ХАРЬКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

# БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ

## ЛЕКЦІЯ 6

Доцент кафедри кібербезпеки та ІТ
к.т.н. Лимаренко Вячеслав Володимирович
к.т. 066-0708586 (Viber, Telegram)

Найбільш поширена проблема в таких відкритих і некерованих середовищах, як бездротові мережі, - можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати дані, що передаються, як показано на рисунку 1.


Рис. 1 Атака «підслуховування»

# ВІДМОВА В ОБСЛУГОВУВАННІ (DENIAL OF SERVICE, DOS)

Повну паралізації мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися один з одним (рис. 2.). Ця атака вимикає всі комунікації в певному районі. Якщо вона проводиться в досить широкій області, то може вимагати значних потужностей. Атаку DOS на безпровідні мережі важко запобігти або зупинити. Більшість бездротових мережевих технологій використовує неліцензовані частоти - отже, допустима інтерференція від цілого ряду електронних пристроїв.


Рис. 2 Атака «відмова в обслуговуванні» в бесзпровідних комунікаціях

# ГЛУШІННЯ КЛІЄНТСЬКОЇ СТАНЦІЇ

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, таким чином, виводячи цей канал з ладу. Атакуючий може використовувати різні способи глушіння.

Глушіння клієнтської станції дає можливість шахраєві підставити себе на місце заглушеного клієнта, як показано на рисунку 3. Також глушіння можуть використовувати для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.


Рис. 3 Атака глушіння клієнта для перехоплення з’єднання

# ГЛУШІННЯ БАЗОВОЇ СТАНЦІЇ

Глушіння базової станції надає можливість підмінити її атакуючої станцією, як показано на рисунку 4. Таке глушіння позбавляє користувачів доступу до послуг.

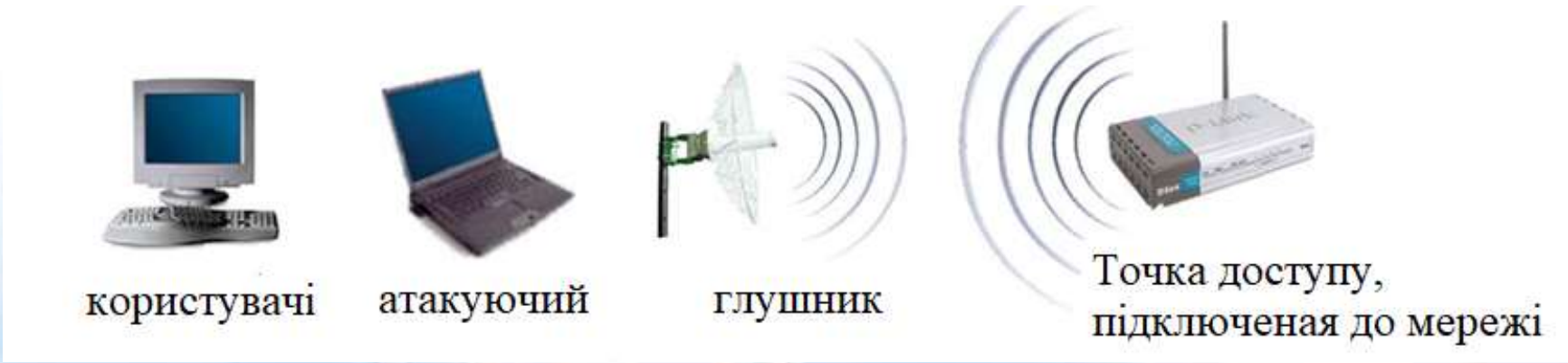



Рис. 4 Атака глушіння базової станції для перехоплення з'єднання

# ЗАГРОЗИ КРИПТОЗАХИСТУ

WEP - це криптографічний механізм, створений для забезпечення безпеки мереж стандарту 802.11. Цей механізм розроблений з єдиним статичним ключем, який застосовується всіма користувачами. Керуючий доступ до ключів, часте їх зміна і виявлення порушень практично неможливі. Дослідження WEP-шифрування виявило вразливі місця, через які атакуючий може повністю відновити ключ після захоплення мінімального мережевого трафіку. В Інтернет є кошти, які дозволяють зловмисникові відновити ключ протягом декількох годин. Тому на WEP не можна покладатися як на засіб аутентифікації і конфіденційності в бездротовій мережі.

# БАЗОВІ ТЕРМІНИ ТА ЇХ ВИЗНАЧЕННЯ

**АУТЕНТИФІКАЦІЯ:** визначення джерела інформації, тобто кінцевого користувача або пристрою (центрального комп'ютера, сервера, комутатора, і т. д.).
**ЦІЛІСНІСТЬ ДАНИХ**: забезпечення незмінності даних в ході їх передачі.
**КОНФІДЕНЦІЙНІСТЬ ДАНИХ**: забезпечення перегляду даних в прийнятному форматі тільки для осіб, які мають право на доступ до цих даних.
**ШИФРУВАННЯ**: метод зміни інформації таким чином, що прочитати її не може ніхто, крім адресата, який повинен її розшифрувати.
**РОЗШИФРУВАННЯ:** метод відновлення зміненої інформації і приведення її в читається вигляд.
**КЛЮЧ**: цифровий код, який може використовуватися для шифрування і розшифровки інформації, а також для її підпису.
**ЗАГАЛЬНИЙ КЛЮЧ**: цифровий код, який використовується для шифрування / розшифрування інформації та цифрових підписів; цей ключ може бути широко поширений; загальний ключ використовується з відповідним приватним ключем.
**ПРИВАТНИЙ КЛЮЧ**: цифровий код, який використовується для шифрування / розшифрування інформації та цифрових підписів; власник цього ключа повинен тримати його в секреті; приватний ключ використовується з відповідним загальним ключем.

# БАЗОВІ ТЕРМІНИ ТА ЇХ ВИЗНАЧЕННЯ

**СЕКРЕТНИЙ КЛЮЧ**: цифровий код, яким користуються двома сторонами для шифрування і розшифровки даних.

**ХЕШ-ФУНКЦІЯ**: математичний розрахунок, результатом якого є послідовність бітів (цифровий код). Маючи цей результат, неможливо відновити вихідні дані, використані для розрахунку.

**ХЕШ:** послідовність бітів, отримана в результаті розрахунку хеш-функції. Результат обробки повідомлення (Message digest): величина, яка видається хеш-функцією (те саме, що і «хеш»).

**ШИФР:** будь-який метод шифрування даних.

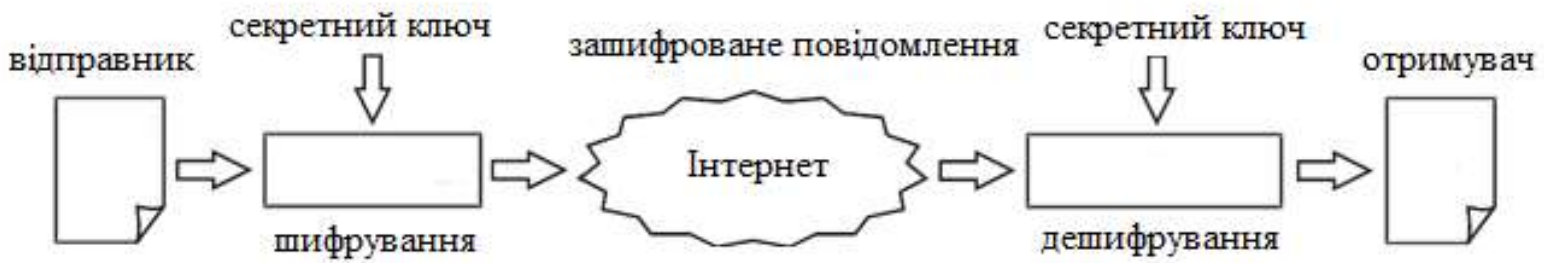
**ЦИФРОВИЙ ПІДПИС**: послідовність бітів, яка додається до повідомлення (Зашифрований хеш), яка забезпечує аутентифікацію і цілісність даних.

**AAA** (Authentication, Authorization, Accounting): архітектура аутентифікації, авторизації та обліку.

**VPN** (Virtual Private Networks): віртуальні приватні мережі.

**IDS** (Intrusion Detection System): системи виявлення вторгнень.

## СИММЕТРИЧНЕ ШИФРУВАННЯ




## АСИММЕТРИЧНЕ ШИФРУВАННЯ

# БЕЗПЕЧНА ХЕШ ФУНКЦІЯ

Безпечною хеш-функцією називається функція, яку легко розрахувати, але зворотне відновлення практично неможливо, так як вимагає непропорційно великих зусиль. Вхідне повідомлення пропускається через математичну функцію (хеш-функцію), і в результаті на виході ми отримуємо якусь послідовність бітів (рис. 5). Ця послідовність називається «хеш» (або «результат обробки повідомлення»). Хеш-функція приймає повідомлення будь-якої довжини і видає на виході хеш фіксованої довжини.


Рис. 5 Обчислення хеш-функції

Звичайні хеш-функції включають:

- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритм безпечного хеша (Secure Hash Algorithm, SHA).

# ЦИФРОВА ПІДПИС

Цифровий підпис є зашифрований хеш, який додається до документа. Принцип шифрування з цифровим підписом легко зрозуміти з рисунка 6.

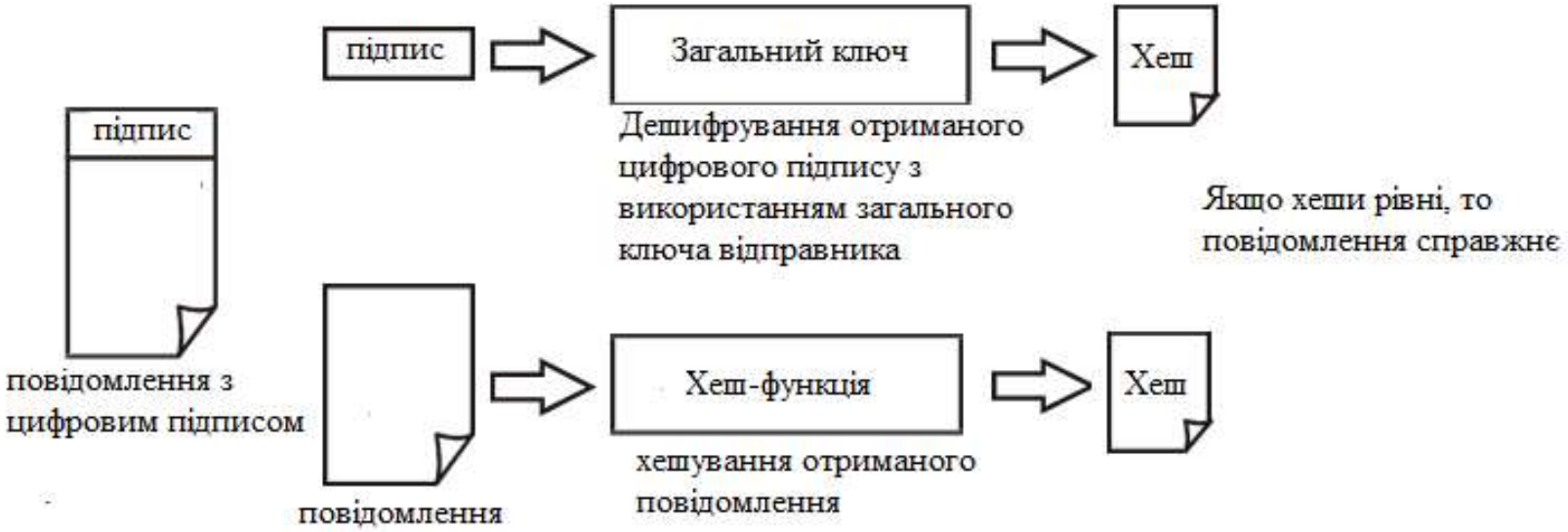



Рис. 6 Перевірка справжності повідомлення з цифровим підписом

Вона може використовуватися для аутентифікації відправника та цілісності документа. Цифрові підписи можна створювати за допомогою поєднання хеш-функцій і криптографії загальних ключів.

# ЦИФРОВИЙ СЕРТИФІКАТ

Цифровим сертифікатом називається повідомлення з цифровим підписом, яке в даний час зазвичай використовується для підтвердження дійсності загального ключа. Загальний формат широко поширеного сертифіката X.509, включає наступні елементи:

- номер версії;
- серійний номер сертифіката;
- емітент інформації про алгоритм;
- емітент сертифікату;
- дати початку і закінчення дії сертифіката;
- інформацію про алгоритм загального ключа суб'єкта сертифіката;
- підпис емітує організації.

# ЦИФРОВИЙ СЕРТИФІКАТ

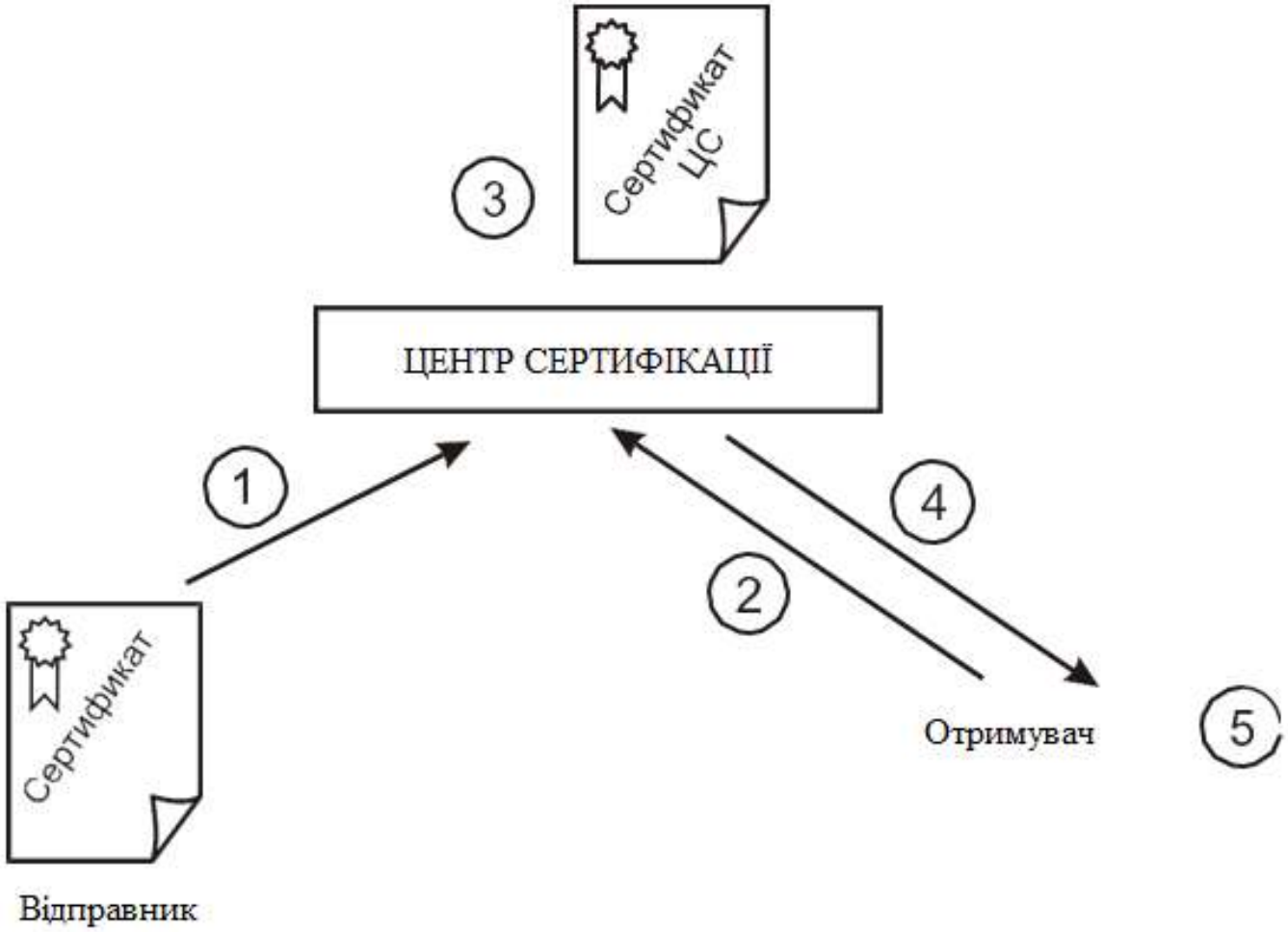



Рис. 7. Передача ключа с цифровим сертифікатом

# МЕХАНІЗМ ШИФРУВАННЯ WEP

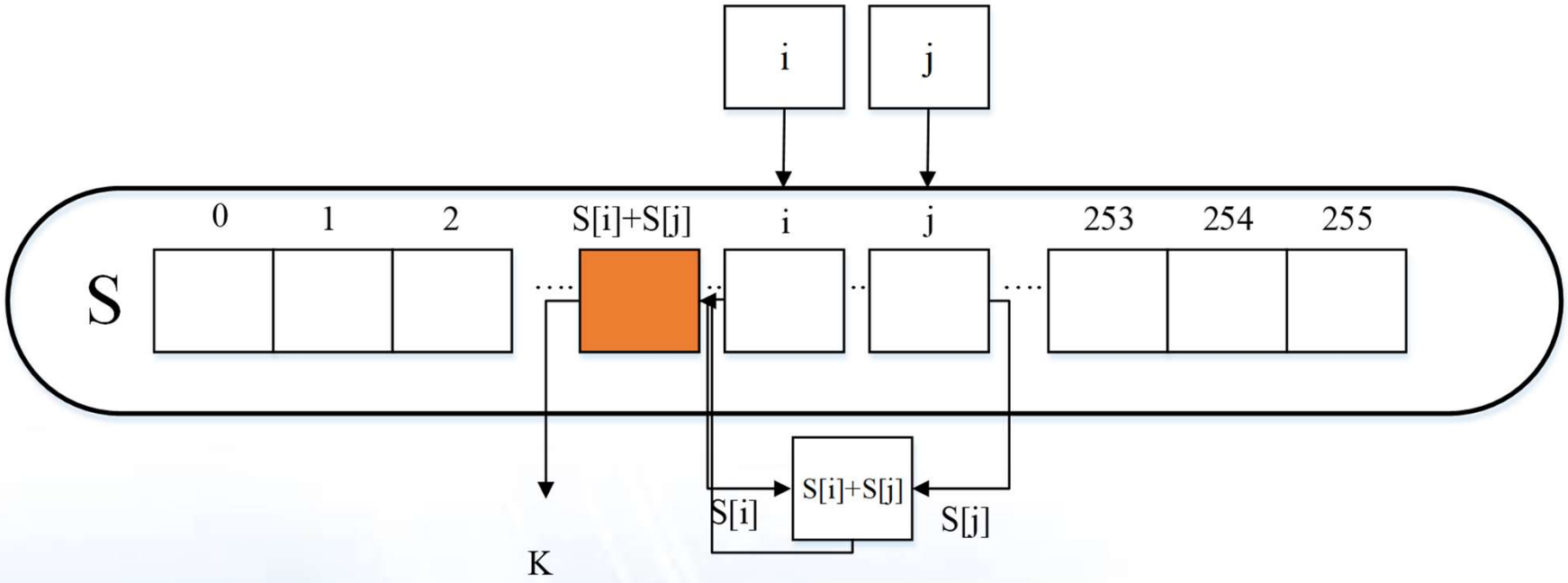



Рис. 7. Алгоритм поточного шифрування RC4

Шифрування WEP (Wired Equivalent Privacy, секретність на рівні дротового зв'язку) засновано на алгоритмі RC4 (Rivest's Cipher v.4, код Ривеста), що представляє собою симетричне потокове шифрування, для нормального обміну даними користувачів ключі шифрування у абонента і точки радіодоступу повинні бути ідентичними.

# ПОТОКОВЕ ШИФРУВАННЕ/БЛОЧНЕ ШИФРУВАННЯ

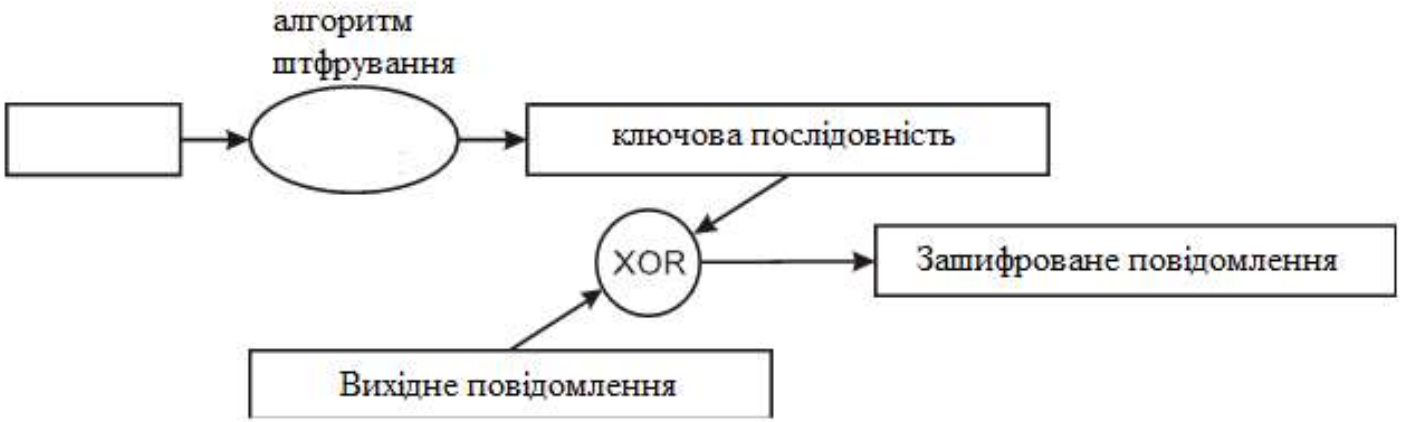



Рис. 8. Потоковое шифрование

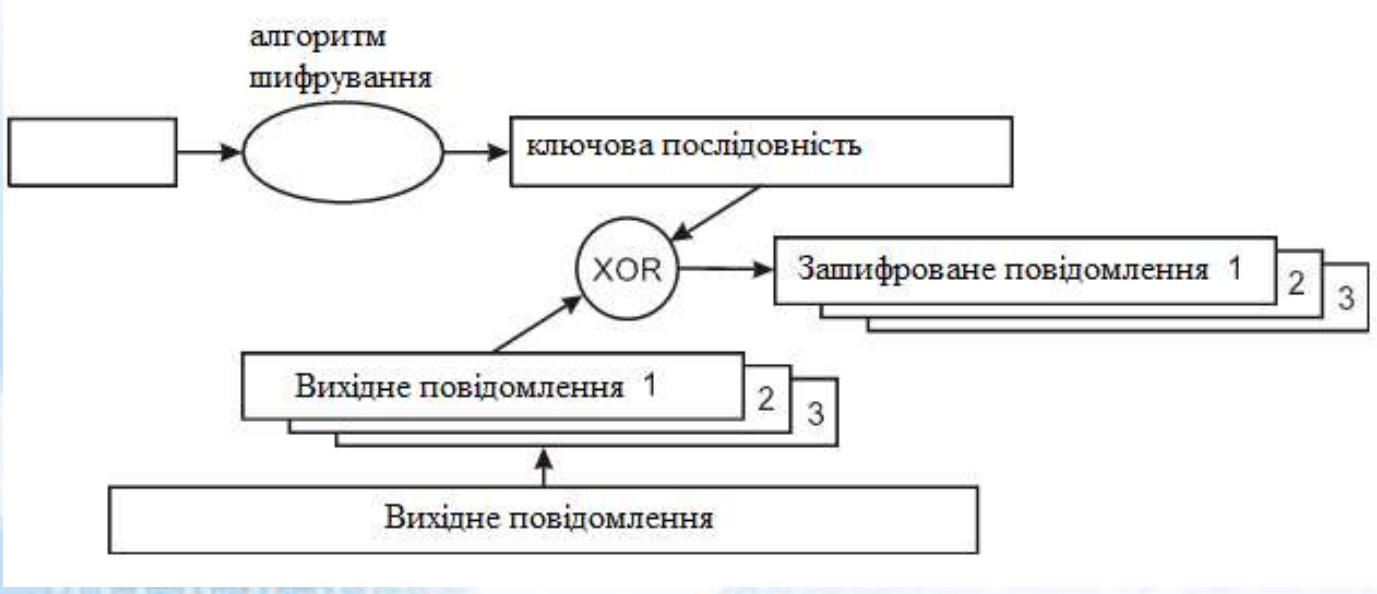



Рис. 9. Блочне шифрование

# ШИФРОВАННЯ ЗІ ЗВОРОТНИМ ЗВ'ЯЗКОМ

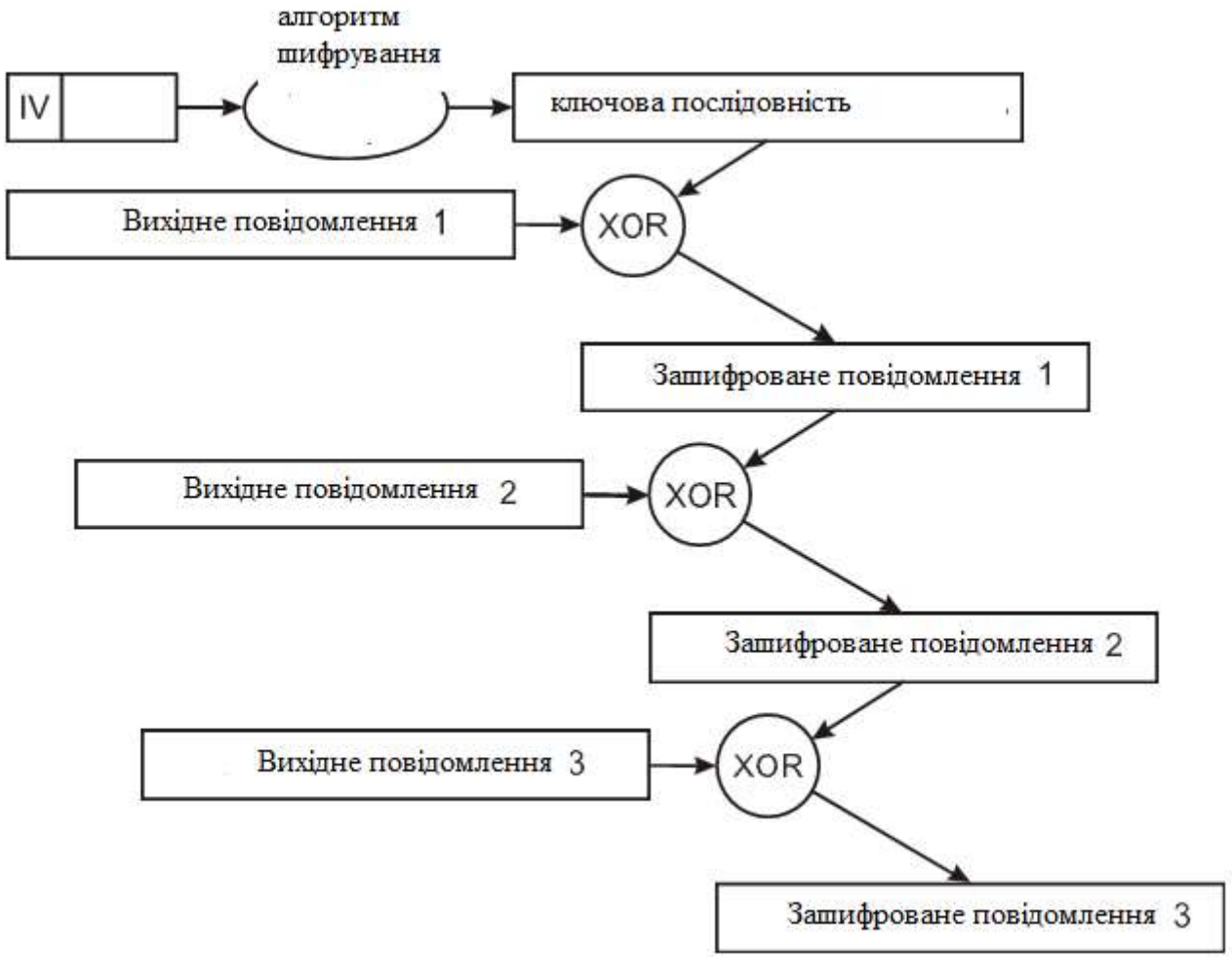



Рис. 10. Шифрування зі зворотним зв'язком

# АКТИВНІ МЕРЕЖЕВІ АТАКИ


Рис. 11. Повторне використання вектора ініціалізації

# АКТИВНІ МЕРЕЖЕВІ АТАКИ

1. Хакер багаторазово надсилає абоненту бездротову локальну мережу по провідній мережі повідомлення відомого змісту (наприклад, IP-пакет, лист електронної пошти, і т.п.).
2. Хакер пасивно прослуховує радіоканал зв'язку абонента з точкою радіодоступу і збирає фрейми, імовірно містять шифрування повідомлення.
3. Хакер обчислює ключову послідовність, застосовуючи функцію XOR до передбачуваного шифрованому і відомому нешифрований повідомленнями.
4. Хакер «вирощує» ключову послідовність для пари вектора ініціалізації і секретного ключа, що породила ключову послідовність, обчислену на попередньому кроці.

В основі атаки лежить знання того, що пара вектора ініціалізації і секретного ключа шифрування, а значить і породжувана ними ключова послідовність, може бути повторно використана для відтворення ключовий послідовності достатньої довжини для порушення конфіденційності через бездротову локальну мережу в умовах використання WEP.

Після того, як ключова послідовність обчислена для фреймів деякої довжини, вона може бути «вирощена» до будь-якого необхідного розміру, як описано нижче і проілюстровано на рис. 11.

# АКТИВНІ МЕРЕЖЕВІ АТАКИ

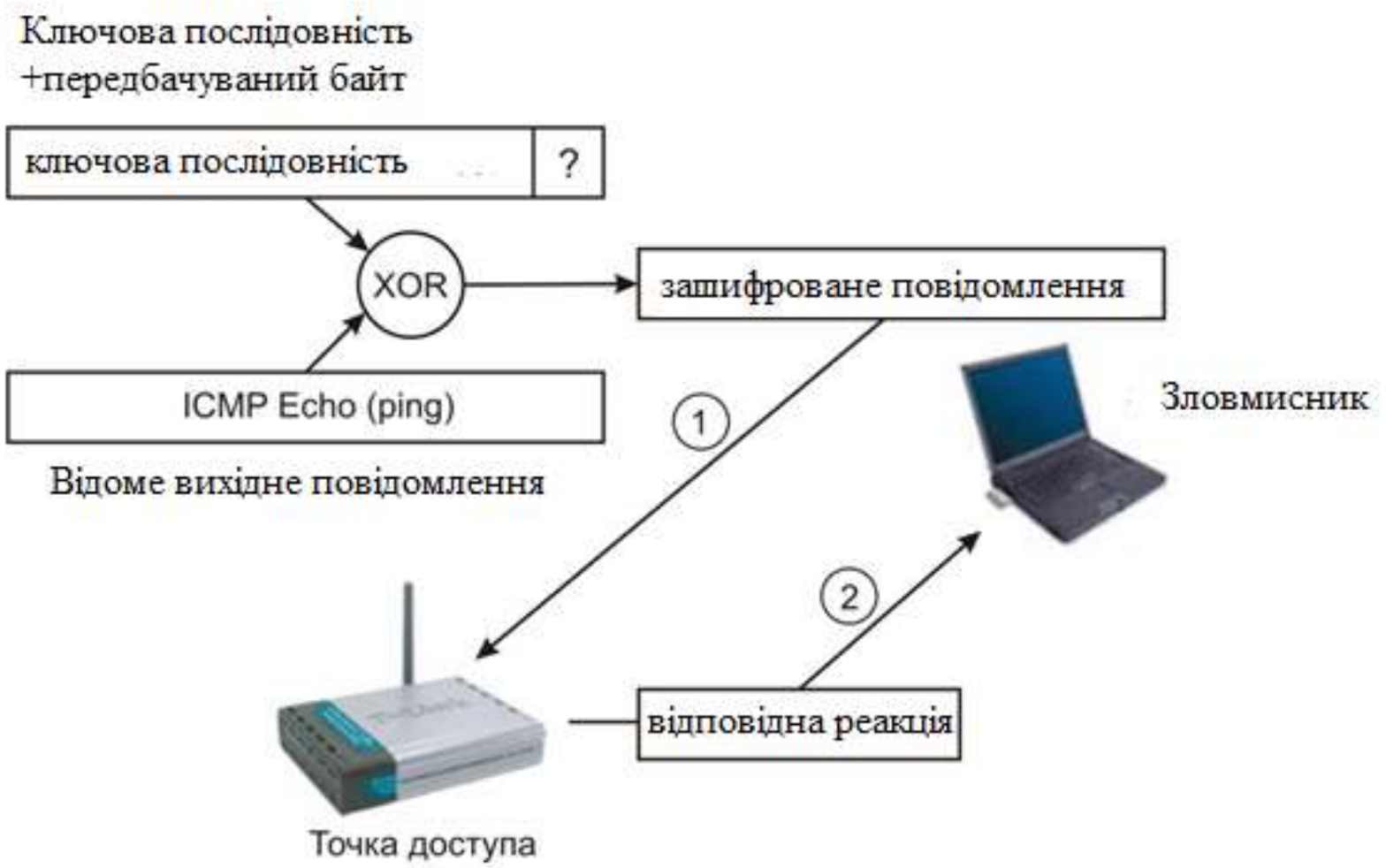



Рис. 11.«Вирощування» ключовий послідовності

# АКТИВНІ МЕРЕЖЕВІ АТАКИ

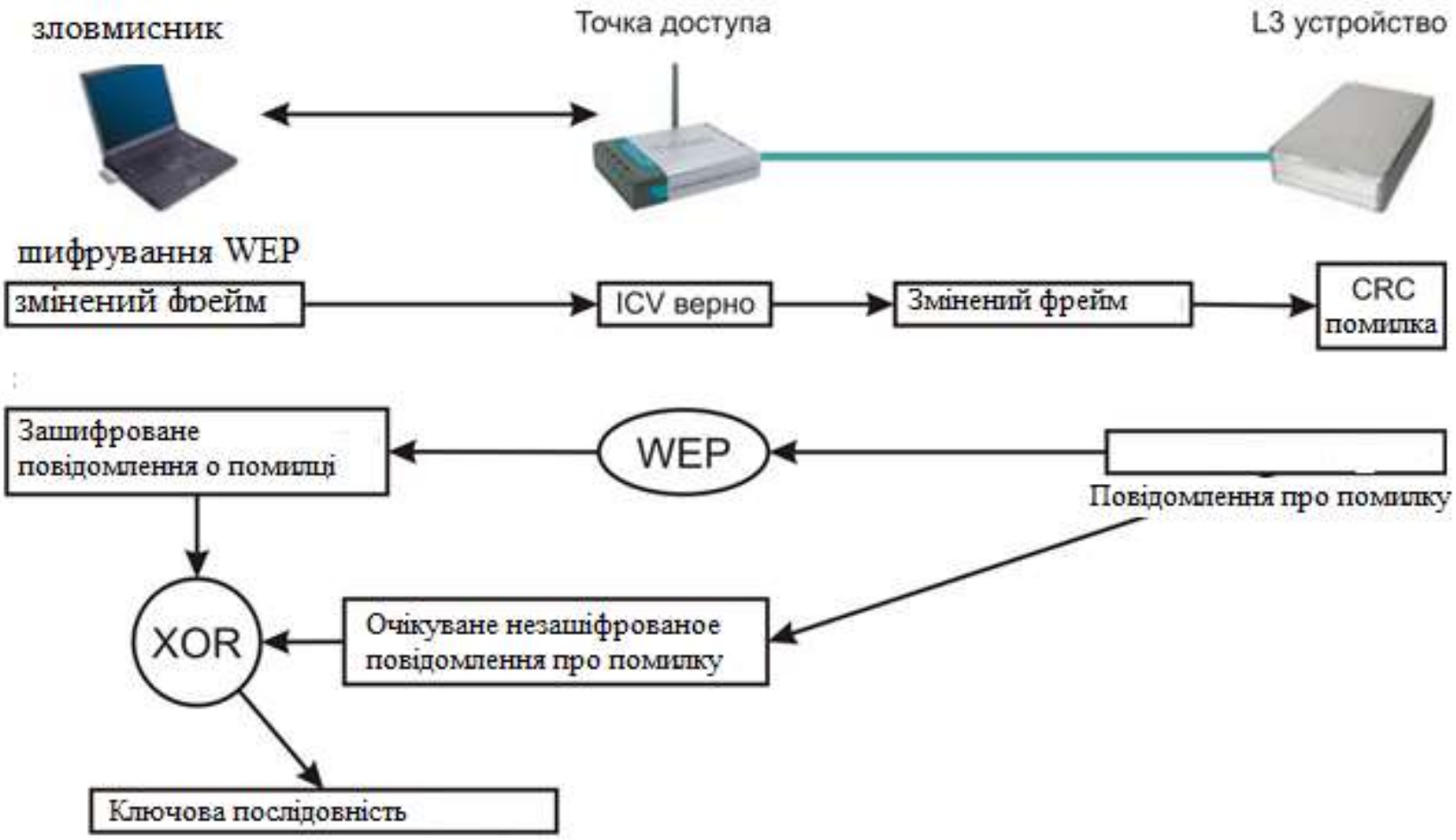



Рис. 12. Атака с манипуляцией битами

# АКТИВНІ МЕРЕЖЕВІ АТАКИ

Маніпуляція бітами (Bit-Flipping Attacks)

Маніпуляція битами переслідує ту ж мету, що і повторне використання вектора ініціалізації, і спирається на вразливість вектора контролю цілісності фрейма ICV. Призначені для користувача дані можуть відрізнятися від фрейму до фрейму, в той же самий час багато службові поля та їх положення усередині кадру не змінюється.

Хакер маніпулює битами призначених для користувача даних усередині фрейму 2-го (канального) рівня моделі OSI (Open Systems Interconnection) з метою спотворення 3-го (мережевого) рівня пакета. Процес маніпуляції проілюстрований на рис. 2.16.

1. Хакер пасивно спостерігає фрейми бездротову локальну мережу за допомогою засобів аналізу трафіку протоколу 802.11.
2. Хакер захоплює фрейм і довільно змінює біти в поле даних протоколу
3-го рівня.
3. Хакер модифікує значення вектора контролю цілісності фрейма ICV (як саме буде описано нижче).
4. Хакер передає модифікований фрейм в бездротову локальну мережу.
5. Приймаюча сторона (абонент або точка радіодоступу) обчислює значення вектора контролю цілісності фрейма ICV для отриманого модифікованого фрейма.
6. Приймаюча сторона порівнює обчислене значення вектора ICV з наявними в отриманому модифікованому фреймі.
7. Значення векторів збігаються, кадр вважається неспотвореним і не відкидається.
8. Приймаюча сторона деінкапсулірует вміст фрейма і обробляє пакет мережевого рівня.
9. Оскільки маніпуляція бітами відбувалася на канальному рівні, контрольна сума пакета мережного рівня виявляється невірною.
10. Стек протоколу мережевого рівня на приймаючій стороні генерує передбачуване повідомлення про помилку.
11. Хакер спостерігає за бездротовою локальною мережею в очікуванні зашифрованого фрейму з повідомленням про помилку.
12. Хакер захоплює фрейм, що містить зашифроване повідомлення про помилку і обчислює ключову послідовність, як це було описано раніше для атаки з повторним використанням вектора ініціалізації.

# АУТЕНТИФІКАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ

Основними стандартами аутентифікації в бездротових мережах є стандарти IEEE 802.11, WPA, WPA2 і 802.1x.. Розглянемо основи цих стандартів.

Стандарт IEEE 802.11 з традиційною безпекою (Tradition Security Network, TSN) передбачає два механізми аутентифікації бездротових абонентів: відкриту аутентифікацію (Open Authentication) і аутентифікацію із загальним ключем (Shared Key Authentication). У аутентифікації в бездротових мережах також широко використовуються два інших механізму виходять за рамки стандарту 802.11, а саме призначення ідентифікатора бездротової локальної мережі (Service Set Identifier, SSID) і аутентифікація абонента по його MAC-адресу (MAC Address Authentication).

# АУТЕНТИФІКАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ
## Принцип аутентифікації абонента в IEEE 802.11

Аутентифікація в стандарті IEEE 802.11 орієнтована на аутентифікацію абонентського пристрою радіодоступу, а не конкретного абонента як користувача мережевих ресурсів. Процес аутентифікації абонента бездротової локальної мережі IEEE 802.11 складається з наступних етапів (рис. 2.18):

1. Абонент (Client) посилає фрейм Probe Request в усі радіоканали.
2. Кожна точка радіодоступу (Access Point, AP), в зоні радиовидимости якої знаходиться абонент, посилає у відповідь кадр Probe Response.
3. Абонент вибирає кращу для нього точку радіодоступу і посилає в обслуговується нею радіоканал запит на аутентифікацію (Authentication Request).
4. Точка радіодоступу посилає підтвердження аутентифікації (Authentication Reply).
5. У разі успішної аутентифікації абонент посилає точці радіодоступу фрейм асоціації (Association Request).
6. Точка радіодоступу посилає у відповідь кадр підтвердження асоціації (Association Response).
7. Абонент може тепер здійснювати обмін призначеним для користувача трафіком з точкою радіодоступу та провідний мережею.

# АУТЕНТИФІКАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ
## Принцип аутентифікації абонента в IEEE 802.11

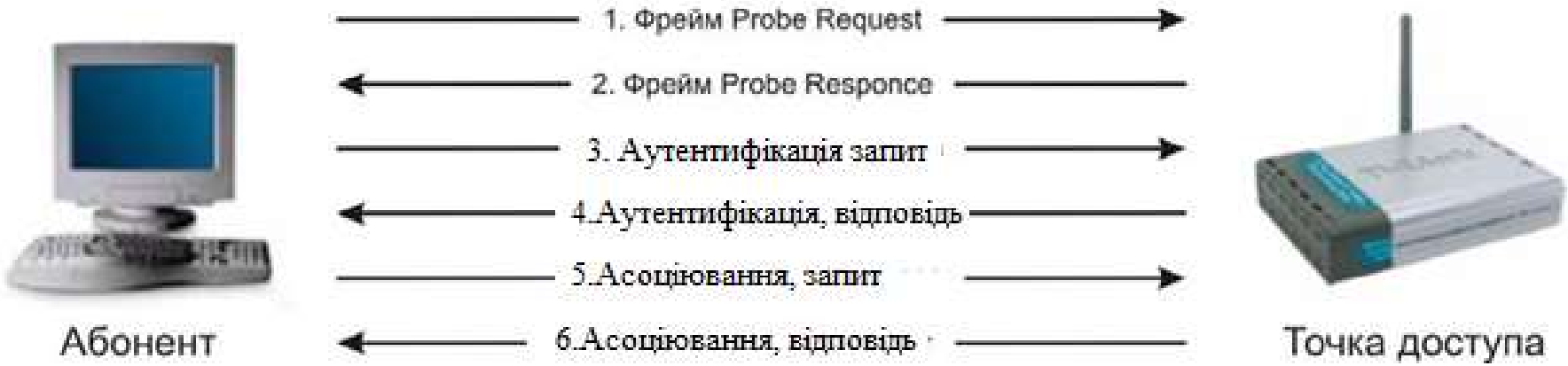



Рис. 13 Аутентифікація по стандарту 802.11

# АУТЕНТИФІКАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ
## Відкрита аутентифікація

В процесі відкритої аутентифікації відбувається обмін повідомленнями двох типів:
- запит аутентифікації (Authentication Request);
- підтвердження аутентифікації (Authentication Response).

Таким чином, при відкритій аутентифікації можливий доступ будь-якого абонента до бездротової локальної мережі. Якщо в бездротової мережі не використовується шифрування, то будь-який абонент, що знає ідентифікатор SSID точки радіодоступу, отримає доступ до мережі. При використанні точками радіодоступу шифрування WEP самі ключі шифрування стають засобом контролю доступу. Якщо абонент не має коректним WEP-ключем, то навіть у разі успішної аутентифікації він не зможе ні передавати дані через точку радіодоступу, ні розшифровувати дані, передані точкою радіодоступу (рис. 14).


Рис. 14 Відкрита аутентифікація