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

видів. У загальному випадку необхідно враховувати всі види погроз, що виникають в каналах і комунікаційних вузлах систем зв'язку.

Найбільш ефективним засобом захисту інформації в каналах зв'язку є застосування криптографії і спеціальних зв'язних протоколів. Криптографічний захист є сукупністю методів і засобів, призначених для шифрування текстів, тобто для перетворення форми початкових (відкритих) текстів повідомлень таким чином, що їх зміст стає незрозумілим для будь-якої особи, що не володіє секретом. Прямий процес перетворення відкритого тексту з метою приховування його змісту називається шифруванням, а його результат - шифртекстом. Зворотний процес перетворення шифртекста у відкритий текст з метою відновлення загальнозрозумілості повідомлень називається розшифруванням.

У більшості криптографічних систем секретність способу шифрування даних базується на двох елементах: - алгоритмі шифрування даних, що є набором математичних правил, що визначають послідовність виконання елементарних дій над даними, в сукупності забезпечують їх шифрування або розшифрування; - криптографічним ключем, що однозначно визначає конкретний варіант перетворення відкритого тексту в шифртексті (і, навпаки) з різноманіття всіх можливих варіантів, обумовлених алгоритмом шифрування; ключ зазвичай є числом або послідовністю символів і є параметром, що дозволяє набудувати алгоритм шифрування на конкретну роботу. Використовувані на практиці алгоритми шифрування забезпечують таку велику кількість можливих ключів, що дешифровка шифротекстів шляхом їх повного перебору виявляється економічно невигідною або просто неможливою. Сучасні криптографічні системи забезпечують високу стійкість шифрування, навіть якщо алгоритм шифрування даних не є секретом. В цьому випадку стійкість шифротекстів повністю забезпечується за рахунок підтримки режиму секретності криптографічного ключа, використаного в даній дії шифрування. Центральним питанням криптографії є оцінка стійкості вживаних алгоритмів шифрування, що визначає упевненість в тому, що передбачуваний опонент, що не має доступу до використовуваного криптографічного ключа, не зможе розшифрувати і зрозуміти зміст перехопленої зашифрованої інформації [2].

Проведення досліджень, що дозволяють отримати таку оцінку, є вельми трудомісткою і дорогою справою, посильною тільки професійним криптографом. Як приклад гарантовано стійкого алгоритму шифрування можна назвати широко відомий алгоритм по ГОСТ 28147-89, реалізований у ряді серійних програмних і програмно-апаратних засобів захисту, що випускаються. Одним з найбільш складних завдань захисту мереж є генерація і розповсюдження криптографічних ключів. В даний час найбільш перспективним представляються рішення, пов'язані з гібридними криптосистемами, що використовують традиційні методи шифрування з секретним ключем для захисту секретності і цілісності, при одночасному використанні методів шифрування з відкритими ключами для реалізації функцій розподілу ключів.

Важливою вимогою безпеки зв'язку є наявність в мережі ефективних процедур аутентифікації, за допомогою яких видалені абоненти можуть ідентифікувати і перевіряти достовірність один одного. Ця проблема також може ефективно вирішуватися за допомогою криптографічних методів. Зокрема, володіння коректним ключем шифрування може розглядатися як доказ того, що абонент має право вступити в обмін повідомленнями. Для аутентифікації в мережах, побудованих на базі комутованих телефонних каналів зв'язку, можна використовувати простіші, некриптографічні способи, зв'язані із застосуванням модемів, що забезпечують функцію зворотного виклику. При цьому в процесі аутентифікації, окрім традиційної перевірки секретного пароля, автоматично ініціюється зворотний телефонний виклик (з попереднім примусовим розривом з'єднання) до абонента, що претендує на доступ до інформації.

Телефонні лінії використовуються для переговорів непостійно, багато з них більшу частину часу перебувають у відбої. Отже, в цей час можливе перехоплення мовної інформації з приміщень через використання що проходить по ним телефонної лінії і встановленого

телефонного апарату. В даний час жоден з скремблерів, що працюють на міських телефонних лініях, не обладнаний надійною системою запобігання перехопленню мовної інформації з приміщення по телефонній лінії, що перебуває у відбої [3].

Не дивлячись на великий асортимент приладів пропонованих на ринку використовування тільки одного приладу не забезпечує надійного захисту телефонної лінії від несанкціонованого зняття інформації. Для надійного захисту необхідно застосовувати декількох приладів.

Література:

1. Быков С.В. Классификация устройств съема информации в телефонной линии - Новосибирск. Сборник научных трудов НГТУ №2 1999г.

3. Лагутин В.С. Петраков А.В. Утечка и защита информации в телефонных каналах - М.: Энергоатомиздат 1996г

4. Лысов А.В. Остапенко А.Н. Телефон и безопасность (Проблемы защиты информации в телефонных сетях) - Санкт-Петербург: Политехника, 1997г.

УДК 004.681

Довлад О.А.
Західноукраїнський національний університет імені Володимира Даля

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛІ ПРОЦЕСУ АТАКИ НА ТРАФІК ЛОКАЛЬНОЇ МЕРЕЖІ

Актуальність теми: Інформатизація є характерною рисою сучасного життя. Новітні технології активно впроваджуються в усі сфери діяльності суспільства та відіграють важливу роль. Актуальність зазначеної теми обумовлено високими темпами зростання парку персональних комп'ютерів та об'ємів обробляємої інформації; об'єднання їх в локальні мережі та підключення до Інтернету; розширенням кола користувачів, що мають безпосередній доступ до ресурсів та масивів даних; зосередження в єдиних базах даних інформації різної за призначенням та приналежністю; зростання обчислювальної потужності сучасних комп'ютерів при одночасному спрощенні їх в експлуатації.

Метою роботи є забезпечення необхідного рівня захисту інформації, що обробляється у локальних мережах, шляхом розробки моделі процесу атаки на мережевий трафік.

Для досягнення зазначеної мети необхідно вирішити декілька задач, серед яких:

- дослідити фактори, які впливають на рівень інформаційної захищеності локальної мережі;
- проаналізувати можливі причини, що приводять до зниження необхідного рівня захищеності мережі;
- розробити математичну модель процесу атаки на мережевий трафік;
- запропонувати методику, здатну забезпечити потрібний рівень захищеності мережі від атак на її трафік;

Найчастіше термін «локальні мережі» або «локальні обчислювальні мережі» розуміють буквально, тобто це такі мережі, які мають невеликі, локальні розміри, з'єднують близько розташовані комп'ютери. Проте досить подивитися на характеристики деяких сучасних локальних мереж, щоб зрозуміти, що таке визначення не точно. Наприклад, деякі локальні мережі легко забезпечують зв'язок на відстані декількох десятків кілометрів. З іншого боку, по глобальній мережі можуть зв'язуватися комп'ютери, що знаходяться на сусідніх столах в одній кімнаті, але її чомусь ніхто не називає локальною мережею. Невірно і визначення локальної мережі як малої мережі, яка об'єднує невелику кількість комп'ютерів. Дійсно, як пра-