УДК 621.396:004.056

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Павлов В.В.
Науковий керівник – ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: volodymyr.pavlov@nure.ua

The paper discusses passive and active methods of protecting information in cellular communication channels. Methods using cryptographic algorithms for encrypting speech information are promising. It has been established that the most effective is the integrated use of the considered methods.

У період стрімкого розвитку цифрових технологій, інтенсивного зростанням обсягів обміну даними та глибокої інтеграції мобільних технологій у наше повсякденне життя проблема захисту інформації від витоку каналами стільникового зв'язку належить до надзвичайно важливих завдань. Сучасні засоби мобільного зв’язку дають людині багато можливостей для обміну інформацією, але стільниковий телефон може використовуватися як пристрій негласного знімання інформації.

Захист інформації від витоку каналами стільникового зв'язку необхідно вирішувати комплексно, при використанні пасивних, активних та програмних методів захисту, таких як: екранування, індикація несанкціонованої активності мобільного пристрою, активне зашумлення, шифрування трафіку та маскування мовної інформації, а також методи ідентифікації та блокування несанкціонованого доступу до мобільного телефону. Екранування приміщень, локальних технічних пристроїв та їх елементів - один з найефективніших, але і дорогих заходів з протидії технічній розвідці. Спеціальні екрановані приміщення дозволяють досягти ослаблення небезпечного сигналу до 80-100 дб [1]. Екранування мобільного телефону реалізується за допомогою спеціального чохла, який блокує зв’язок телефону з базовою станцією.

Активним методом захисту інформації від витоку каналами стільникового зв'язку є зашумлення приміщень або місць можливого розташування телефонів. Активні методи захисту на основі технології активного зашумлення та додаткової індикації застосовуються у «GSM-сейфі», «GSM-кейсі» та «GSM-Box». GSM SAFE – це акустичний сейф для мобільного телефону, призначений для захисту мовної інформації, що циркулює в місцях перебування власника мобільного телефону, у разі несанкціонованої дистанційної активації з метою прослуховування через канали стільникового зв'язку. Пристрій має вбудований радіочастотний детектор та генератор шуму, що автоматично вмикається під час активації телефону. Це дозволяє йому виявити віддалений доступ до телефону. GSM

SAFE починає генерувати шуми в чутному діапазоні акустичних частот, що маскують мову. Це робить неможливим прослуховування і запис розмови. Прихований дзвінок буде відразу детектуватися у трубці, сторонній особі буде чутний лише шумовий сигнал. При вийманні телефону з GSM SAFE генератор автоматично вимикається [2]. GSM кейс - це акустичний кейс для захисту від прослуховування через мобільний телефон шляхом його дистанційної активації. Захист забезпечується шляхом автоматичного акустичного зашумлення тракту передачі мовної інформації при спробі негласної дистанційної активації мікрофона мобільного телефону, вмикається генератор шуму, і телефон більше не може «підслуховувати». Індикатор активації мобільних засобів зв'язку GSM-Box усуває можливість несанкціонованого доступу до мобільних засобів зв'язку. Якщо телефон розташувати мікрофоном у напрямку до динаміка GSM-Box, шум, що генерується пристроєм, глушить мікрофон, прослуховування простору навколо телефону стає неможливим.

Одними із найдосконаліших способів захисту даних є використання криптографічних алгоритмів шифрування мовної інформації. Цей спосіб використовується для забезпечення конфіденційності телефонних розмов, що здійснюються незахищеним GSM каналом, але він вимагає від абонентів, що спілкуються, наявності однакових пристроїв кодування-декодування сигналу - скремблерів, які забезпечують надійність захисту від будь-якого засобу прослуховування стільникових телефонів, у тому числі і від спеціального обладнання, встановленого у оператора. Шифрування виконується розбиттям спектра звукового сигналу на частини (піддіапазони) та подальшою частотною інверсією кожної з цих частин. Скремблери можуть використовуватися у вигляді телефонної приставки, телефонного апарату, накладки на телефонну трубку. Криптофони - це звичайні смартфони з додатковим програмним забезпеченням. Принцип дії криптофонів, як і скремблерів, полягає в тому, що сигнали з мікрофону оцифровуються, кодуються і відправляються в мережу стільникового зв'язку в зашифрованому вигляді.

Загальний успіх у протидії витоку інформації через канали стільникового зв'язку залежить від інтегрованого підходу до захисту. Використання шифрування, ефективної аутентифікації, фізичних заходів та систем моніторингу визначають ключові аспекти стратегії безпеки. Лише взаємодія цих елементів може гарантувати ефективний захист від витоку даних у сучасному інформаційному середовищі.

Список використаних джерел:

1. Екранування електромагнітних полів: вебсайт. URL: http://um.co.ua/ 2/ 2-15/2150874.html (дата звернення: 10.02.2024).

2. Техніка захисту від прослуховування: вебсайт. URL: https://vesh.ua/ gsm-sejf/ (дата звернення: 11.02.2024).