

Міністерство освіти і науки України

НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Системи технічного захисту інформації

Реферат на тему:

«Засоби виявлення закладнх пристроїв»

**Виконав:**

Студент 4 курсу ФТІ

групи ФБ-61

Агеєнко В. М.

Київ - 2020

Вступ

Інформація – надзвичайно важливий ресурс у сучасному світі, тож на неї завжди буде йти полювання зі сторони зловмисників, і це необхідно враховувати при проектуванні надійної захищеної системи, в якій міститься конфіденційна інформація. Витоки інформації можливі через різні канали: оптичний, матеріально-речовий, радіо, акустичним та електричним.

Для викрадення перехоплення, обробки та передачі мовної інформації використовують спеціальні пристрої, здатні записувати, підсилювати сигнал, перетворювати його на електричний і передавати на відстань. Такі прилади називають *закладними пристроями.*

Із плином часу такі пристрої постійно вдосконалюються, тож повинні розвиватись і засоби виявлення та знешкодження ЗП.

Засоби пошуку закладних пристроїв

Залежно від фізичних властивостей ЗП та характеристики створюваних ними каналів витоку, необхідно застосовувати ті чи інші способи пошуку.

Будь-який сучасний диктофон може бути легко виявлений за допомогою нелінійного локатора (НЛ). Причому ймовірність виявлення досить висока незалежно від розмірів диктофона і його стану.

В основу роботи НЛ покладено властивість провідникових матеріалів відбивати радіохвилі. Оскільки локатор використовує для пошуку радіосигнали, значною завадою можуть стати сторонні шуми та металеві предмети, що торкаються одне одного і можуть спотворювати сигнал. Крім того, неможливим є і використання таких засобів пошуку ЗП в пристроях, де заздалегідь передбачено використання напівпровідників.

Широкого використання останнім часом набули такі нелінійні локатори: «Родник-2К», «NR-900M», «NR- 900E», «Шлюз», «BROOM», «SUPERBROOM», «SUPERSCOUT», «ORION 2.4», «Энвис», «Сандал-СМ», «Изумруд-ДМ», «РК-885-S».

**«Родник-2К»** забезпечує роботу в умовах сильних зовнішніх шумів від мобільного зв’язку, телевізійних передатчиків, радіостанцій тощо.

Технічні характеристики:

* Потужність сигналу 0,8 Вт
* Чутливість апаратури не менша за -150 дБВт
* Частота сигналу 980…1020 Мгц
* Діапазон регулювання чутливості - 45 дБ.

**NR-900M** використовують для пошуку та локалізації пристроїв, що містять напівпровідникові елементи.

Технічні характеристики:

* Потужність сигналу 150 Вт
* Чутливість апаратури не менша за -130 дБВт
* Частота сигналу 900 Мгц
* Діапазон регулювання чутливості - 25 дБ.

**ORION 2.4 HX** може з успіхом застосовуватися службами безпеки і правоохоронними органами для виявлення пристроїв негласного знімання інформації, виявлення заборонених для пронесення і зберігання електронних пристроїв (стільникових телефонів, sim карт і т.і.)

* Потужність сигналу 3,3 Вт
* Чутливість апаратури не менша за -140 дБВт
* Кількість частотних каналів - 60
* Діапазон частот передавача 2,404—2,472 ГГц

Альтернативний спосіб пошуку ЗП – аналіз спектру радіосигналів. На відміну від НЛ, в такий спосіб не можна знайти вимкнений пристрій, але процес пошуку можна автоматизувати, а дані про сигнали записувати в базу даних. Деякі моделі пристроїв здатні навіть класифікувати ЗП за типом сигналу та його візуалізація при використанні спеціального програмного забезпечення.

Приклади аналізаторів спектру:

**OSCOR OSC-5000E**  здатний контролювати різні канали витоку інформації. Може використовуватись як в ручному, так і в автоматичному режимах та знаходити такі ЗП як: мікрофони, телефонні передавачі, передавачі по електромережі, пристрої лазерного зняття інформації.

Технічні характеристики:

* Діапазон аналізу радіосигналів – від 10 кГц до 3 ГГц
* Контроль ліній напругою до 250В
* Потужність аудіо системи – 3 Вт
* Частотний діапазон аудіо системи - 50 Hz – 15 kHz
* Чутливість ВЧ системи - 0,8 мкВ в 15 kHz смузі

**СРМ-700 («Акула») –** універсальний пристрій для знаходження ЗП, в тому числі – кімнатні, телефонні та натільні жучки, відеопередатчики та диктофони.

Технічні характеристики:

* Частотний діапазон НЧ зонду: 15 кГц – 1 Мгц -3дБ
* Максимальна напруга 300 В
* Чутливість -38 дБм
* Вхідна напруга звукового підсилювача 1.7мВ –10 В
* Частотний діапазон: 100 Гц –15 кГц ±3дБ

**Пошуковий комплекс ST-031 “Пиранья”** створено для проведення оперативних заходів по знаходженню і локалізації технічних засобів викрадення інформації, а також для виявлення каналів витоку інформації.

Технічні характеристики:

* Частотний діапазон ВЧ системи: 10 кГц–3000 МГц
* Чутливість ВЧ системи: 0,8 мкВ в смузі 15 кГц
* Детектори ВЧ системи: AM, WFM, NFM, SubC FM, SSB/CW
* Ширина смуги ВЧ системи: 250 кГц, 15 кГц, 6 кГц
* Частотний діапазон аудіо системи: 50 Гц — 15 кГц
* Фільтр мовного діапазона: 300—3000 Гц — 18 дБ/октава
* Вихідна потужність аудіо системи: 3 Вт

Пошук ЗП засновано на принципі акустичної локації – вимірі затримки звукового імпульсу, що поступає з колонок комп’ютера до приймача: чим менша затримка сигналу між мікрофоном та жучком, тим більш точно відоме місце знаходження закладки. Сучасні прилади дозволяють виміряти положення ЗП з точністю до 10 см.

Головною перевагою використання таких методів пошуку ЗП є можливість їх роботи в фоновому режимі – це дозволяє оператору паралельно проводити пошук іншими засобами.

До недоліків слід віднести складність первинного налаштування системи а також відсутність точної інформації про місце знаходження ЗП – відомий тільки напрям, у якому він розташований.

Захист інформації від витоку із використанням зашумлення

Альтернативним способом захисту мовної інформації від прослуховування є **електромагнітне придушення** – активний спосіб. Він передбачає встановлення у приміщенні спеціальних генераторів шумів, які працюють у певних діапазонах частот (частіше, близько 900 мГц), таким чином роблячи неможливим передачу даних закладними пристроями, оскільки їх потужність антен значно менша. Якщо бути точним, то переданий сигнал сильно спотворюється, що унеможливлює виокремлення з нього корисної інформації.

Радіус дії подавляючих пристроїв залежить від потужності передавача та характеристики направленості антени. Звичайно зона придушення має вигляд сектора з кутом 30-80 градусів і радіусом дії 1,5 метри (для диктофонів в екранованому корпусі).

Пристрій придушення диктофонів **Буран-3**

Пристрій "Буран-3" являє собою генератор нечутною для людського вуха шумоподібної перешкоди, керований мікропроцесором, що включає модуль живлення і антенний модуль. В результаті дії приладу на магнітну стрічку диктофона замість мови записується генерований "Бураном" шум. "Буран-3" впливає на звукозаписні пристрої вузько направленим плоскополяризованим випромінюванням.

Площина поляризації хвилі випромінювання збігається з площиною максимального габариту приладу. Ширина діаграми спрямованості випромінювання становить 45 градусів (в ортогональної площині ширина діаграми спрямованості - 15 градусів).

Ефект від роботи приладу полягає у впливі імпульсного випромінювання на нелінійні елементи схем диктофонів. Шум, що генерується приладом, записується на магнітну стрічку.

"Буран-3" може встановлюватися як стаціонарно, так і в кейс для оперативного використання. Включення приладу здійснюється за допомогою кнопки (під столом або під ручкою кейса). Додатково прилад може комплектуватися пультом дистанційного керування (по радіоканалу).

Пристрій придушення диктофонів **«R-2000»** призначено для попередження спроб запису мовної інформації на магнітофони як аналогового, так і цифрового типів. Пристрій виконано у вигляді кейсу, в якому знаходяться: антена, пристрій придушення, батарея та пристрій дистанційного керування.

Технічні характеристики:

* Зона придушення – сектор з кутом 60 градусів
* Відстань придушення для диктофонів в металевому корпусі – 2 метри
* Відстань придушення «жучків» - близько 4 метрів
* Час роботи в автономному режимі – 1 година
* Потужність в режимі придушення – 50Вт

Окрім електромагнітного зашумлення, використовуються і генератори акустичних сигналів. Перевагою такого способу є те, що сигнал буде спотворено при знятті не тільки диктофонами та жучками, але і при витоку віброакустичним каналом (наприклад, прослуховування через стіну). Але при занадто високій потужності шуми викликатимуть дискомфорт у працівників, а при занадто низькій будуть мало ефективними. Крім цього, впливає людський фактор: через шуми, працівники часто починають говорити гучніше, що нівелює користь від використання генераторів шумів.

Мобильний генератор шуму **iProTech MNG-300 Rabbler** генерує мовоподібні шуми, які захищають від запису. Завдяки досить малим розмірам, пристрій можна помістити в кишеню.

Технічні характеристики:

* Діапазон частот: 300 – 3600 Гц (еквівалент розмови в натовпі людей)
* Струм – 120 мА
* Розміри 85х53х21 мм

Більш універсальними є генератори ультразвукових шумів: вони заважають роботі підсилювачів сигналу, придушуючи роботу жучків, при цьому працюючи поза діапазоном людського розпізнання звуків.

Комплекс ультразвукового захисту "Завес"

Порушення працездатності (придушення) різних мікрофонних пристроїв, призначених для несанкціонованого перехоплення акустичної інформації (диктофонів, закладних пристроїв).

Комплекс призначений для роботи в замкнутому просторі і забезпечує захист, в залежності від необхідності, будь-якої локальної області або приміщення в цілому, використовуючи багатоканальну версію комплексу.

Мінімальна конфігурація комплексу - двоканальна. При необхідності комплекс має можливість нарощування до 4-х, 6-ти, 8-ми і тд. канальних версій.

2-х канальна система забезпечує захист в обсязі 27 куб. м.

Відмінною особливістю комплексу є вплив на мікрофонний пристрій і його підсилювач достатньо могутнім ультразвуковим сигналом (групою сигналів), що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що призводять в остаточному підсумку до порушення працездатності мікрофонного пристрою (його придушення).

Оскільки вплив здійснюється по каналу сприйняття акустичного сигналу, то зовсім не важливі подальші трансформація, способи і канали передачі перехопленої акустичної інформації (вони можуть бути як завгодно складними), так як інформаційний акустичний сигнал пригнічується на етапі сприйняття його. Все це робить комплекс достатньо універсальним в порівнянні з існуючими комплексами і засобами активного захисту акустичної інформації від витоку технічними каналами.

Висновок

В даній роботі було проведено огляд сучасних засобів виявлення та знешкодження закладних пристроїв та каналів витоку інформації. Було розглянуто активні засоби захисту – генератори електромагнітних та акустичних шумів та засоби знаходження жучків – нелінійні локатори та аналізатори спектру.

На даний момент існує дуже багато пристроїв для захисту інформації від витоку. Вони різняться за розмірами, технічними характеристиками, способом використання і призначенням. Кожен з них має свої переваги і недоліки: так, нелінійні локатори є найбільш універсальним способом пошуку жучків, але не завжди здатні показати точний результат, в той час, як аналізатори спектру дають більш точні результати, але не здатні знаходити неактивні закладні пристрої. Генератори акустичних сигналів запобігають витоку інформації не тільки за допомогою жучків та диктофонів, але і попереджають підслуховування через стіни, але при цьому можуть створювати дискомфорт для працівників організації, в той час як генератори електромагнітних шумів не впливають безпосередньо на людину, але можуть заважати роботі пристроїв системи.

Вибір засобів захисту інформації залежить від специфіки системи, в якій необхідно проводити заходи. Також необхідно розглядати використання кількох засобів захисту в комплексі.

Список використаних джерел:

1. Заставні пристрої з передачею інформації по провідним каналам URL: um.co.ua/4/4-10/4-102849.html
2. **Промышленный Шпионаж** URL: <https://studall.org/all-175562.html>
3. Заходи щодо блокування ТКВІ з використанням активних засобів URL: <https://sites.google.com/site/kanalivitokuinformaciie/metodi-ta-zasobi-zahistu-vid-vitoku-informaciie/zahodi-sodo-blokuvanna-tkvi-z-vikoristannam-aktivnih-zasobiv>
4. Как обнаружить прослушку. Как найти жучок URL: <https://oxpana.by/stat/41-zaschita-ot-proslushki.html>
5. Технічні характеристики пристроїв: <http://www.bnti.ru/>