

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ІМПЕДАНСНИХ ВИМІРЮВАНЬ У ЗАДАЧАХ ВИЯВЛЕННЯ ТЕЛЕФОННИХ ЗАКЛАДНИХ ПРИСТРОЇВ

© Іванюк В.М., 2008

Розглянуто ефективність використання імпедансних вимірювань у задачах виявлення закладних пристроїв на абонентських телефонних лініях. Проаналізовано особливості встановлення ЗП, котрі впливатимуть на виявляючі властивості методу.

Efficiency of using impedance measurements is considered in the tasks of exposure of devices of establishment on subscriber public-call lines. Features are analysed establishments of ZP, which will influence on discovering property of method.

1. Постановка проблеми та задачі дослідження. Трафік телефонного зв'язку був і залишається переважаючим за обсягом передаваних повідомлень у телекомунікаційних системах. Зацікавленість зловмисників несанкціонованим доступом до абонентських телефонних ліній (АТЛ) зумовлюють такі чинники: розширена топологія мережі телефонного зв'язку, передавання інформації у відкритому вигляді на ділянці від абонентського закінчення до АТС, протяжність ліній, можливість отримання інформації у реальному часі. Прослуховування сигналів можна здійснити під'єднанням монтерської слухавки або інших побутових засобів. При використанні складніших технічних засобів можна здійснити передавання сигналів по радіоканалу або його запис на магнітну плівку чи цифрові запам'ятовуючі носії. Такі технічні засоби називаються телефонними закладними пристроями (ТЗП), що разом із АТЛ утворюють технічний канал витоку інформації.

За типом під'єднання ТЗП поділяються на контактні та безконтактні (індукційні давачі, давачі Холла) [2, 3]. Своєю чергою, контактні ТЗП можуть під'єднуватись до телефонної лінії двома способами – паралельним та послідовним.

При послідовному під'єднанні ТЗП живлення здійснюється від телефонної лінії, що забезпечує необмежений час роботи. Послідовні під'єднання легко виявити за рахунок зміни параметрів лінії, зокрема за рахунок різкого падіння напруги. Покращані варіанти ЗП, що під'єднуються до лінії послідовно, мають пристрої компенсації падіння напруги, але реалізація цього потребує додаткового джерела живлення. Телефонні закладки з паралельним під'єднанням до лінії виявити важче, тому що їхнє живлення здійснюється від зовнішнього джерела.

У зв'язку з покращанням параметрів ТЗП задача їхнього виявлення значно ускладнилась. Засоби контролю, побудовані на основі відомих методів, не можуть виявляти широкий клас пристроїв несанкціонованого отримання інформації з абонентських телефонних ліній. Тому актуальним є пошук нових та удосконалення вже відомих методів. Оскільки більшість методів ґрунтуються на дослідженні характеристик АТЛ, вважаємо доцільним першочергово звернути увагу на дослідження первинних параметрів лінії.

Відомо, що кабельні лінії характеризуються первинними і вторинними параметрами [4,7]. До первинних параметрів належать опір, ємність, індуктивність і провідність, що рівномірно розподілені по всій її довжині. Враховуючи, що частотний діапазон каналу тональної частоти становить 300 – 3400 Гц, а довжина АТЛ не перевищує 5 км, лінію можна розглядати як систему із зосередженими параметрами, еквівалентна схема якої подана на рис. 1.

Активний електричний опір є сумою опорів двох струмопровідних жил і втрат, викликаних впливом електромагнітного поля на сусідні провідники та інші металеві конструкції кабелю (зокрема на екрани).

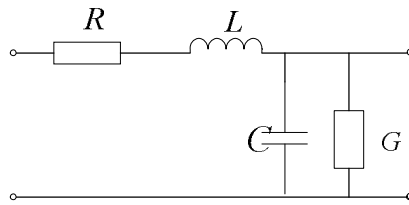


Рис.1. Схема заміщення абонентської телефонної лінії [4]

Індуктивність кабелю складається з внутрішньої індуктивності кабелю та зовнішньої індуктивності, зумовленої зовнішнім магнітним потоком.

Ємність лінії передачі аналогічна ємності конденсатора, де роль обкладинок виконують два провідники, а діелектриком слугує матеріал, що ізолює їх один від одного. Ємність кабельної лінії прийнято називати робочою ємністю, на відміну від часткової ємності (між двома окремо взятими провідниками, між провідником та ізолювальною оболонкою, між провідником і землею).

Провідність ізоляції кабельної лінії складається з провідності ізоляції на постійному і змінному струмах. Провідність ізоляції змінного струму залежить від опору на постійному струмі, діелектричних втрат і частоти струму. Ці параметри ще називають погонними або первинними параметрами лінії.

На підставі аналізу літературних джерел [1, 2, 6, 8] встановлено перелік методів, які використовуються для виявлення під'єднань засобів технічної розвідки до АТЛ. Їх можна поділити на дві групи:

- дослідження здійснюються, коли АТЛ під'єднана до АТС (методи контролю напруги, ВАХ, сигналів та вимірювання струму витoku);
- дослідження здійснюються, коли АТЛ від'єднана від АТС (контроль параметрів імпедансу, контроль опору постійному струму, асиметрії жил та дослідження АТЛ методом імпульсної рефлектометрії).

Зручним інструментом для комплексного дослідження первинних параметрів АТЛ є імпедансні вимірювання. У статті досліджується придатність імпедансних методів для дослідження абонентських ліній, що складаються з однотипного кабелю, без розподільних коробок і розподільних шаф.

2. Обґрунтування математичної моделі АТЛ. На результати дослідження значний вплив мають стан лінії, тривалість її використання, дефекти виготовлення тощо. Старіння лінії призводить до незначної зміни параметрів індуктивності та ємності у схемі заміщення, які переважно будуть спричиняти похибку в діапазоні високих частот. Тому під час досліджень імпедансної характеристики у діапазоні нижніх частот можна збільшити виявляючі властивості пристроїв пошуку ТЗП.

У схемі (рис. 2) запропоновано виконувати вимірювання у режимі, коли лінія від'єднана від АТС. У лінію подається змінний синусоїдальний сигнал і в усталеному режимі здійснюються заміри струму в лінії і напруги на затискачах. Після вимірювань частоту сигналу змінюють із кроком 25 Гц, у межах діапазону $f \in (100; 3500)$. Інформативними параметрами у такому разі будуть вигляд характеристики повного опору та відхилення параметрів імпедансу лінії від паспортних даних. З боку абонента під'єднується вимірювальний прилад, який складається з джерела синусоїдальних коливань змінної частоти.

На рис. 3 зображена схема заміщення ТЗП, який постійно під'єднаний до АТЛ. Конденсатор C_z пропускати лише змінний сигнал з лінії, який підсилюватиметься операційним підсилювачем. Резистор $R_{ш}$ використовується для регулювання сталої часу ТЗП. При моделюванні паралельного ТЗП використанні $C_z = 10^{-7}$ Ф, $R_{ex} = 10^8$ Ом, $R_{ш} = 2,04 \cdot 10^5$ Ом, стала часу дорівнює 20 мілісекунд. На рис.4 наведена характеристика повного опору такого ТЗП від частоти.

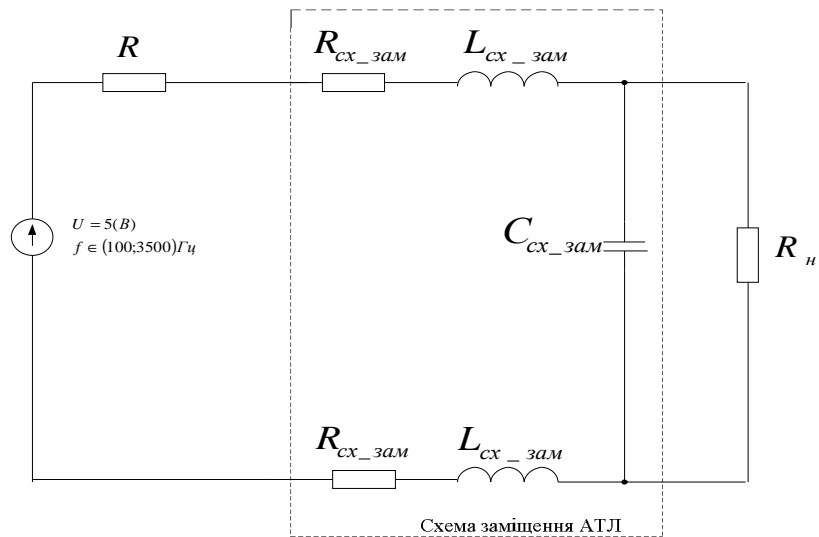


Рис. 2. Схема заміщення АТЛІ при вимірюванні повного опору у режимі навантаження

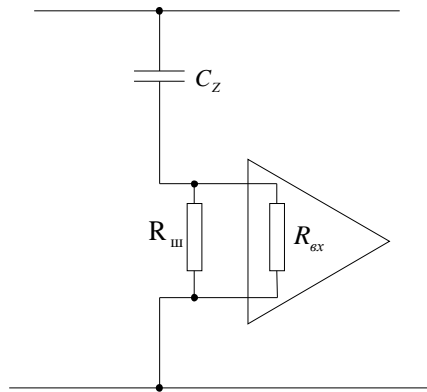


Рис.3. Схема заміщення вхідного кола паралельного ТЗП

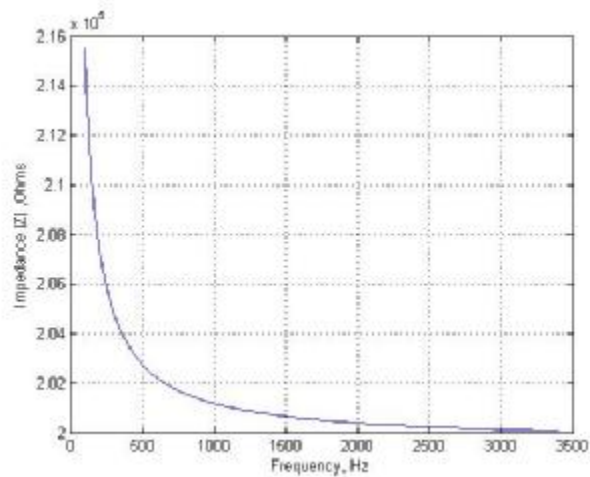


Рис.4. Характеристика модуля імпедансу паралельного ТЗП

Послідовний закладний пристрій вмонтовується в розрив АТЛІ (рис. 5). Для захисту від високого спаду напруги на вхідному опорі ТЗП, його підбирають таким, що дорівнює одиницям Ом. Імпеданс такого пристрою несанкціонованого отримання інформації є незалежним від частоти, оскільки не містить у вхідному колі ємнісних та індуктивних елементів.

3. Вибір параметрів моделі АТЛ та характеристика моделювання. При побудові телефонних мереж на ділянці від розподільної шафи до розподільної коробки дуже часто використовуються кабелі типу Т (марки ТГ, ТБ, ТВК, ТК). Залежно від типу ізоляції, змінюється й погонна індуктивність. Для моделювання було вибрано кабель типу ТГ, з паперовою ізоляцією. Первинні параметри такого кабелю дорівнюють $R = 90(\text{Ом})$, $L = 4,16 \cdot 10^{-4}(\text{Гн})$, $C = 50 \cdot 10^{-9}(\text{Ф})$. Цей тип кабелю випускається відповідно до ГОСТ 20902–75, і використовується на ділянці від розподільної коробки до розподільної шафи

При побудові телефонних мереж довжина ділянок АТЛ описується співвідношенням 4:1. Тобто довжина ділянки, на якій використовується кабель такого типу, може становити 800 м, оскільки довжина АТЛ загалом не перевищує 5 км.

4. Аналіз результатів моделювання. Під час аналізу наявності ТЗП на АТЛ використовується порівняння за абсолютними показниками (різниця між очікуваним і вимірними значеннями) і візуальними (порівняння відповідних графіків). У табл. 1 та табл. 2 наведено значення модуля та фази повного опору “чистої” лінії довжиною 800 метрів у режимах холостого ходу (ХХ), короткого замикання (КЗ) та узгодженого навантаження (УН).

Таблиця 1

Параметри \ F, Гц		F, Гц					
		100	200	300	500	800	1000
ХХ	$ Z $, Ом	$3,9789 \cdot 10^4$	$1,9894 \cdot 10^4$	$1,3262 \cdot 10^4$	$0,7957 \cdot 10^4$	$0,4972 \cdot 10^4$	$0,3977 \cdot 10^4$
	j , °	-89,8963	-89,7926	-89,6889	-89,4815	-89,1703	-88,9628
КЗ	$ Z $, Ом	72.0003	72.0012	72.0027	72.0076	72.0194	72.0304
	j , °	0.1664	0.3328	0.4992	0.8319	1.3310	1.6635
УН	$ Z $, Ом	671.9217	671.6870	671.2963	670.0505	667.0417	664.2990
	j , °	-0.7535	-1.5067	-2.2590	-3.7598	-5.9954	-7.4710

Таблиця 2

Параметри \ F, Гц		F, Гц				
		1500	2000	2500	3000	3500
ХХ	$ Z $, Ом	$0,2650 \cdot 10^4$	$0,1987 \cdot 10^4$	$0,1589 \cdot 10^4$	$0,1322 \cdot 10^4$	$0,1132 \cdot 10^4$
	j , °	-88,4433	-87,9229	-87,4012	-86,8779	-86,3526
КЗ	$ Z $, Ом	72.0683	72.1214	72.1895	72.2728	72.3710
	j , °	2.4944	3.3243	4.1527	4.9794	5.8041
УН	$ Z $, Ом	655.0236	642.6474	627.6878	610.7034	592.2458
	j , °	-11.0882	-14.5719	-17.8900	-21.0192	-23.9441

Для визначення оптимальних умов інструментального контролю, виконаємо моделювання усіх режимів вимірювання імпедансу при послідовно і паралельно під'єднаних ТЗП на АТЛ.

Для моделювання послідовно під'єданого ТЗП на АТЛ приймемо, що він розташований на середині лінії. У режимі холостого ходу, у діапазоні частот $f \in (100; 3500)$, такий ТЗП викличе різницю модуля імпедансу $|Z| \in (0,005; 0,045) \text{Ом}$ і фази імпедансу $j \in (0,001 - 0,08)^\circ$, у режимі короткого замикання $|Z| \in (3; 2,985) \text{Ом}$ і $j \in (0,001 - 0,35)^\circ$, а в режимі узгодженого навантаження $|Z| \in (3; 2,5) \text{Ом}$ і $j \in (0 - 0,01)^\circ$.

Результати моделювання показали, що в режимі холостого ходу та узгодженого навантаження різниця модулів та фаз імпедансу “чистої” телефонної лінії та лінії з послідовним ТЗП є незначною, тому виявлення послідовно увімкнених ТЗП, що мають низькоомні вхідні кола, неможливе. У режимі короткого замикання на початку частотного діапазону різниця модулів імпедансу “чистої” АТЛ та лінії з послідовно увімкненим ТЗП визначається вхідним опором, а потім поступово спадає. Тому виявлення послідовно увімкнених ТЗП найкраще здійснювати у режимі короткого замикання у нижньому діапазоні частот каналу тональної частоти.

За використання паралельно під’єданого ТЗП його легше виявити у діапазоні нижніх частот КТЧ в режимі холостого ходу. У цьому режимі для аналізу можна використовувати як модуль, так і фазу імпедансу, оскільки вони зазнають необхідного для виявлення відхилення. При збільшенні частоти виявляючі властивості методу знижуються. Під час інструментального контролю у цьому режимі можна виявляти навіть ТЗП з малими сталими часу (одиниці мілісекунд). У режимах короткого замикання та узгодженого навантаження виявляючі властивості методу значно погіршуються.

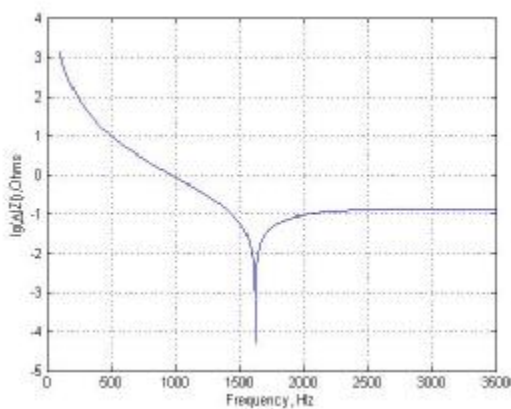


Рис.5. Різниця модулів імпедансних характеристик “чистої” АТЛ та з паралельно під’єданим ТЗП (XX)

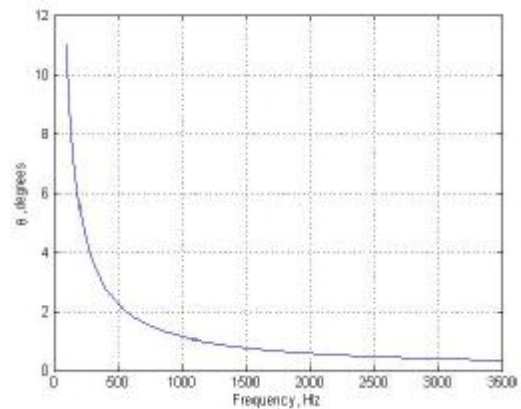


Рис.6. Різниця фаз імпедансних характеристик “чистої” АТЛ та з паралельно під’єданим ТЗП (XX)

Розглянемо, як впливає довжина лінії на виявляючі властивості методу. Для такого аналізу введемо функціональну залежність $\Delta|Z| = f(l)$ та $\Delta j = f(l)$, що відобразить абсолютну різницю модулю і фази імпедансів “чистої” лінії і лінії з ТЗП (при $R_{BX_TSP} = \text{const}$, $f = \text{const}$). Для дослідження чутливості методу при різних довжинах відтинку АТЛ виберемо тестовий сигнал частотою 300 Гц.

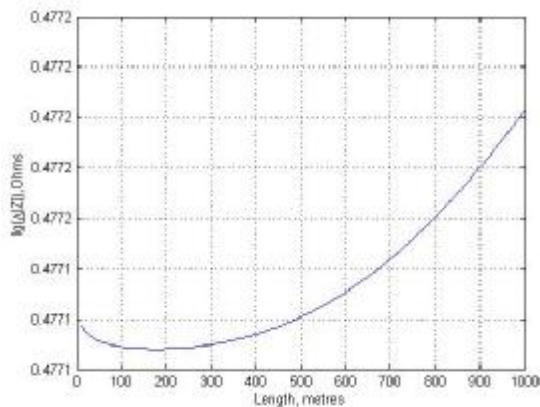


Рис.7. $\Delta|Z| = f(l)$ при послідовно під’єданому ТЗП

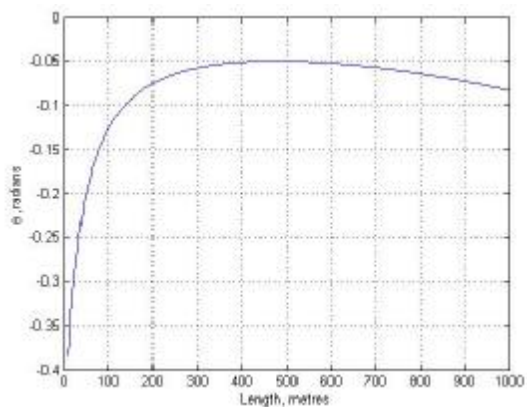


Рис.8. $\Delta j = f(l)$ при послідовно під’єданому ТЗП

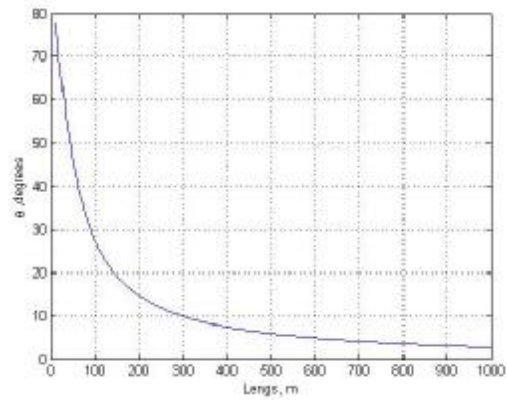
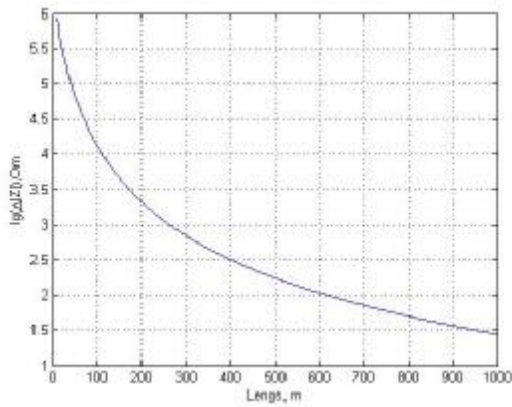


Рис.9. $\Delta|Z| = f(l)$ при паралельно під'єданому ТЗП Рис.10. $\Delta j = f(l)$ при паралельно під'єданому ТЗП

Враховуючи, що цей тип кабелю використовується на ділянці, довжина якої не перевищує 800м, можна вважати цей приріст чутливості при збільшенні довжини АТЛ неістотним.

Отже, виявляючі властивості методу при паралельно під'єданому ТЗП знижуються при збільшенні довжини лінії.

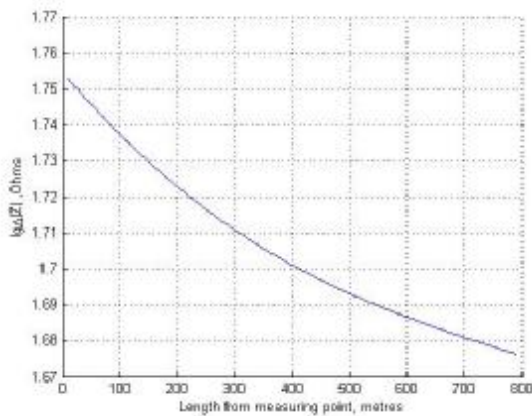


Рис.11. Різниця імпедансних характеристик "чистої" ТЛ і з паралельно під'єданим ТЗП, при різних відстанях монтажу

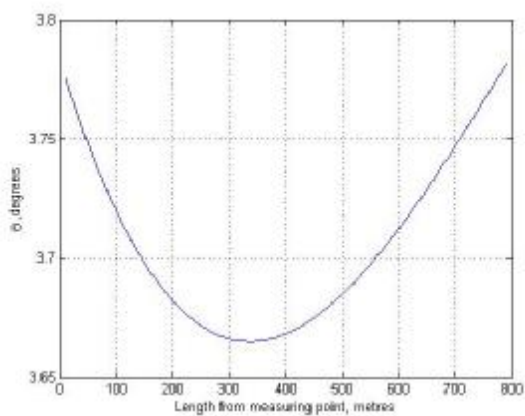


Рис.12. Різниця імпедансних характеристик "чистої" ТЛ і з паралельно під'єданим ТЗП, при різних відстанях монтажу

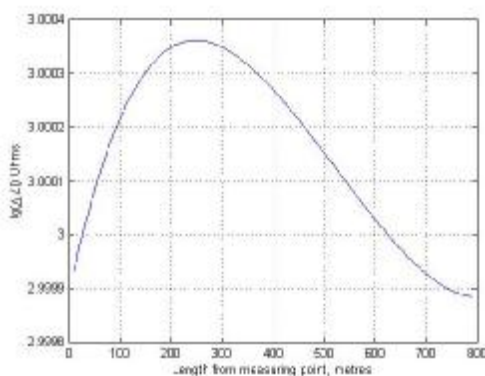


Рис.13. Різниця імпедансних характеристик "чистої" ТЛ і з послідовно під'єданим ТЗП, при різних відстанях монтажу

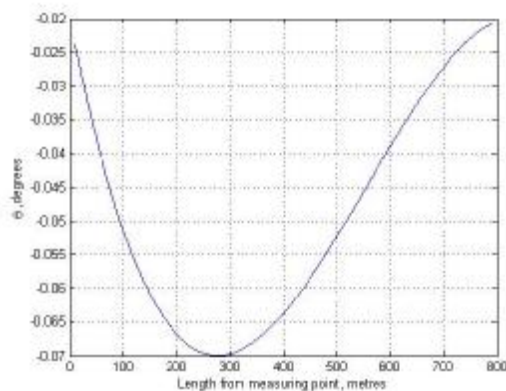


Рис.14. Різниця імпедансних характеристик "чистої" ТЛ і з послідовно під'єданим ТЗП, при різних відстанях монтажу

Розглянемо як впливає віддалення місця під'єднання ТЗП від точки виконання інструментального контролю, при сталій частоті тестового сигналу (300 Гц) і довжині лінії (800 м) при послідовно підключеному ТЗП із паралельно підключеним ТЗП тестового сигналу (300 Гц).

Враховуючи незначні відхилення досліджуваних параметрів, можна зробити висновок, що відстань від точки виконання інструментального контролю до місця встановлення ТЗП не зумовлює значного впливу на виявляючі властивості.

5. Висновки. Високоєфективним для виявлення засобів ведення технічних розвідок на телефонних лініях є імпедансні вимірювання. При їхньому використанні у початковому діапазоні частот КТЧ значно покращується виявлення високоомних паралельно під'єднаних ТЗП та паралельно під'єднаних через конденсатор ТЗП із сталою часу, що дорівнює одиницям мілісекунд.

Під час робіт з виявлення послідовних закладних пристроїв для підвищення ефективності лінію необхідно досліджувати у режимі короткого замикання. Для виявлення паралельно під'єданого через конденсатор ТЗП ефективніше досліджувати лінію у режимі холостого ходу. Загалом властивості цього методу значною мірою залежать від довжини, стану АТЛ та величини і характеру вхідного опору ТЗП.

1. НД ТЗІ 4.7.-001-2001 “Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань”. 2. Халяпин Д.Б. *Защита информации. Вас подслушивают? Защищайтесь.* – М.: НОУ ШО “Баярд”, 2004. – 432 с. 3. Хорев А.А. *Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие.* – М.: Гостехкомиссия России, 1998. – 320 с. 4. Парфенов Ю.А. *Кабели электросвязи.* – М.: Эко-Трендз, 2003 – 256 с. 5. Хорошко В.А., Чекатов А.А. *Методы и средства защиты информации.* – К.: Юниор, 2003. – 504 с. 6. Лагутин В.С., Петряков А.В. *Утечка и защита информации в телефонных каналах.* – М.: Энергоатомиздат, 1996. – 304 с. 7. Нефедов В.И., Сигов А.С., Битюков В.К. *Метрология и электрорадиоизмерения в телекоммуникационных системах.* – 3-е изд. – М.: Высш. шк., 2005. – 599 с. 8. *Универсальный анализатор проводных коммуникаций ULAN-2. Руководство по эксплуатации.*