Приймання інформації проводиться також відносно загального корпусу, але вже через другий провід лінії. Амплітудний детектор приймача дозволяє виділити низькочастотну огинаючу для подальшого підсилення та запису. Якість перехоплюваної інформації тим краще, чим ближче здійснено підключення до телефонного апарату. Для ВЧ-сигналу розімкнутий механічний контакт є повітряним конденсатором, опір якого зменшується зі збільшення частоти сигналу генератора.

При дії ВЧ-випромінювання на телефонний апарат нелінійні процеси відбувають у ряді елементів його електричної схеми. Найбільш сильно вони виявляються у мікрофоні, опір якого змінюється по закону випадкового акустичного сигналу, що призводить до амплітудної модуляції несучої. Для гарантованого виникнення зазначеного ефекту рівню зондую чого сигналу у мікрофонному ланцюгу повинен бути не меншим за 150мВ, а вихідний опір генератора повинен бути більшим, чим у мікрофона, у 5-10 разів. Частота зондуючого сигналу повинна бути у діапазоні 30кГц....20МГц. Частіше її вибирають приблизно рівною 1МГц, так як при цьому забезпечуються найкращі умови розповсюдження...

Метод зондування стосується не тільки ліній телефонних апаратів, а також других пристроїв та інших видів інформації, у тому числі по ланцюгам живлення, заземлення і т. і.

Пристрої, які використовують принцип ВЧ-нав'язування через електромагнітне поле, здійснюють зняття акустичної інформації з використанням пасивних закладок, напівактивних (аудіотранспондери).

Транспондери починають працювати тільки при опромінюванні їх потужним вузькополосним високочастотним зондуючим сигналом. Приймачі транспондерів виділяють зондуючий сигнал та подають його на модулятор, де відбувається модуляція сигналу.

Перспективним методом також є використання лазерних мікрофонів. Принцип роботи цих пристроїв, які отримали назву лазерних систем акустичної розвідки, полягає у наступному. Лазерне випромінювання (ВЧ-сигнал) розповсюджується через атмосферу, відбивається від поверхні віконного скла, модулюється при цьому по закону акустичного сигналу, який також діє на скло, повторно переборює атмосферу і приймається фотоприймачем, який відновлює мовний сигнал.

УДК 004.056

Мінін А.В.
Західноукраїнський національний університет імені Володимира Даля

СТВОРЕННЯ МЕТОДИКИ ПРОТИДІЇ З'ЙОМУ ІНФОРМАЦІЇ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

У мережах мобільного зв'язку з недавніх пір очолююче значення займають мережі пакетної передачі даних, об'єднання цих мереж і створення на їх базі нових сервісів, формує новий інформаційно-телекомунікаційний простір, в якому захист інформації стає необхідною умовою існування таких мереж.

На сьогоднішній день існує декілька стандартів мобільного зв'язку: GSM900, GSM1800, CDMA, NMT-450i, AMPS/NAMPS, DAMPS.[1]

Найбільш популярні в нашій країні - GSM1800 (для великих міст) і GSM 900 (для малонаселених територій).

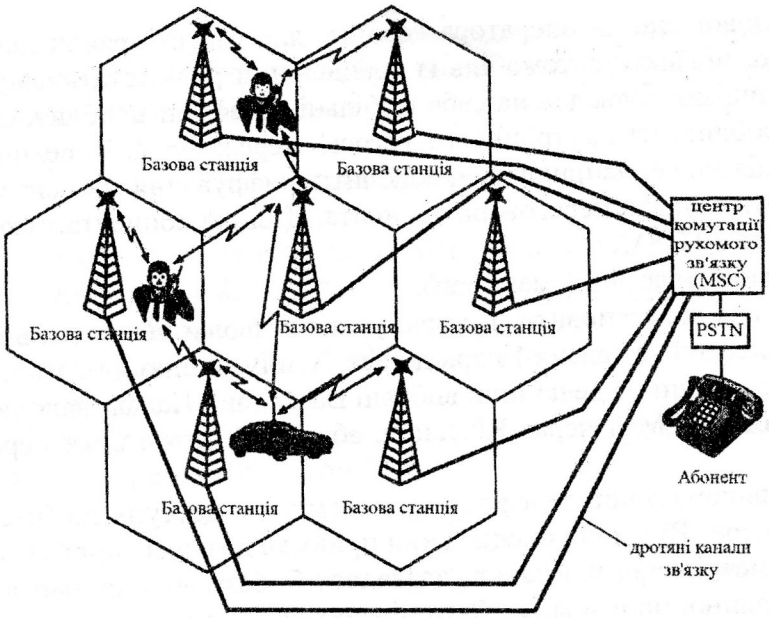

Рис.1 Схема мережі стандарту GSM

Як відомо, мобільний зв'язок, точніше його бездротова частина, захищений стандартними алгоритмами шифрування A5(/1, /2, /3). Відомо так само, що починаючи 2000 року ці алгоритми послідовно зламувалися криптоаналітиками, звіти про це надруковані як в професійній, так і в звичайній пресі [2, 3]. Так само треба відзначити що зашифрованою інформація йде на ділянці мобільний телефон - базова станція, а далі при передачі по проводах інформація йде у відкритому .

Самими незахищеними ділянками в мережах мобільних операторів (рис.1) є:

1) мобільний телефон/антенна базової станції – на цій ділянці система безпеки складається з трьох основних частин: ідентифікація (рис.2), аутентифікація (рис.2) і шифрування даних.

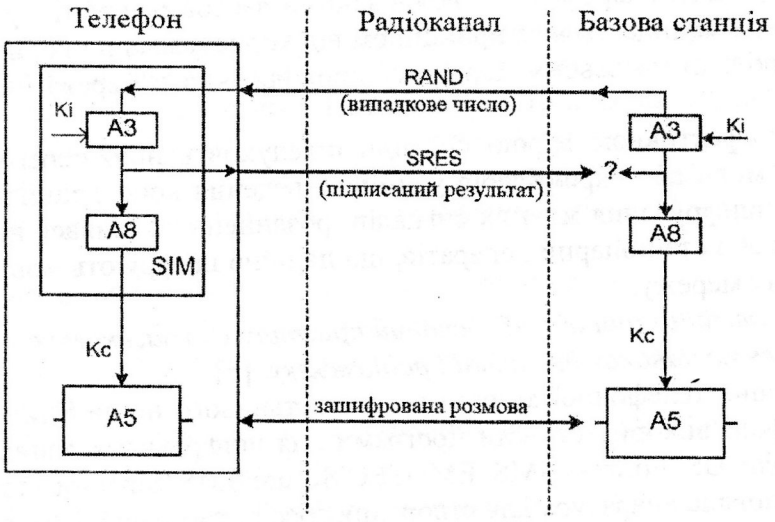

Рис.2 Схема ідентифікації і аутентифікації абонента.

Нині існує декілька видів атак на даній ділянці зв'язку. Наприклад:

- перехоплення за допомогою сканера частот, на цій ділянці найлегше зняти інформацію, тим більше повну, навіть якщо її не можна розшифрувати на льоту, то можна записати і розшифрувати пізніше;

- підміна базової станції оператора «своїй», для цього в район перебування абонента, що цікавить, може під'їхати автомобіль із спеціальним радіоустаткуванням, яке, прикинувшись базовою станцією, «заведе» на себе мобільні телефони найближчих околиць. Зробити це дозволяють особливості внутрішнього устрою мереж GSM. Перехопивши трафік, фальшива базова станція може, наприклад, відключити шифрування абонентського трафіку - і далі просто дозволить слухати переговори абонента. Дзвінки абонента така станція передає далі, в справжню мережу GSM.

2) сам мобільний телефон (смартфон):

- у телефон можна встановити програму, яка дозволяє зберігати в пам'яті всі події, що відбуваються в телефоні за заданий період часу. У внутрішню пам'ять записуються всі розмови, СМС – повідомлення, і деякі інші вибрані Вами дані. Надалі накопичена інформація по команді за допомогою СМС, через Bluetooth, або Wi-Fi може бути перенесена на комп'ютер.[4]

- також при використанні телефону як модему для доступу до Інтернету, при підключенні комп'ютера через Bluetooth спеціальний приймач дозволяє приймати сигнал Bluetooth з відстаней в сотні метрів, так що навіть, здавалося б, безмовна «розмова» за допомогою зашифрованої електронної пошти може бути підслуханий з даху сусіднього з офісом хмарочоса.

- інший метод, Bluebug, дозволяє стороннім особам встановлювати зв'язок з Bluetooth-сумісними телефонами і непомітно прослуховувати розмови користувачів.

3) Базова станція / центр комутації рухомого зв'язку – на цій ділянці інформація передається у відкритому (по специфікації стандарту GSM), але кожен оператор застосовує свої правила безпеки, у тому числі і на цій ділянці. Тому сподіватимемося, що інформація шифрується своїми протоколами і не може потрапити до чужих рук.

Існуючі методи захисту:

1) Використовувати принцип абонентського шифрування. Мережа стільникового зв'язку "надбудовується" для певної категорії користувачів додатковими засобами захисту до необхідного рівня конфіденційності і цілісності. Для цього використовуються спеціальні стільникові телефони (криптосмартфони) з вбудованими засобами криптографічного захисту. При цьому інформація захищається за принципом від користувача до користувача, що принципово важливе, оскільки по всьому маршруту проходження в мережі інформація криптографічно захищена.

2) Також ефективною мірою протидії підслуховуванню переговорів є використання маскираторів мови або скремблерів у момент ведення конфіденційного спілкування. На сьогодні техніка шифрування мовних сигналів розвинена і з'явилася на ринку у вигляді зручних переносних або стаціонарних апаратів, що надійно шифрують мовний сигнал до його подачі в телефонну мережу.

Скремблер - це автономний або вбудований пристрій для засекречування мовної інформації, що передається по каналах дротяної і радіозв'язку. [5]

3) Зберігання телефонної книги і всього останнього не на SIM-карте, а в пам'яті телефону. А в телефоні використовувати програми для шифрування даних, наприклад такі як: Pointsec for Symbian OS, Fortress SMS, EMOSEC Secure SMS, SmsProtector і тому подібне.

ще не запропонована апаратура для створення абсолютно надійного мобільного каналу рухомого зв'язку. Не один з методів не дає гарантії стовідсоткової конфіденційності.

На нашу думку для створення надійного мобільного каналу рухомого зв'язку потрібно застосовувати симбіоз з криптографічного інструменту і частот передачі. Тобто, апарати абонентів конфіденційної мережі передають цифровий потік в зашифрованому, по своїх протоколах і плюс протоколами оператора, , і частота передачі кожні, наприклад, 25мс міняється на різний крок.

У завершені можна сказати, що існуючі алгоритми шифрування в стандарті GSM (A5/1, A5/2) на сучасному етапі дуже ненадійні, тому створення власної моделі захисту інформації на рівні абонента є перспективним напрямом.

Літеретура

1. *И.Шахнович* «Современные технологии беспроводной связи» - Техносфера, 2004
2. *Elad Barkan, Eli Biham, Nathan Keller*, «Instant ciphertext-only cryptanalysis of GSM encrypted communication»,
3. http://offline.computerra.ru/offline/2003/510/29324/index.html
4. http://www.thespyphone.com
5. *Ленков С.В., Перегудов Д.А., Хорошко В.О.* Методы и средства защиты информации. В 2-х томах – К.: Арий, 2008. – Том II.

УДК 681.327.8

Звєрєва О.С.
Західноукраїнський національний університет імені Володимира Даля

ОЦІНКА ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕФОННИХ ЛІНІЯХ ЗВ'ЯЗКУ

Актуальність теми: Серед всього різноманіття способів несанкціонованого перехоплення інформації особливе місце займає прослуховування телефонних переговорів, оскільки телефонна лінія — найперше, найзручніше і при цьому саме незахищене джерело зв'язку між абонентами на даний час.

На зорі розвитку телефонного зв'язку ніхто особливо не замислювався про захист ліній від прослуховування, і електричні сигнали розповсюджувалися по проводах у відкритому вигляді. В наш час мікроелектронної революції прослуховувати телефонну лінію стало простою і дешевою справою. Можна упевнено заявити про те, що якщо зловмисник ухвалив рішення про «розробку» об'єкту, то перше, що він швидше за все зробить, це почне контроль телефонних переговорів. Його можна здійснювати, не заходивши в приміщення, при мінімальних витратах і мінімальному ризику. Потрібно просто підключити до телефонної лінії об'єкту спеціальний пристрій, що передає або реєструючий пристрій.

Мета і завдання. Метою роботи є оцінка ефективності захисту телефонних ліній зв'язку, принципи і механізми функціонування телефонних ліній зв'язку при передачі інформації.

Для досягнення мети роботи поставлені наступні задачі:

1.Аналіз можливих каналів просочування інформації в телефонних лінія зв'язку.

2.Аналіз існуючих засобів і методів перехоплення і захисту інформації в телефонних лініях зв'язку.

Для захисту звичайних міських телефонних каналів сьогоднішній ринок представляє п'ять різновидів спеціальної техніки [1]:

- - криптографічні системи захисту (скремблери);
- аналізатори телефонних ліній;
- односторонні маскувальники мови;
- засоби пасивного захисту;
- постановники активної загороджувальної перешкоди.

Прийнято вважати, що скремблери забезпечують найвищий ступінь захисту телефонних переговорів. Даний вид захисту спрямований на запобігання можливості несанкціонованого доступу до конфіденційної і цінної інформації циркулюючого по каналах зв'язку різних