к.т.н., проф. РАЕ Козубцов І.М. (НЦЗІ ВІТІ НТУУ “КПІ”)
к.т.н.Борисов І.В. (ВІТІ НТУУ „КПІ”)
Оксенчук І.В. (ВІТІ НТУУ „КПІ”)
Якименко В.В. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМ ПІДБОРУ КОМБІНАЦІЇ БАЗОВОЇ СТАНЦІЇ МОБІЛЬНОГО ЗВ’ЯЗКУ

На сьогоднішній день системи мобільного зв’язку не дають можливості надійного забезпечення конфіденційності інформаці, особливо у керівників держави, політиків і бізнесменів. Кожне інформаційне повідомлення каналів сучасних комунікацій можуть прочитати та побачити багато хто, від приватних осіб до найпотужніших розвідок світу. На свідомості людей все більше використовується маніпулятивних технологій.

У всьому світі йдуть перегони за технологіями, конфіденційною та компроментуючою інформацією, захистом комунікаційних систем. Для цього найпотужніші держави світу вкладають величезні бюджети, тут мова йде про мільярди доларів. Інформаційні війни, навіть в мирних країнах – вже реальність.

Зараз технології дозволяють не тільки прослухати переговори в звичайному режимі, але і коли телефон лежить поруч з вами, навіть відключений (в якості пасивного мікрофону). Також можливо постійно відслідковувати маршрут власника телефону. Вже навіть в Україні є така послуга – по мобільному телефону можна визначити місце знаходження будь кого і будь де. Мобільними телефонами користується все керівництво державою. Доречі, переговори можна прослуховувати не тільки з місця провайдингу послуги, тобто оператору мобільного зв'язку, а і з супутнику. Тобто прослухати будь-які телефонні перемовини з будь-якої країни світу немає великих проблем, навіть не заважають різні стандарти зв’язку. Проблема – знайти в такій кількості інформації щось корисне, але і тут є багато пошукових систем, та систем, які можуть робити первинний аналіз.

Для забезпечення безпеки зв’язку від таких систем використовується аутентифікація та ідентифікація абонента.

Цю проблему можливо вирішити завдяки алгоритму ідентифікації базової станції, який дає змогу ідентифікувати базову станцію, таким чином збільшити рівень безпеки інформації від систем прослуховування та моніторингу і забезпечити скритність та надійність передачі інформації.

Після включення пересувної станції (мобільного апарата) відбувається аутентифікація абонента, по закінченню цього процесу пересувна станція посилає сигнал-запиту псевдо випадкову послідовність по радіоканалу на базову станцію. При прийомі такого сигналу базова станція розуміє, що в неї запитують процедуру ідентифікації, та здійснює додавання псевдо випадкової послідовності з *ID*-кодом даної базової станції.

Закодований сигнал (Кз) передається назад по радіоканалу на пересувну станцію. Після приймання сигналу в пересувній станції відбувається додавання прийнятого закодованого сигналу (Кз) з усіма *ID*-кодами дозволених базових станцій, які записані в *SIM*-карті (модуль ідентифікації абонента).

Після додавання вирахувана псевдо випадкова послідоввність порівнюється з тою що посилалась на базову станцію і якщо вони співпадають, то відбувається ідентифікація базової станції, а якщо ні то розрив з’єднання.

Отже запропонований алгоритм дає змогу покращити рівень захищеності систем мобільного зв’язку від несанкціонованого доступу до інформації, що передається у мережі мобільного зв’язку.

Література

1. Урядников Ф.Ю. Надширокосмуговий зв’язок. Теорія і застосування / Ф.Ю. Урядников С.С. Аджемов.– М.: СОЛОН-Прес, 2005. – 368 с. (Серія „Бібліотека студента”).

2. Іпатов В.П., Орлів В.К., Самойлов І.М., Смирнов В.Н. Системи мобільного зв’язку: навчальний посібник для вузів / під ред. В.П. Іпатова. – М.: Гаряча лінія Телеком, 2003.– 272 с.

3. Крухмальов В.В., Гордієнко Н.В., Моченов А.Д. Основи побудови телекомунікаційних систем і мереж: підручник для вузів / під. ред. В.Н. Гордієнко і В.В. Крухмальова. – М.: Гаряча лінія Телеком, 2004. – 510 с.: мул.