**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО**-**ТЕХНІЧНИЙ НСТИТУТ**

**Реферат:**

**Современные решения в области закрытия телефонных каналов связи**

**Виконав:**

**студент**

**групи ФБ**-63

**Цикало Гліб**

**Київ –** 2020

Оглавление

[Вступ 3](#_Toc36841636)

[Способи перехоплення 3](#_Toc36841637)

[Захист телефонних каналів 5](#_Toc36841638)

[Сучасні способи використання безпечних телефонних каналів 8](#_Toc36841639)

[Висновоки 12](#_Toc36841640)

[Джерела 12](#_Toc36841641)

# Вступ

В сучасному техногенному світі неймовірно важливим стає конфіденційність та безпечність зв’язку. В теперішніх умовах доступності та простоти використання гаджетів, людей із бізнесу, силових структур або державних установ не задовольняє якість та надійність базового захисту найбезпечніших систем світових стандартів зв’язку які на даний момент GSM, UMTS, CDMA, HSDPA, адже розмову можна перехопити, якщо не з допомогою спеціального обладнання, так з допомогою електронних систем на кшталт ‘Ешелону’. Нам відомо, що розвиток технічних пристроїв (скремблерів), перешкоджаючих перехопленню та розкриттю телефонного каналу зв’язку почався не пару років тому, але бурхливий розвиток мобільного зв’язку підштовхнув ріст попиту на пристрої його захисту, поява програмного забезпечення для смартфонів та комутаторів нікого не здивувала, як й рішення операторів зв’язку, про появу спеціальної системи конфіденційного зв’язку.

Побудова спеціальних терміналів й програмного забезпечення для захисту розмови по мобільному зв’язку, вимушена міра, адже шифрування для мобільного зв’язку, містить ключі, які ймовірно крадуться зловмисниками, разом із зашифрованою ними інформацією. Також, виробники й оператори мобільного зв’язку не розголошують інформацію, про незашифровані ланки трафіку, які не попадають на ефірну частину, отже перед нами постає питання, про побудову такої моделі зв’язку, яка гарантує конфіденційність від прилада до прилада на кожній ланці зв’язку. Данна проблема можлива, як введенням спеціальних терміналів, використовуючих обмін закодованою інформацією, так і програмними рішеннями.

# Способи перехоплення

У разі знаходження абонента зі своїм стільниковим телефоном в будь-якій європейській країні при наявності цікавого набору ключових слів в його розмові, вона (розмова), без сумніву, буде перехоплена автоматизованою глобальною системою перехоплення і передачі електронних сигналів "Ешелон". Спочатку "Ешелон" створювався як спільна програма Національного агентства безпеки США і розвідслужби Великобританії. Пізніше до неї підключилася Канада, Австралія і Нова Зеландія. Перша версія "Ешелону" з'явилася в 1971 році. Тоді велика частина ресурсів мережі працювала проти СРСР і його союзників. Після закінчення "холодної війни" її можливості були сфокусовані на так званих "державах-ізгоях" (таких як Ірак, Іран і Лівія), а також на міжнародних кримінальних і терористичних організаціях. Технічною основою системи "Ешелон" є десятки геостаціонарних супутників стеження, які перехоплюють будь-які інформаційні сигнали наземних засобів зв'язку, і мережа суперкомп'ютерів, здатна аналізувати в день до 10 млрд. Повідомлень. Для "вилова" цікавих для розвідки відомостей використовуються закладені в пам'ять комп'ютерів ключові слова, адреси, прізвища та номери телефонів. Створення цієї глобальної системи радіорозвідки не залишилося без відповіді з боку СРСР, і з 1979 року в ньому почав діяти аналог "Ешелону" - система об'єднаного обліку даних про противника (СОУД). Приводом для її створення стали Олімпійські ігри 1980 року в Москві, а першим завданням - збір інформації про можливі ворожі акції зарубіжних спецслужб під час Олімпіади. У радянські часи СОУД користувалися не тільки спецслужбами СРСР, а й країнами Східного блоку, Монголією, Кубою, В'єтнамом. Крім того, в Росії успішно функціонує і розвивається СОРМ - система внутрішнього моніторингу інформації, переданої по мережах документального електрозв'язку. У США діє її "усічена" версія, яка почала будуватися мінімум на п'ять років пізніше СОРМ. Вона називається Carnivore (в перекладі - "м'ясоїдна тварина, хижак"), але в ФБР її вважають за краще називати DCS1000 (Digital Collection System - система цифрового накопичення). Вона використовується для спостереження за електронною поштою громадян, які перебувають на підозрі у ФБР.

Технічні вимоги до СОРМ були затверджені ще 10 років тому, але з тих пір вона серйозно розвивалася. Її склад досить тривіальний - спеціальне програмне і апаратне забезпечення, правда, все ділиться на дві частини - апаратно-програмні засоби в складі вузла зв'язку і такі ж засоби в складі віддаленого пункту управління. Простіше кажучи, управління і отримання всіх необхідних ресурсів здійснюється з територіального органу ФСБ по спеціальному і дуже потужному каналу зв'язку, який передбачається також резервувати, тобто створювати рівний по потужності канал. Система повністю автономна, має незалежне живлення, безпосередньо пов'язана з резервними джерелами живлення. Крім усього цього, весь трафік шифрується.

Незважаючи на здавалося б чіткі документи по СОРМ, існує і подвійне тлумачення деяких моментів. Наприклад, відповідно до документами, СОРМ повинна мати доступ до всіх даних про користувача і минаючи оператора - тобто безпосередньо. З іншого боку - представники операторів не заперечують проти "прослуховування ефіру", проте білінг і дані про абонентів передавати не хочуть, вимагаючи рішення суду. Є два основні режими роботи системи - повний і статистичний контроль. Категорія "статистичний контроль" означає, що розмовний канал не підключається на пульт управління, а просто в реальному масштабі часу передається інформація про фази встановлення з'єднань і дані про контрольовані виклики. При повному ж контролі на пульт управління передається в реальному масштабі часу інформація про фази встановлення з'єднань, дані про контрольовані виклики, а також здійснюється збір і трансляція на пульт управління інформації, переданої в розмовному тракті контрольованого абонента. У цього режиму є свої особливості. Перша і основна (найпродуктивніша) - це фіксація розмови по ключовим словам. Серед шуму і гомону ефіру виокремлюються ключові фрази і, якщо їх кількість в одній розмові перевалює певний поріг, телефони беруть на контроль.

Популярний сервіс sms також є контрольованим - адже це, по суті своїй, тільки набір символів, текст. А його, на відміну від голосу, можна систематизувати шляхом шаблонів, словників і всіляких комбінацій російською та англійською мовами. Не дуже складно виділити на цю справу невелику частину ресурсів комп'ютерної системи - тим більше програму перехоплення, швидше за все, переробляли з взятої за основу системи перехоплення пейджингових повідомлень. Ще одна зручність - текстові послання легко зберігати, адже 160 символів зовсім небагато, а жорсткі диски у компетентних органів величезні.

Крім того, прослухати стільниковий зв'язок можна й за допомогою персональних систем - спеціального програмного забезпечення, ноутбука і комплекту антен для сканування радіоефіру. Зазвичай такі системи (наприклад, GSS-ProA і аналогічні) являють собою не тільки пристрій для перехоплення і прослуховування сигналів мережі GSM, але також мають вбудований складний локатор, за методом тріангуляції визначає місце розташування об'єкта. При вказівці системі номера мобільного терміналу, який необхідно контролювати, вона відстежує його місцезнаходження в мережі і автоматично включається на запис при виході телефону в ефір.

Існують й інші джерела загрози абонентам мобільних систем зв'язку. Однією з таких загроз є Access Fraud - шахрайський доступ - несанкціоноване використання послуг стільникового зв'язку за рахунок навмисного або ненавмисного втручання, маніпулювання або перепрограмування номерів стільникових апаратів ESN (Electronic Serial Number) і / або MIN (Mobile Identification Number). В AMPS (Advanced Mobile Phone Service - вдосконалена рухома телефонна служба - аналоговий стандарт мобільного зв'язку в діапазоні частот від 825 до 890 МГц) ці номери можуть бути перехоплені за допомогою сканера і використані для програмування інших телефонів - метод створення нелегального "двійника". Спосіб можливий на мережах без аутентифікації. Іншим видом загроз безпеки в мобільних системах зв'язку можна вважати Stolen Phone Froud - шахрайство з вкраденим телефоном - несанкціоноване використання вкраденого або втраченого стільникового телефону. Спосіб працює як правило, поки власник не повідомить компанію і та не заблокує доступ з вкраденого телефону.

# Захист телефонних каналів

Захист телефонних каналів може бути здійсненний за допомогою криптографічних систем захисту (скремблерів), аналізаторів телефонних ліній, односторонніх маскіраторів мови, засобів пасивного захисту, постановників активної загороджувальної перешкоди. Захист інформації може здійснюватися на семантичному (смисловому) рівні із застосуванням криптографічних методів і енергетичному рівні.

Існуюча апаратура, що протидіє можливості прослуховування телефонних переговорів, за ступенем надійності поділяється на три класи:

I клас - найпростіші перетворювачі, які спотворюють сигнал, порівняно дешеві, але не дуже надійні - це різні шумогенератори, кнопкові сигналізатори і т. д;

II клас - скемблери, при роботі яких обов'язково використовується змінний ключ-пароль, порівняно надійний спосіб захисту, але фахівці-професіонали за допомогою хорошого комп'ютера можуть відновити сенс записаної розмови;

III клас - апаратура кодування мови, що перетворює мову в цифрові коди, що представляє собою потужні обчислювачі, більш складні, ніж персональні ЕОМ. Не знаючи ключа, відновити розмову практично неможливо.

скремблерування

Установка на телефон засоб кодування мовного сигналу (скремблера) забезпечує захист сигналу на всьому протязі телефонної лінії. Мовне повідомлення абонента обробляється за допомогою якого-небудь алгоритму (кодується), оброблений сигнал направляється в канал зв'язку (телефонну лінію), потім отриманий іншим абонентом сигнал перетвориться по зворотному алгоритму (декодируется) в мовний сигнал.

Цей метод, однак, є дуже складним і дорогим, вимагає установки сумісного обладнання у всіх абонентів, що беруть участь в закритих сеансах зв'язку, і викликає тимчасові затримки на синхронізацію апаратури і обмін ключами з початку передачі і до моменту прийому мовного повідомлення. Скремблери можуть забезпечувати також закриття передачі факсових повідомлень. Портативні скремблери мають слабкий поріг захисту - за допомогою комп'ютера його код можна розгадати за кілька хвилин.

Аналізатори телефонних ліній сигналізують про можливе підключення на основі вимірювання електричних параметрів телефонної лінії або виявлення в ній сторонніх сигналів.

Аналіз параметрів ліній зв'язку та провідних комунікацій полягає в вимірі електричних параметрів цих комунікацій і дозволяє виявляти закладні пристрої, що зчитують інформацію з ліній зв'язку або передають інформацію по провідних лініях. Вони встановлюються на попередньо перевірену телефонну лінію і налаштовуються з урахуванням її параметрів. При наявності будь-яких несанкціонованих підключень пристроїв, що живляться від телефонної лінії, видається сигнал тривоги. Деякі типи аналізаторів здатні імітувати роботу телефонного апарату і тим самим виявляти підслуховуючі пристрої, що приводяться в дію сигналом виклику. Однак такі пристрої характеризуються високою частотою помилкового спрацьовування (так як існуючі телефонні лінії вельми далекі від досконалості) і не можуть виявляти деякі види підключень.

Для захисту від «мікрофонного ефекту» слід просто включити послідовно з дзвінком два запараллеленних в зустрічному напрямку кремнієвих діода. Для захисту від «високочастотної накачування» необхідно включити паралельно мікрофону відповідний (ємністю 0,01-0,05 мкФ) конденсатор, закорачується високочастотні коливання.

Метод «синфазного маскування» маскує низькочастотні перешкоди застосовується для придушення пристроїв знімання мовної інформації, підключених до телефонної лінії послідовно в розрив одного з проводів або через індукційний датчик до одного з проводів. При розмові в кожен провід телефонної лінії подаються узгоджені по амплітуді і фазі маскуючи перешкоджаючі сигнали мовного діапазону частот (дискретні псевдовипадкові сигнали імпульсів М-послідовності в діапазоні частот від 100 до 10000 Гц). Так як телефон підключений паралельно телефонної лінії, узгоджені по амплітуді і фазі перешкоджаючі сигнали компенсують один одного і не призводять до спотворення корисного сигналу. У закладних пристроях, підключених до одного телефонного дроту, завадовий сигнал не компенсується і «накладається» на корисний сигнал. А так як його рівень значно перевершує корисний сигнал, то перехоплення переданої інформації стає неможливим.

Метод високочастотної маскуючої перешкоди. У телефонну лінію подається завадовий сигнал високої частоти (зазвичай від 6-8 кГц до 12-16 кГц). В якості маскуючого шума використовуються широкосмугові аналогові сигнали типу «білого» шуму або дискретні сигнали типу псевдовипадкової послідовності імпульсів з шириною спектру не менше 3-4 кГц. У пристрої захисту, підключеному паралельно в розрив телефонної лінії, встановлюється спеціальний фільтр нижніх частот з граничною частотою вище 3-4 кГц, який пригнічує (шунтирує) перешкоджаючі сигнали високої частоти і не робить істотного впливу на проходження низькочастотних мовних сигналів.

Метод підвищення або зниження напруги. Метод зміни напруги застосовується для порушення функціонування всіх типів електронних пристроїв перехоплення інформації з контактним (як послідовним, так і паралельним) підключенням до лінії, з використанням її в якості джерела живлення. Зміна напруги в лінії викликає у телефонних закладок з послідовним підключенням і параметричної стабілізацією частоти передавача «догляд» несучої частоти і погіршення розбірливості мови. Передавачі телефонних закладок з паралельним підключенням до лінії при таких скачках напруги в ряді випадків просто відключаються. Ці методи забезпечують придушення пристроїв знімання інформації, що підключаються до лінії тільки на ділянці від захищаємого телефонного апарату до АТС.

Компенсаційний метод. На приймаючу сторону подається «цифровий» маскуючий шумовий сигнал мовного діапазону частот. Цей же сигнал ( «чистий» шум) подається на один з входів двоканального адаптивного фільтра, на другий вхід якого надходить суміш одержуваного мовного сигналу і маскуючого шуму. Фільтр компенсує шумову складову і виділяє приховуваний мовний сигнал. Цей спосіб дуже ефективно пригнічує всі відомі засоби ‘негласного’ знімання інформації, що підключаються до лінії на всій ділянці телефонної лінії від одного абонента до іншого.

Так зване «випалювання» здійснюється подачею високовольтних (більше 1500 В) імпульсів потужністю 15-50 Вт з їх випромінюванням в телефонну лінію. У гальванічно приєднаних до лінії електронних пристроїв знімання інформації «вигорають» вхідні каскади і блоки живлення. Результатом роботи є вихід з ладу напівпровідникових елементів (транзисторів, діодів, мікросхем) засобів знімання інформації. Подача високовольтних імпульсів здійснюється при відключенні телефонного апарату від лінії. При цьому для знищення паралельно підключених пристроїв подача високовольтних імпульсів здійснюється при розімкнутої, а послідовно підключених пристроїв - при «закороченому» (як правило, в телефонній коробці або щиті) телефонної лінії.

# Сучасні способи використання безпечних телефонних каналів

Дзвінки через власний сервер голосового зв'язку: BlackBox

Покупці BlackBox отримують власний потужний інструмент захисту розмов, який ідеально підходить для використання вузьким колом осіб, в компанії або організації.

Принцип роботи:

* на сервер покупця встановлюється програмне забезпечення BlackBox, яке управляє дзвінками і захистом розмов;
* для користувачів видаються індивідуальні короткі номери (наприклад, 003, 055, 111) на які вони можуть дзвонити один до одного і нікуди більше;
* на смартфонах користувачів встановлюється додаток для дзвінків, який через Інтернет підключається до сервера BlackBox і шифрує розмови.

Основна перевага використання BlackBox - захищений голосовий зв'язок без сторонніх і посередників, в якому покупець самостійно розпоряджається, кого підключати в «закритий клуб», кого відключати і кому давати права на обслуговування своєї системи розмов.

плюси:

* спецслужби не мають інструментів для прослуховування за данним видом шифрування;
* немає прив'язки до номера мобільного телефону, email-адреси або банківської карткиж;
* голосовий зв'язок між співрозмовниками шифруються від телефону до телефону (end-to-end);
* покупець має необмежений доступ до сервера, завдяки чому може організувати незалежний аудит безпеки на предмет виявлення «троянських» програм в системі;
* на сервері не зберігається персональна інформація абонентів і записи розмов, тому що він працює в ролі посередника, який з'єднує дзвінки між абонентами і шифрує розмови;
* централізоване управління всіма користувачами.

мінуси:

* для роботи зв'язку необхідний сервер (особистий або орендований в дата-центрі);
* потрібен свій технічний фахівець (адмін), якому власник системи довірить настройку смартфонів для їх підключення до сервера і подальшого обслуговування голосового зв'язку;
* платний додаток для розмов.

Дзвінки через платний сервіс голосового зв'язку: Silent Phone

Сервіс захисту розмов компанії Silent Circle набрав більшу популярність у всьому світі після скандалу з масовим прослуховуванням розмов спецслужбами завдяки документам Едварда Сноудена. Голосовий зв'язок працює через сервера Silent Circle, до яких підключаються користувачі за допомогою програми Silent Phone.

Принцип роботи:

Використовується така ж технологія захисту розмов як у BlackBox.

Захист розмов всій лінії зв'язку (end-to-end) працює тільки з тими, хто встановили собі Silent Phone і також пройшов процедуру реєстрації. Після того як співрозмовники обміняються своїми логінами, вони можуть дзвонити один до одного.

Важливо!

* Компанія Silent Circle, що володіє Silent Phone, заснована Майком Дженкі (Mike Janke), колишнім «морським котиком» ВМС США. Після армії він працював як підрядник з виконання замовлень в сфері інформаційної безпеки для армії. Саме тісна співпраця Майка Дженко з США у багатьох викликає недовіру до сервісів його компанії.
* Silent Phone збирає дані про місцезнаходження (геодані) смартфона користувача. Для організації конфіденційних розмов такі дані абсолютно не потрібні! Наївно вважати, що якщо користувач заборонить додату використовувати геодані смартфона, це дозволить приховати його місце розташування. Silent Circle все-одно може бачити, звідки до нього підключаються користувачі за іншими параметрами.

плюси:

* потужний протокол шифрування розмов;
* немає прив'язки до номера мобільного телефону;
* поєднує в собі функції захищених відео дзвінків і текстового чату;
* дозволяє швидко організувати захист розмов між групою людей.

мінуси:

* голосовий та відео зв'язок працює через сервера і устаткування «посередників»;
* Silent Circle (посередник) бачить місце розташування своїх користувачів;
* при оплаті за послуги користувачі «світяться» своїми банківськими даними.

Дзвінки через безкоштовний сервіс голосового зв'язку: Signal (RedPhone)

Послуги захисту розмов компанії Open Whisper Systems також набрали велику популярність після скандалу з масовим прослуховуванням розмов спецслужбами світових держав. Голосовий зв'язок працює через сервера Open Whisper Systems до яких підключаються користувачі за допомогою програми Signail (iOS) і RedPhone (Android). Використовується така ж технологія захисту розмов як у BlackBox і Silent Phone.

Важливо!

1. Щоб не виникало плутанини, невелике пояснення: до 2015 року для iOS і Andorid було єдине програмне забезпечення для дзвінків під назвою «RedPhone». З 2015 року для iOS розробники анонсували додаток під новою назвою «Signal».
2. Судячи з Google Play, додаток RedPhone для Android не розвивається. На момент написання реферату поновлення до додатка не виходили більше 2 років, при цьому до роботи додатка є багато зауважень, які не виправляються розробниками.

плюси:

* безкоштовний зв'язок;
* стійка система шифрування голосового зв'язку;
* поєднує в собі функції захищеного текстового чату.

мінуси:

* прив'язка до номера мобільного телефону;
* Open Whisper Systems (посередник) бачить місце розташування своїх користувачів;
* дзвінки проходять через сервера «посередників»;
* додаток RedPhone для Android не розвивається.

Підсумок попередніх пунктів

* власний сервер голосового зв'язку надає найбільший захист;
* шифрування розмов не ефективно, якщо на смартфон потрапив троян-шпигун.

Непрослуховуємий телефон і безпечний канал зв'язку.

При використанні традиційного мобільного зв'язку або системи Інтернет між абонентами завжди є посередник - провайдер зв'язку, який з'єднує дзвінки і через нього проходять усі дані. На прикладі мобільного зв'язку це працює таким чином: Абонент 1 -> стільникові вишки / наземні мережі -> дата центр -> стільникові вишки / наземні мережі -> Абонент 2. Аналогічно з інтернет зв'язком. Найвразливіше місце в цьому ланцюжку - це проходження сигналу в дата центрі і стільникових вишках. Саме на них найпростіше перехоплюются необхідні дані, при цьому абоненти можуть навіть не підозрювати про це, на відміну від прямої прослушки, яку можна помітити. Навіть якщо ваш пристрій шифрує дані, вони все-одно можуть бути перехоплені, тому що вони також проходять через місцеві наземні мережі, а на будь-який замок завжди знайдеться свій лом.

Виходить, щоб максимально убезпечити свої дані, необхідно позбутися від "посередника". На даний момент тільки системи супутникового зв'язку пропонують мінімальну участь "посередника" і наземних мереж при зв'язку абонентів.

Система супутникового зв'язку працює схожим чином. При дзвінку з супутникового телефону на будь-який стаціонарний / мобільний телефон в світі, сигнал йде від супутникового телефону на супутник і з супутника через дата-центр по наземних мережах проходить до абонента дозвону. Хоча сигнал шифрується за стандартом AES 256, але як уже говорилося, до будь-якого замку знаходиться свій лом.

Кардинально інша ситуація при дзвінку з супутникового телефону на супутниковий телефон. Сигнал в такому випадку взагалі не торкається землі і проходить через супутники безпосередньо на супутниковий телефон дозвону. На землю, в дата-центр, йдуть тільки технічні дані, такі як: тривалість виклику (щоб відрахувати з рахунку вартість дзвінка) та гео-позиція з точністю до континенту (в деяких тарифах вартість дзвінка в різних точках світу може відрізнятися). Таким чином дзвінки зі супутникового телефону на супутниковий телефон, фактично, неможливо прослухати. Більш того, сигнал від супутникового телефону НЕ конусний (як на мобільних телефонах), а спрямований, що робить практично не можливим прослуховування телефону спрямованими спецзасобами, тому що для цього необхідно перебувати в зоні сигналу, а це можливо тільки якщо зависнути в повітрі над телефоном на вертольоті або безпілотнику.

Саме через особливості роботи супутникового зв'язку його використовують не тільки як зв'язок у віддалених місцях планети, де немає покриття наземних мереж, але і як безпечний канал зв'язку і телефон захищений від прослуховування.

# Висновоки

У сучасному світі питання безпечного зв'язку стоїть дуже гостро. На ринку пропонуються всі можливі рішення: анонімні сім карти, шифрувальне обладнання, анонімні телефони. Але як відомо, ідеальної системи захисту не буває, це ж стосується і системи зв'язку.

Слід розуміти, що кожен комп'ютер (планшет, ноутбук, смартфон) має свою IP-адресу, за якою досить легко можна ідентифікувати власника і переглянути історію його дій. Щоб ускладнити завдання зацікавленим особам, можна почати з простого:

* завести додаткові облікові записи (кілька адрес електронних пошт, додатковий аккаунт);
* ніколи не змішувати публічний профіль з приватним;
* по можливості не користуватися пошуковими системами і сервісами тієї країни де проживаєте;
* періодично міняти точки доступу до мережі Інтернет під час користування вашим девайсом (кафе, парки, комп'ютерні клуби).

Такі нескладні дії допоможуть приховати мережеву і реальну IP-адресу і ненадовго заплутають зловмисників.

Проте за словами Клода Шенонна кожну систему можна зламати, питання полягає тільки в ресурсах(часі, коштах, спеціалістах), але можна виокремити таку межу, коли ваша система буде дорогою ресурсно для атаки.

Користуючись інформацією вказаною в рефераті ви зробите вашу систему зв’язку стійкою до атак.

# Джерела

* Матеріали web-сторінки //http:// www.signal-com.ru/ ЗАО «Сигнал-КОМ».
* Матеріали web-сторінки https://tech.wikireading.ru/12653
* Матеріали web-сторінки //http://www.businesspundit.com/ Обзор криптофонов.
* Журнал "Information Security"http://www.itsec.ru/newstext.php?news\_id=54366
* Матеріали web-сторінки <http://www.warning.dp.ua/tel.htm>
* Матеріали web-сторінки <https://ain.ua/2015/11/09/tri-sposoba-zashhity-razgovorov-ot-proslushki-kolonka-eksperta/>
* Матеріали web-сторінки https://satphone.com.ua/blog/blog-18.php