УДК 621.395

ОГЛЯД ЗАСОБІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ПІДКЛЮЧЕНЬ ДО ТЕЛЕФОНИХ ЛІНІЙ У СТОРОЖОВОМУ РЕЖИМІ

Описано загрози для інформації на абонентських телефонних лініях. Наведено огляд і характеристику методів та засобів захисту від прослуховування приміщень через абонентські телефонні лінії, а також захисту телефонних повідомлень від перехоплення на ділянці абонентських телефонних ліній.

The security threats on subscriber telephone loops are described. The protecting methods and means against listening of building spaces through subscriber telephone loops and also the protecting methods and means against telephone messages interception in the subscriber telephone loops section are reviewed and described.

1. ВСТУП

Не зважаючи на бурхливий розвиток комп'ютерних мереж і медіатехнологій, передача телефонних повідомлень продовжує займати значний сегмент у загальному трафіку сучасної телекомунікації [1]. Це зумовлено передовсім простотою та поширеністю телефонного зв'язку. Разом з тим телефонний зв'язок є одним з найбільш незахищених у сенсі інформаційної безпеки.

За даними досліджень [2,3,4], загрози інформаційній безпеці для абонентів телефонних мереж загального користування найчастіше реалізуються шляхом несанкціонованих підключень (НСП) до абонентської телефонної лінії. Для захисту від подібних загроз застосовуються такі методи і засоби як запобігання несанкціонованим підключенням шляхом обмеження фізичного доступу до ліній, контроль параметрів телефонних ліній з метою виявлення засобів технічної розвідки, а також застосування пристроїв технічного захисту для знешкодження телефонних закладок або маскування інформаційних сигналів [5,6,7].

Метою статті є проаналізувати специфіку загроз для інформації, описати відомі способи несанкціонованого використання абонентських телефонних ліній. Також охарактеризувати відомі методи виявлення несанкціонованих підключень та пристрої які

[1] НУ "Львівська політехніка", кафедра захисту інформації,
[2] Політехніка Опольська, інститут автоматики і інформатики

працюють в сторожовому режимі для забезпечення безпеки абонентських телефонних ліній.

2. НЕСАНКЦІОНОВАНІ ПІДКЛЮЧЕННЯ ДО ТЕЛЕФОННИХ ЛІНІЙ ЯК ДЖЕРЕЛО ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Абонентська телефонна лінія (АТЛ) є дводротовою фізичною лінією, що з'єднує телефонний апарат чи інший термінал абонента, наприклад, модем із телефонною станцією, концентратором чи іншим обладнанням телефонної мережі. Часто застосовуються також і такі назви АТЛ як абонентський шлейф (local loop) чи остання миля (last mile).

АТЛ є складовою телефонного тракту, який утворюється у телефонній мережі на час обміну телефонними повідомленнями (рис. 1). Будучи найбільш доступною і незахищеною абонентська телефонна лінія є найуразливішим компонентом телефонії.

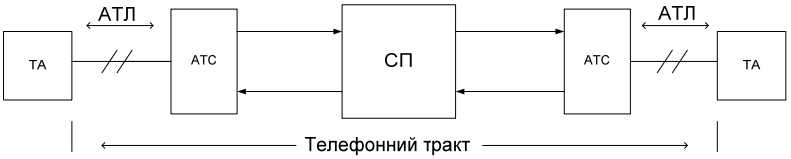

Рис. 1. АТЛ як складова телефонного тракту

Абонентська телефонна лінія не є однорідною за своєю будовою. У її складі зазвичай можна виділити найпротяжнішу ділянку міського магістрального кабелю, а також ділянки розподільчого кабелю і абонентського проводу (рис. 2).

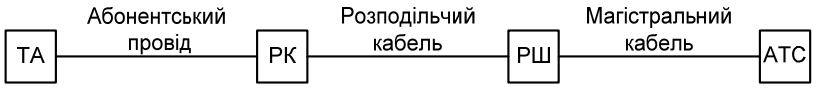

Рис. 2. Будова АТЛ

Несанкціоноване підключення до АТЛ становить загрозу підслуховування телефонних переговорів (загроза конфіденційності) та несанкціонованого використання ресурсів телефонного зв'язку (телефонне шахрайство). Для прикладу зловмисник із телефонного

апарату підключеного до АТЛ паралельно із основним може здійснювати міжміські розмови коштом легального абонента, за яким прикріплена дана телефонна лінія.

Проте існує ще один аспект загрози конфіденційності абонентів телефонного зв'язку. Йдеться про можливість прослуховування приміщень, де розташований телефонний апарат. Технічні канали витоку конфіденційної інформації із приміщення утворюються як штатними елементами телефонного апарата (так званий «мікрофонний ефект»), так і нелегально впровадженими засобами технічної розвідки у вигляді телефонних закладок чи віддаленого застосування принципу високочастотного нав'язування [8].

Загроза інформаційній безпеці на об'єктах із телефонним зв'язком найчастіше реалізується шляхом несанкціонованих підключень до абонентської телефонної лінії засобів технічної розвідки (ЗТР). ЗТР, які застосовуються для перехоплення телефонних переговорів називаються також телефонними закладками. Розрізняють контактні та безконтактні телефонні закладки. Безконтактні телефонні закладки використовують побічні електромагнітні випромінювання, тому їх вплив на АТЛ практично відсутній. Натомість контактні телефонні закладки мають гальванічний зв'язок із АТЛ, через що проявляється їх вплив на параметри АТЛ.

Таблиця 1

Тип підключення до АТЛ засобу технічної розвідки	Вид загрози, що реалізується			Вплив підключення на параметри АТЛ
	Перехоплення телефонних повідомлень	Прослуховування приміщень	Телефонне шахрайство	
Безконтактний	так	ні	ні	відсутній
Контактний	так	так	так	проявляється

3. АНАЛІЗ ВПЛИВУ КОНТАКТНИХ ПІДКЛЮЧЕНЬ ЗАСОБІВ ТЕХНІЧНОЇ РОЗВІДКИ НА ПАРАМЕТРИ ТЕЛЕФОННИХ ЛІНІЙ

Контактні засоби технічної розвідки за способом підключення до АТЛ поділяються на паралельні та послідовні.

Паралельні засоби технічної розвідки підключаються одночасно до обох дротів телефонної лінії (рис. 3, а), тому має місце шунтувальний вплив на АТЛ. Послідовні телефонні закладки встановлюються у

розрив одного із дротів телефонної лінії (рис. 3, б), тому їх вплив проявляється насамперед через збільшення імпедансу цього дроту. Очевидно, що демаскувальний вплив паралельних закладок зменшується за збільшення їх вхідного імпедансу, а послідовних навпаки – за зменшення цього параметра.

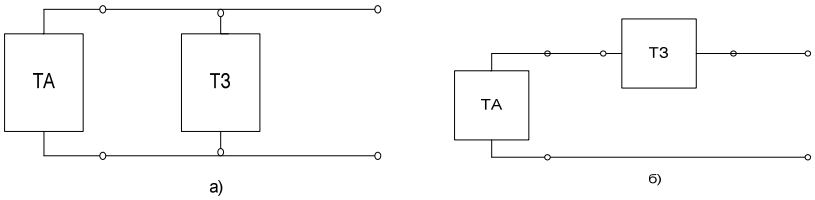

Рис. 3. Підключення телефонних закладок: а)паралельно, б)послідовно; ТА – телефонний апарат; ТЗ – телефонна закладка.

У разі відключення АТЛ від телефонної станції (АТЛ у знеструмленому стані) для виявлення контактних підключень можна безпосередньо контролювати на постійному струмі опір дротів телефонної лінії $R_{TЛ}$ та ізоляції $R_{ІЗ}$, а також параметри імпедансу – ємність C_0, індуктивність L_0, опір R_0 і провідність G_0 на змінному струмі. Далі потрібно порівняти одержані результати із паспортними даними АТЛ на момент монтажу (параметри так званої «чистої лінії»).

Паралельні закладки можна виявити вимірюючи опір ізоляції, ємність та провідність розімкненої на віддаленому кінці лінії змінному струму постійному та змінному струмах, а також ємність. Наприклад, якщо вхідний адмітанс паралельної закладки має активну G_P і ємнісну C_P складові, то за результатами контролю можна встановити відхилення від параметрів «чистої лінії»

$$G_0 \parallel G_P \geq G_0;$$

$$C_0 \parallel C_P \geq C_0.$$

Для виявлення послідовних закладок телефонну лінію замикають на віддаленому кінці та вимірюють опір на постійному і змінному струмі, а також індуктивність лінії. Якщо вхідний імпеданс послідовної закладки має активну R_S і ємнісну L_P складові, результати контролю відрізняються від параметрів «чистої лінії»

$$R_0 + R_P \geq R_0;$$

$$L_0 + L_P \geq L_0.$$

Розглянемо детальніше, які параметри АТЛ у робочому стані можуть зазнавати змін внаслідок паралельних і послідовних підключень.

У робочому стані АТЛ, як дводротова фізична лінія, забезпечує під'єднання телефонного апарата до спеціального інтерфейсу, який у сучасних цифрових системах комутації називається лінійним абонентським модулем (Subsriber Line Interface Circuit). Саме через цей модуль (рис. 4) забезпечується доступ абонента до телефонної мережі, а сам модуль виконує низку функцій, перелік яких відомий під англомовною абревіатурою BORSCHT:

- B (Battery feed) — електроживлення;
- O (Overload Protection) — захист від перенапруги, яка може виникнути на кількакілометровій АТЛ в силу різних причин;
- R (Ringing) — посилка сигналів виклику;
- S (Supevision) — контроль за станом шлейфа;
- C (Coding) — оцифровування мовного сигналу та його відновлення до аналогового вигляду, які здійснюється відповідно кодером на передачі та декодером на прийомі;
- H (Hybrid) — перехід із двопровідної АТЛ на чотирипровідну лінію для систем комутації і передачі, що реалізується за допомогою диференційної системи;
- T (Test) — випробування абонентських ліній.

З огляду на вплив контактних підключень та роботу пристроїв виявлення НСП важливо розглянути дві функції — B і S.

Живлення абонентського терміналу (функція B) здійснюється від станційної батареї номіналом $E_Ж$=48 В із заземленим позитивним полюсом. Струм у абонентській лінії обмежується опорами обмоток реле близько R_{OP}=500 Ом, які встановлені симетрично у кожному проводі лінії. Ці ж реле використовуються для контролю стану АТЛ (функція S) - замикання шлейфу призводить до спрацювання реле.

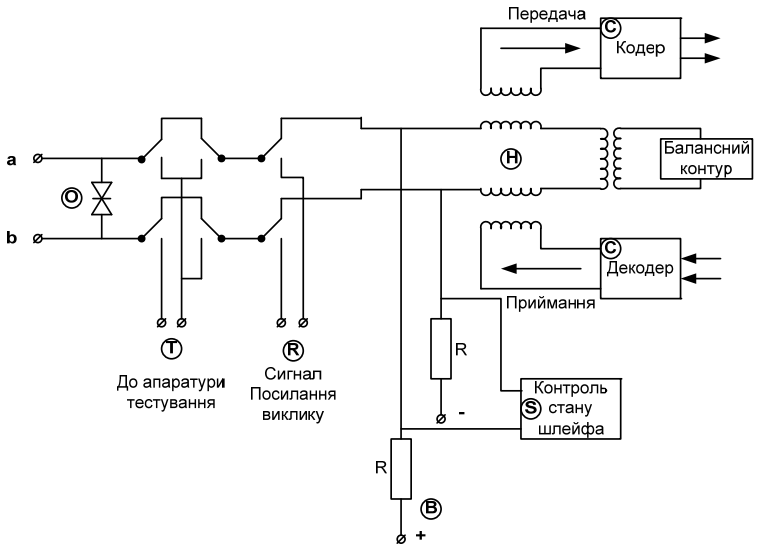

Рис. 4. Узагальнена схема абонентського модуля

В режимі «Очікування» (за покладеної слухавки) роздільний конденсатор C_P викличного дзвінка телефонного апарата заряджається до значення напруги живлення батареї, а струм у АТЛ відсутній $I_{ЗШ} = 0$ (рис. 5, а). Тому режим «Очікування» називають розмиканням шлейфа. Під'єднання паралельної закладки до АТЛ знижує рівень напруги U_{TA} на штатному телефонному апараті, що і є демаскувальним фактором. Послідовні закладки не впливають на рівень напруги в режимі «Очікування».

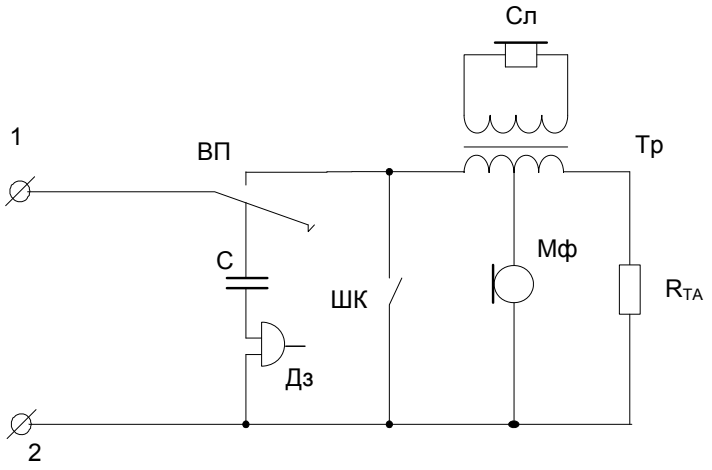

Рис. 5. Схема телефонного апарата: ВП – важільний перемикач;

В режимі «Розмова» (після підняття слухавки) важіль підключає до АТЛ розмовну частину телефонного апарата (рис. 5), з опором R_{TA} на постійному струмі. Цей опір із урахуванням опору телефонної лінії $R_{TЛ}$, а також обмоток реле зумовлює протікання по АТЛ струму

$$I_{ЗШ}=E_Ж / (R_{TЛ} + 2\ R_{TA} + 2\ R_{OP}),$$

тому режим «Розмова» називають замиканням шлейфа. Під'єднання до АТЛ послідовної чи паралельної закладки змінює значення струму $I_{ЗШ}$ замкненого шлейфу, що можна використати для виявлення НСП.

Посилка сигналів виклику (функція R) полягає у надсиланні на тлі сталої складової $E_Ж$ радіоімпульсів амплітудою близько 90 В частотою заповнення 25 Гц, тривалістю 4 с і паузою 1 с.

Окрім сигналів виклику, по АТЛ можуть передаватися інші види сигналів, що теж потрібно враховувати під час виявлення НСП. Також важливо розглянути можливість появи цих сигналів у контексті роботи телефонної мережі.

Телефонна мережа використовує принцип комутації каналів, для якого характерні фази встановлення з'єднання, обміну повідомленнями (розмова) та роз'єднання. На етапі встановлення з'єднання використовуються сигнали телефонної сигналізації, що поділяються на лінійні, оповіщувальні та адресні.

Лінійні сигнали визначають стан пристроїв мережі на основних етапах встановлення з'єднання (зайняття, відбій, роз'єднання та ін.). До таких, зокрема належить струм шлейфа для реалізації розглянутої вище функції S.

Оповіщувальні акустичні сигнали передаються від телефонної станції до телефонного апарата і слугують для інформування абонента про етапи встановлюваного з'єднання:

- посилка виклику (розглянута вище функція R);
- відповідь станції;
- зайнято;
- контроль посилки виклику.

Адресні або керуючі сигнали, які передають відомості між керуючими пристроями комутаційних вузлів про маршрут в мережі до абонентського пристрою призначення. У багатьох системах також передаються сигнали про категорію виклику, запиту апаратури автоматичного визначення номера тощо.

Наявність службових сигналів у АТЛ ускладнює завдання виявлення несанкціонованих підключень через погіршення умов роботи пристроїв контролю, оскільки високий рівень службових сигналів є серйозним перешкоджаючим фактором, що знижує достовірність результатів контролю.

4. ХАРАКТЕРИСТИКА МЕТОДІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ПІДКЛЮЧЕНЬ ДО ТЕЛЕФОННИХ ЛІНІЙ

Несанкціоновані підключення засобів технічної розвідки змінюють не лише рівень напруги живлення чи струм шлейфу порівняно із так званим станом «чистої лінії», але також електрофізичні параметри АТЛ, зокрема імпеданс. Власне реєстрація такого впливу на параметри АТЛ і лежить в основі роботи пристроїв виявлення НСП. Постійне вдосконалення технічних і експлуатаційних характеристик телефонних закладок призводить до зменшення їх впливу на параметри АТЛ, в відтак ускладнює задачу виявлення НСП. Ще одним фактором, що ускладнює роботу пристроїв виявлення НСП, є часова нестабільність параметрів телефонної лінії, зумовлена передовсім впливом довкілля (температура, вологість тощо).

Методи і засоби, що застосовуються для виявлення несанкціонованих підключень до АТЛ, можна поділити на такі категорії:

- залежно від способу використання – пошукові і сторожові;

- залежно від стану АТЛ – лінія у робочому стані або знеструмлена.

У пошуковому режимі телефонний апарат зазвичай відключається від АТЛ, а на його місце вмикається пристрій виявлення НСП. Телефонна лінія у цьому випадку може знаходитися у робочому стані чи бути знеструмленою (відімкнутою від обладнання АТС).

На цей час найбільш поширеними і досконалими у сенсі достовірності результатів контролю АТЛ є пошукові пристрої виявлення НСП, що працюють на знеструмлених (відключених від телефонних станцій) лініях. В основі роботи таких пристроїв лежать методи вимірювання:

- опору шлейфа;
- асиметрії АТЛ;
- параметрів імпедансу (опору змінному струму, ємності та індуктивності лінії);
- вольт-амперної і перехідної характеристик АТЛ;
- характеристики Лісажа.

Крім того, для виявлення НСП на знеструмлених лініях застосовуються пристрої, що реалізують методи нелінійної локації та імпульсної рефлектометрії.

Сторожові пристрої виявлення НСП за своїм призначенням повинні працювати в умовах перебування АТЛ у робочому стані. Наявність напруги живлення, різних службових сигналів та шунтувальний вплив обладнання абонентського інтерфейсу телефонної мережі різко обмежує арсенал придатних методів і засобів контролю параметрів АТЛ.

На цей час сторожові пристрої переважно реалізують метод контролю напруги живлення на телефонному апараті. Достовірність роботи таких пристроїв обмежується нестабільністю напруги живлення та різного роду завадами. Тому актуальним є пошук нових підходів до побудови сторожових пристроїв виявлення НСП, які б забезпечили достовірність контролю.

5. ОГЛЯД ІСНУЮЧИХ ПРИСТРОЇВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ПІДКЛЮЧЕНЬ НА ОСНОВІ АНАЛІЗУ ЕЛЕКТРОФІЗИЧНИХ ПАРАМЕТРІВ ТЕЛЕФОННИХ ЛІНІЙ

Для вимірювання параметрів досліджуваних ліній можна використовувати як універсальні, так і спеціалізовані вимірювальні

пристрої, що побудовані для проведення пошукових робіт і оснащені спеціальними адаптерами для під'єднання до різного типу ліній. Існуючі засоби контролю провідних ліній, як правило, реалізують кілька методів вимірювання параметрів АТЛ.

Таблиця 1

Пристрій	**Режим роботи**	**Стан лінії**	**Виявлення підключення/локалізація**	**Застосовувані методи контролю**	**Контрольовані параметри**
Counter TeK TE-4800	пошуковий	робочий	виявлення підключення	пасивні	напруга
THE TAP TRAP II-Wiretap Detector	пошуковий	робочий	виявлення підключення	пасивні	опір, ємність
Counter TeKPro Telephone Analyzer	пошуковий, сторожовий	робочий	виявлення підключення	пасивні, активні	напруга ємність
SuperTap Buster	сторожовий	робочий	виявлення підключення	активні	напруга
Telephone Tap Nullifier	пошуковий	робочий	виявлення підключення	пасивні	напруга, ємність
TALAN Telephone and LineAnalyzer	пошуковий	робочий знеструмлений	виявлення та локалізація	пасивні, активні	напруга, струм, опір, ємність
ULAN 2	пошуковий	робочий знеструмлений	виявлення та локалізація	пасивні, активні	напруга, струм, опір, ємність
CPM-700	пошуковий	робочий	виявлення	пасивні, активні	напруга, ємність
PT-030	пошуковий	робочий	виявлення та локалізація	активні	опір, струм

6. ВИСНОВКИ

Для вимірювання параметрів досліджуваних ліній можна використовувати як універсальні, так і спеціалізовані вимірювальні пристрої, що побудовані для проведення пошукових робіт і оснащені спеціальними адаптерами для під'єднання до різного типу ліній. Існуючі засоби контролю провідних ліній, як правило, реалізують кілька методів вимірювання параметрів АТЛ.

Аналізуючи функціональні можливості існуючих засобів контролю провідних ліній, зазначимо деякі важливі, на наш погляд, недоліки та обмеження вищевказаних приладів, а саме:

– відсутність комплексності та універсальності проведення всіх вимірювань характеристик ліній, одним приладом із зіставленням результатів;

– недостатня чутливість, а відтак і достовірність результатів контролю параметрів досліджуваних ліній;

– не всі прилади оснащено інтерфейсом для передавання результатів контролю АТЛ на персональний комп'ютер для подальшого опрацювання та формування звітної документації;

– не всі прилади мають функції запам'ятовування і відтворення записаної інформації для проведення аналізу;

– зазвичай контроль абонентської телефонної лінії у робочому стані зводиться лише до аналізу наявних в лінії сигналів.

1. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии / Б.И.Крук, В.Н.Попантонопуло, В.П.Шувалов; под ред. профессора В.П.Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия – телеком, 2005. – 647 с. 2.Б.З.Берлик, А.С.Брискер и др. Справочник. Городская телефонная связь. — М.: Радио и связь, 1987г. — 280 с. 3. Хома В.В. Інформаційна безпека абонентів стаціонарних телефонних мереж // Вісник НУ "Львівська політехніка".– 2008.- №608. — С. 74-85. 4. Безопасность информационных технологий. Методология создания систем защиты / В.В.Домарев. – К.:ООО "ТИД ДС". 2001. – 698 с. 5.Универсальный анализатор проводных коммуникаций ULAN-2. Техническое описание и инструкция по эксплуатации. М.:2004, 88 с.6. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия РФ, 1998. – 320 с. 7.Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и средства защиты информации. – Санкт-Петербург: ООО Издательство Полигон, 2000, с. 320. 8.Современные технологии безопасности: Каталог.– М.: ЦБИ «Маском», 2006.– 52 с. 9.Лысов А.В. Остапенко А.Н. Телефон и безопасность (Проблемы

*защиты информации в телефонных сетях) -Санкт-Петербург: Политехника. - 1997. 10.Технические системы и средства защиты информации: Информационные материалы. – М:НПЦ «Нелк», 2006. – 67 с. 11.Петраков А.В., Лагутин В.С. Защита абонентского траффика - М.: Радио и связь, 2001, 504 с. 12.Сайт Державної служби спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua. 13.Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии / Б.И.Крук, В.Н.Попантонопуло, В.П.Шувалов; под ред. профессора В.П.Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия – телеком, 2005. – 647 с.: ил. 14. Безопасность информационных технологий. Методология создания систем защиты / В.В.Домарев. – К.:ООО "ТИД ДС". 2001. – 698 с. 15.Петраков А.В. Основы практической защиты информации. – М.: Радио и связь. 1999.- 368 с. 16.Системы электросвязи: Учебник для вузов / Под ред. В.П.Шувалова. - М.: Радиосвязь. 1987, с. 512. 17.Б.З.Берлик, А.С.Брискер и др. Справочник. Городская телефонная связь. — М.: Радио и связь, 1987г. — 280с.18.И.Н.Балахничев, А.В.Дрик, А.И.Крупа. Борьба с телефонным пиратством. Мн.: Наш город, 1998г. — 116 с. 19.Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия РФ, 1998. – 320 с. 20. Быков С.В. Классификация устройств съема информации в телефонной линии - Новосибирск. Сборник научных трудов НГТУ №2 199. 21.Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах.– М.: Энергоатомиздат. 1996. – 304 с. 22.Кравченко В.Б. Защита речевой информации в каналах связи // Специальная техника, 1999, №4. 23.Абалмазов Э.И. Новая технология защиты телефонных разговоров // Специальная техника. 1998, № 1. – С. 4 – 8. 24.Дудикевич В.Б., Хома В.В., Пархуць Л.Т., Захист засобів і каналів телефонного зв'язку: Навчальний посібник. – Львів: Видавництво Національного університету «Львівська політехніка», 2012. – 212 с 25.*ULAN-2 Техническое описание и инструкция по эксплуатации г. Москва *26.Інтернет ресурс* http://www.das-ua.com/catalog/13/cpm-700-deluxe *27. http://www.analitika.info/zaschita.php?page=1&full=block_article102&articlepage=3 28. Інтернет ресурс http://www.pimall.com/nais/countertekdefender.html*