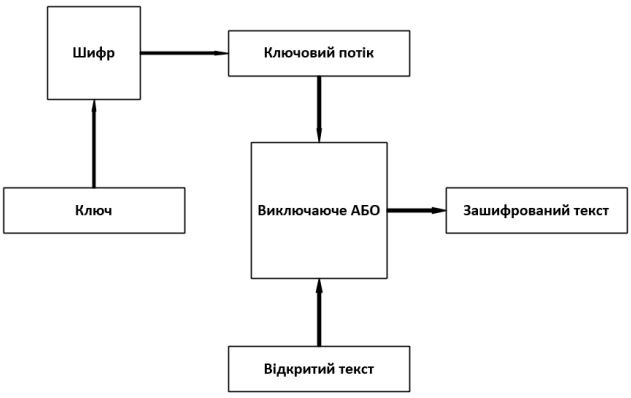

Рис. 1.1. Здійснюється потокове шифрування

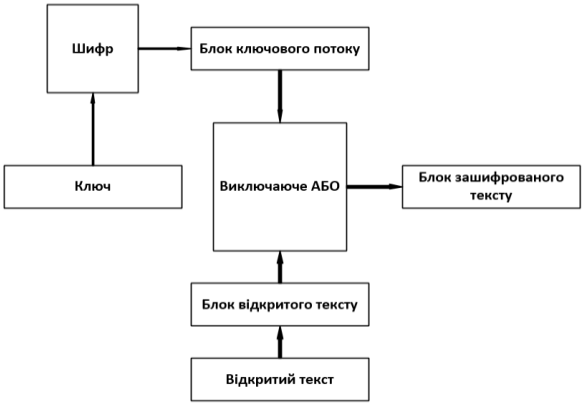

Рис. 1.2. Здійснюється блочне шифрування.

Процедура кодування з механізмом поточних і блокових шифрів, називається порядком кодування с підтримкою бази електроних кодів (Electronic Code Book, ECB). Порядок шифрування ECB характеризується тим, що єдиний і цей же розкритий документ вже після кодування реорганізується в єдиний і цей же закодований документ.

Способи кодування дають можливість знайти рішення:

1. Вектори ініціалізації (initialization vectors, IV).

2. Режими зі зворотним зв'язком (feedback modes).

Вектор ініціалізації - це номер, що додається до ключа, кінцевим результатом цього вважається зміна даних основного потоку. Вектор ініціалізації весь час змінюється, в такому випадку те саме відбувається з основним потоком. У рис. 1.3 (а, б) представлені 2 сценарії. 1-ий належить до шифрування із застосуванням поточного коду в відсутності використання вектора ініціалізації. В даному випадку розкритий документ DATA вже після змішування з основним потоком 12345 постійно реорганізується в закодований документ AHGHE. Другий план демонструє, як той же

розкритий документ змішується з основним потоком, доповненим вектором ініціалізації з метою вилучення іншого зашифрованого тексту. Звернемо увагу на те, що закодований документ у другому випадку розрізняється в першому. Зразок 802.11 радить міняти вектор ініціалізації пофреймово (on a per-frame basis). Це означає, то що, якщо один і той же фрейм відданий двічі, досить високою виявиться можливість цього, то, що закодований документ стане різним.

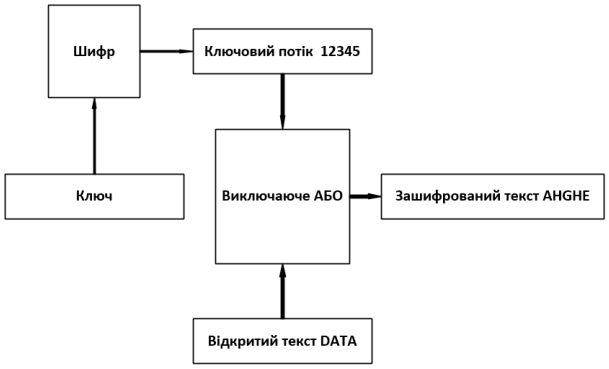

Рис. 1.3(а) – Шифрування без вектора ініціалізації.

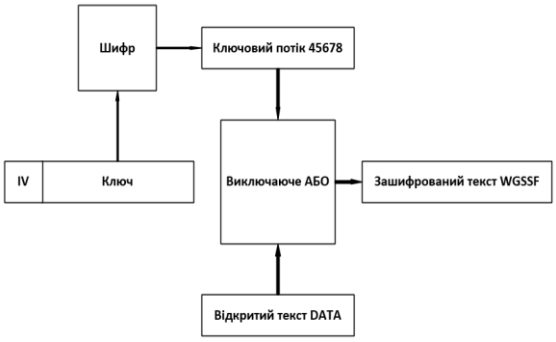

Рис. 1.3(б) – Шифрування і вектори ініціалізації

Специфікація стандарту 802.11 передбачає гарантування захисту інформації з використанням методу WEP. Даний метод базується в застосуванні симетричного поточного коду RC4. Симетричність RC4 означає, те, що узгоджені WEP-шлюзи величиною 40 або 104 біт статично змінюються в клієнтських пристроях і в місцях доступу. Метод WEP був обраний ключовим способом внаслідок того, що він ніяк не вимагає занадто великих обчислень. Для того щоб виключити кодування в режимі ECB, WEP використовує 24-розрядний вектор ініціалізації, який додається до ключу перед виконанням оброблення згідно з методом RC4. Специфікація стандарту 802.11 вимагає, щоб схожі WEP-джерела були налаштовані як в клієнтах, таким чином і в пристроях інфраструктури мережі

Література

1. Свідоцтво про авторське право на твір №76226 від 24.01.2018 р. «Модель проектування бездротової мережі Wi-Fi на основі стандарту 802.11». Автори: Єрмаков А.В., Наритник Т.М., Авдєєнко Г.Л., Вальчук Д.С., Бондарчук С.О., Гошко А.П., Сердюк Д.О.
2. Свідоцтво про авторське право на твір №66937 від 29.07.2016 «Модель процесу управління захистом від перенавантажень мереж передачі даних». Автори: Романов А.І., Єрмаков А.В.