УДК 004.7
А.В. Марковський
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В BLUETOOTH-МЕРЕЖАХ ПЕРЕДАВАННЯ ДАНИХ

A.M. Markovskiy

METHODS AND MEANS OF INFORMATION SECURITY IN BLUETOOTH-NETWORKS OF DATA TRANSMISSION

Інформаційні загрози у Bluetooth-мережах можуть мати такі передумови: кількісна недостатність; якісна недостатність; діяльність розвідувальних органів; промислове шпигунство; зловмисні дії кримінальних елементів; недобросовісні дії оточення [1].

Основні заходи захисту систем передачі даних на базі протоколу 802.15: організація безпечних каналів аутентифікації в Bluetooth (використання алгоритму аутентифікації E1 на основі алгоритму шифрування SAFER+; шифрування даних на основі алгоритму E0, управління з використанням ключів).

Існує кілька видів атак на Bluetooth-пристрої: від цілком нешкідливих - типу BlueSnarf, до повноцінних DoS-атак і міжнародних дзвінків без відома власника телефону, або "просто" викрадення СМС-повідомлень. Крім того, існують віруси, що поширюються за допомогою Bluetooth. Для забезпечення конфіденційності, цілісності та доступності даних необхідно провести аудит безпеки. Для аудиту інформаційної безпеки системи передачі даних можна використати будь-яку із спеціалізованих утиліт для виявлення та унеможливлювання спроб несанкціонованого доступу, таких як Bluesnarfing, BluePrinting, BlueBugging, Blueover, Backdoor, BlueBumping і т.п.

Для захисту мобільних пристроїв використовуються пасивні, активні та програмні методи захисту, в т.ч. екранування, індикація несанкціонованої активності мобільного пристрою, активне зашумлення, шифрування трафіку та маскування мовної інформації, а також методи ідентифікації та блокування несанкціонованого доступу до мобільного пристрою.

За матеріалами дослідження можна надати наступні рекомендації щодо практичних способів захисту при підозрі прослуховування чи несанкціонованого використання даних: повернення телефону до заводських установок; встановлення надійного антивірусного програмного забезпечення; завантаження додатків лише з офіційних магазинів; уникати підключення до відкритих і ненадійних мереж Wi-Fi; не вмикати Wi-Fi та Bluetooth без потреби; використовувати блокування екрану з паролем; не зберігати важливу інформацію на телефоні.

Окрім того, не лише безпосередньо користувачі дбають про убезпечення своєї інформації, а й сьогодні впроваджуються нові технології захисту даних у стільникових мережах, а саме аутентифікація користувача (використання PIN-коду в поєднанні з SIM-картою) та шифрування даних для передачі в радіоефірі (використання криптографічних методів кодування даних).

Література

1. Петренко А.Б. Захист інформаційних потоків у мобільних мережах стандарту CDMA2000 / А.Б. Петренко, А.Б. Єлізаров, С.А. Шматок, В.О. Ващук // Наукоємні технології. – №2 (22). – К., 2014. – С.192-195