

## ПЕРЕДАЧА ПРИХОВАНИХ ПОВІДОМЛЕНЬ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

*Ничипоренко С. В., магістрант*

*Національний технічний університет України  
«Київський політехнічний інститут», м. Київ, Україна*

На сьогодні, проблема забезпечення конфіденційності даних являється надзвичайно гострою. Тим більше, якщо ці дані потрібно передавати мережею.

Одним із способів захисту може стати шифрування даних (криптографія), але виявлення самого факту шифрування означає, що передаються секретні дані.

Іншим способом захисту даних є стеганографія. Ідея стеганографії полягає в тому, щоб приховати сам факт передачі конфіденційних даних.

Перевага стеганографії над криптографією полягає в тому, що повідомлення не привертає до себе уваги. Як правило, повідомлення буде виглядати, як малюнок, стаття, листівка або навіть аудіо потік [1].

Приховані за допомогою стеганографії дані можна передавати через мережі мобільного зв'язку. Це дає ряд переваг:

- дані при передачі шифрують, що дає додатковий захист даних [2];
- мобільні телефони широко розповсюджені, мають невеликі габарити та вагу;
- покриття мобільного зв'язку охоплює значні території;
- дані передаються в режимі реального часу.

Недоліком є те, що при апаратній реалізації стеганокодера, необхідно змінювати схемотехнічне рішення телефону, що не завжди можливо і виправдано. Обійти цей недолік дозволяє використання бездротової (*Bluetooth*) гарнітури. Використання гарнітури дає додаткові переваги:

- не змінюється схемотехнічне рішення телефону;
- одна і та ж гарнітура може використовуватись з різними телефонами;
- передача прихованих даних буде відбуватися під час звичайної розмови по телефону.

Розглянемо одну з можливих реалізацій даної системи прихованої передачі даних. Маємо *Bluetooth*-гарнітуру в яку вбудовано стеганокодер. Стеганокодер вбудовує секретні дані (наприклад прочитані з карти пам'яті) в пакет даних, що передається від *Bluetooth*-гарнітури до телефону.

Для цього можна використати інтерфейси, що наявні в *Bluetooth*-модулях. Для прикладу *Bluetooth*-модуль *LMX9838* фірми *National Semiconductor* має наступні інтерфейси, які можна використати для наших цілей:

- цифровий аудіоінтерфейс для підключення зовнішнього PCM-кодека;

- інтерфейс *UART*, призначений для передачі цифрової інформації.

Далі відбувається звичайна розмова по телефону. На іншій стороні використовується така ж *Bluetooth*-гарнітура, яка з отриманого пакету даних відокремлює секретні дані. Це відбувається за допомогою стеганодекодера вбудованого в гарнітуру.

При такій реалізації передача даних відбувається лише в одну сторону, тобто напівдуплексна передача, але для передачі коротких повідомлень вона повністю виправдана.

#### **Література**

1. Википедия. Стеганографія. — Електрон. дані: <http://ru.wikipedia.org> — Назва з екрана.
2. Википедия. GSM. — Електрон. дані: <http://ru.wikipedia.org/wiki/GSM> — Назва з екрана.
3. Офіційний сайт Bluetooth Special Interest Group. — Електрон. дані: <https://bluetooth.org> — Назва з екрана.