*Литература: **1.** Барсуков В. С. Безопасность: технологии, средства, услуги. – М.: КУДИЦ-ОБРАЗ, 2001 **2.** Генне О. В. Основные положения стеганографии // Защита информации. Конфидент, № 3, 2000 **3.** E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996. **4.** Markus G. Kuhn and Ross J. Anderson: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. (http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf)*

УДК 621.396

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ В ПАСИВНИХ ЕЛЕМЕНТАХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Михайло Прокофьєв, Андрій Тодоренко, Володимир Свірський*
НДЦ "ТЕЗІС" НТУУ "КПІ"
**НТУУ "КПІ"*

Анотація: **Розглянута проблема вибору покажчика призначення для оцінки захищеності інформації, яка циркулює в пасивних елементах локальних обчислювальних мереж, від витоку каналами побічних електромагнітних випромінювань.**
Summary: **The problem of choice the parameter of purpose for an estimation of the information security, which circulates in passive elements LAN from outflow on TEMPEST channels, is considered.**
Ключові слова: **Локальна обчислювальна мережа, побічні електромагнітні випромінювання, тестові сигнали, гармонічний сигнал, покажчик призначення.**

I Вступ

Будь-яка локальна обчислювальна мережа (ЛОМ) містить в собі три такі основні елементи: кінцеве обладнання користувачів (робочі станції, сервери), активне комутаційне обладнання (концентратори, комутатори, маршрутизатори), пасивне обладнання (інсталяційні кабелі, комутаційні шнури, з'єднувальні модулі, комутаційні панелі).

Перші два елементи є прикладом об'єктів, зосереджених в обмеженому просторі, а третій елемент – є розосередженим. Система технічного захисту інформації (ТЗІ) передбачає схожі для всіх трьох елементів методи захисту інформації від витоку за рахунок побічних електромагнітних випромінювань (ПЕМВ): екранування, активне або пасивне зашумлення. Опис витоку інформації каналами ПЕМВ та реалізація методів захисту інформації від витоку такими каналами розглянуті в [1 – 6].

В статті розглянуто питання оцінки ступеню захищеності інформації, що циркулює лише у пасивному обладнанні ЛОМ, бо для нього чинні нормативні документи в галузі технічного захисту інформації визначають покажчики призначення, їх нормативи та методи розрахунків, які не можуть бути застосовані для порівняння між собою пасивного обладнання ЛОМ різних виробників до початку виконання робіт з монтажу цього обладнання.

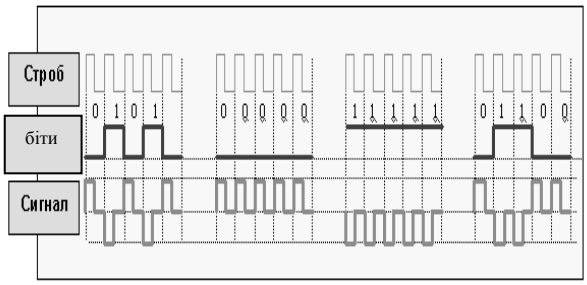
II Основна частина

Оцінка ступеню захищеності інформації, що циркулює в елементах ЛОМ, від витоку каналами ПЕМВ здійснюється за методикою, яка як покажчик призначення використовує величину радіуса зони II і передбачає проведення випробувань лише на конкретному об'єкті. При цьому просторова конфігурація всіх елементів, що входять до її складу, має бути відома. Будь-яка майбутня заміна встановленого пасивного обладнання ЛОМ на інше, або в іншому місці спричинить необхідність проведення повторних випробувань. Більше того, внаслідок проведення вимірювань у конкретних умовах не можливо порівняти властивості пасивного обладнання ЛОМ різних виробників з точки зору ТЗІ. Крім того, якщо результати випробувань будуть незадовільними, то перебудова ЛОМ потребує від її власника додаткових фінансових витрат. Для того, щоб проектувальник ЛОМ зміг вирішити, які компоненти і якого виробника йому слід обрати аби досягти потрібного ступеня захисту інформації, необхідно провести попередні випробування всіх елементів ЛОМ в однакових умовах.

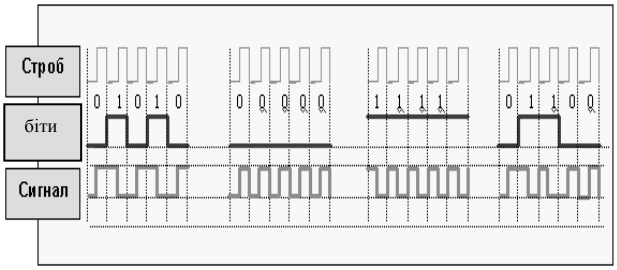
Оцінка захищеності інформації за існуючою методикою передбачає створення тестового сигналу, що задовольняє таким вимогам: схожість структури реального інформативного сигналу та тестового;

забезпечення максимальної завантаженості елементу ЛОМ під час обробки ним тестового сигналу; забезпечення максимального співвідношення "сигнал/шум" для тестового сигналу.

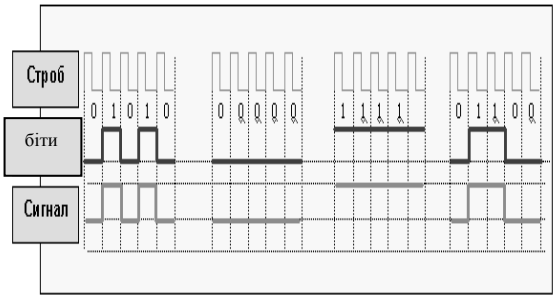
ЛОМ як фізичне середовище передавання інформації використовує кабельну мережу. Інформація при передаванні через кабельну мережу кодується з використанням певних методів кодування. На сьогоднішній день кількість методів кодування інформації, що використовують в ЛОМ, перевищила десяток. Структура бітів інформації та інформаційних сигналів декількох методів кодування наведена на рис. 1.



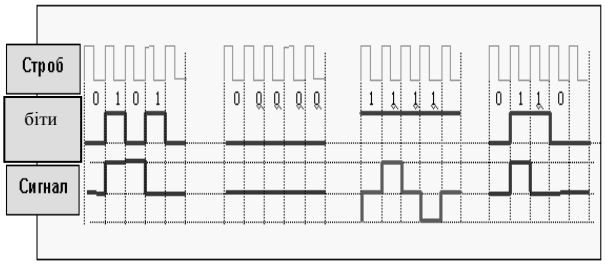
трьохрівневий код RZ



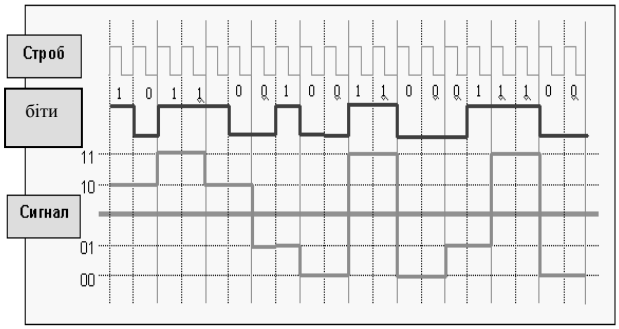
дворівневий код Manchester II



дворівневий код RZ



трьохрівневий код MLT-3



п'ятирівневий код PAM-5

Рисунок 1 – Структура бітів інформації та інформаційних сигналів для різних методів кодування

З структури випливає, що для виконання перших двох вимог потрібно буде створити тестові сигнали для кожного з існуючих методів кодування. При цьому значно зростає обсяг та вартість експертних випробувань. До того ж створити такі тестові сигнали за допомогою спеціальних генераторів дуже складно і тому при проведенні випробувань потрібно використовувати реальне кінцеве та активне комутаційне обладнання.

Внаслідок малої амплітуди сигналів від кінцевого обладнання та активного комутаційного обладнання для виконання третьої вимоги треба розташовувати пасивне обладнання ЛОМ у екранованому приміщені. Оскільки розміри кабельних мереж складають сотні метрів, то використовувати такі екрановані приміщення дуже проблематично. Крім того екрановані приміщення мають власні резонансні частоти і результати вимірювання на цих частотах будуть некоректні [7].

Для рішення цих проблем тестовий сигнал має бути таким, щоб результати випробувань за ним можна

було розповсюдити на всі існуючі методи кодування та мати можливість порівнювати результати випробувань пасивного обладнання ЛОМ різних виробників.

Прикладом такого тестового сигналу може стати гармонічний сигнал. Використання гармонічного сигналу як тестового є досить розповсюдженим явищем. Комунікаційні тестери (Omni Scan та багато інших) використовують саме гармонічний тестовий сигнал. Відома випробувальна лабораторія "3р" (Данія) при проведенні випробувань кабелів використовує також гармонічні сигнали.

Впровадження гармонічного тестового сигналу замість імпульсного дозволить отримати наступні переваги:

- не застосовувати кінцеве обладнання та активне комутаційне обладнання під час проведення випробувань; це позбавляє зайвих ПЕМВ, що виникають під час роботи цього обладнання;
- значно збільшити амплітуду тестового сигналу в порівнянні з амплітудою сигналу від кінцевого та активного комутаційного обладнання, що дозволяє підвищити співвідношення "сигнал/шум" і таким чином відмовитись від проведення випробувань у екранованих приміщеннях;
- отримати незалежність результатів випробувань від існуючих методів кодування інформації;
- порівнювати результати випробувань пасивного обладнання ЛОМ різних виробників.

Впровадження гармонічного тестового сигналу потребує використання генераторів гармонічних сигналів із симетричним виходом або створення спеціальних симетрируючих пристроїв. Подібні симетрируючі пристрої виготовляє випробувальна лабораторія "3р" (Данія).

Проте застосування гармонічного тестового сигналу не знімає проблеми проведення випробувань пасивного обладнання ЛОМ в умовах невизначеності її просторового розташування. Остаточно розрахована величина радіусу зони II за методикою оцінки захищеності при проведенні випробувань пасивного обладнання ЛОМ може бути як більшою за величину радіусу зони II, розрахованої на конкретному об'єкті захисту, так і меншою.

Слід відзначити, що величина випромінювання залежить від первинних характеристик пасивного обладнання ЛОМ (нерівномірність кроку звиву дротів та пар дротів у кабелі та інші). Конкретне значення первинної характеристики має ймовірний характер, тому і величина випромінювання теж буде мати ймовірний характер.

Намагаючись уніфікувати просторову конфігурацію пасивного обладнання ЛОМ при випробуваннях розглянемо такі два варіанти.

Перший варіант випливає з методики оцінки захищеності, яка передбачає створення таких умов випробувань, коли випромінювання інформативного сигналу максимальне. Максимального випромінювання можна досягти, якщо відрізок елементу пасивного обладнання ЛОМ максимальної довжини (100 м) згорнути у кільце, причому довжина одного кільця має бути кратною довжині хвилі інформативного сигналу. Але такі умови випробувань не відповідають просторовій конфігурації пасивного обладнання ЛОМ у реальних умовах.

Просторову конфігурацію пасивного обладнання ЛОМ також можна розглядати як сукупність прямолінійних відрізків різної довжини, у граничному вигляді – це один великий прямолінійний відрізок. З цього випливає другий варіант, коли просторова конфігурація виглядає як відрізок максимальної довжини, прокладений прямолінійно. Відомо, що існує залежність величини випромінювання сигналу від матеріалу підлоги та способу прокладання (по поверхні, під нею, у повітрі) [8]. В більшості випадків пасивне обладнання ЛОМ прокладають безпосередньо по поверхні стін та підлоги, і тому перший варіант найбільш вірогідний.

При цьому виникає два питання: у скількох точках уздовж пасивного обладнання ЛОМ треба проводити вимірювання та в якому діапазоні частот.

Чим більше кількість точок вимірювання, тим краще. В ідеалі будемо мати суцільну залежність величини випромінювань уздовж всього пасивного обладнання ЛОМ. Мінімальна кількість точок визначається найменшою довжиною хвилі тестового сигналу.

Пасивне обладнання ЛОМ, як випливає з назви, призначене тільки для передавання сигналів між мережевим адаптером (мережевої картки) та активним комутаційним обладнанням. Мережевий адаптер генерує інформативні сигнали за законом зміни бітів інформації. Вищі гармоніки інформативних сигналів дійсно можуть значно перевищувати діапазон робочих частот кабелю. Інколи при вимірюваннях випромінювань на частотах вищих гармонік від системи "мережевий адаптер – пасивне обладнання ЛОМ" їх величина перевищує нормативні значення. Наразі проблему зменшення цієї величини намагаються вирішити за рахунок застосування заходів щодо пасивного обладнання ЛОМ. Але такий підхід вимагає більших витрат на заходи з екранування або зашумлення. На наш погляд заходи із зменшення амплітуди вищих гармонік треба застосовувати до мережевого адаптера, а не до пасивного обладнання ЛОМ, це значно зменшить витрати часу та коштів. Такий підхід вимагає лише застосування обмежувальних фільтрів вищих частот на

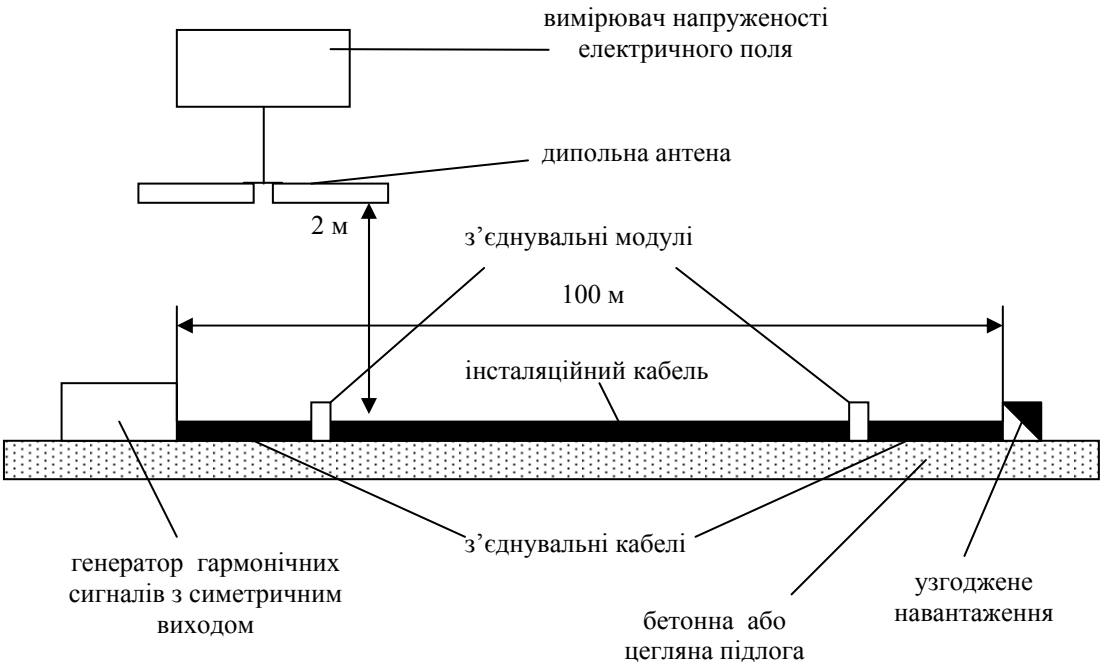


Рисунок 2 – Випробувальний стенд для вимірювання випромінювань

виході мережевого адаптера.

Реалізація варіанту випробувального стенду для вимірювання випромінювань, коли пасивне обладнання ЛОМ виглядає як відрізок максимальної довжини, прокладений прямолінійно, наведена на рис. 2.

Розглянемо також інший спосіб вибору покажчика призначення оцінки захищеності пасивного обладнання ЛОМ – використання типових характеристик пасивного обладнання ЛОМ, викладених в [9]. Однією з таких характеристик може стати Coupling Loss (втрати на зв'язок) або Coupling Attenuation (загасання зв'язку). Використання цієї характеристики як визначного параметру вже обговорювалося в [10]. Фізичний зміст цієї характеристики полягає у співвідношенні переданої потужності в елемент пасивного обладнання ЛОМ до випроміненої нею потужністю на фіксованій частоті та від фіксованої точки елементу пасивного обладнання ЛОМ. Формула розрахунків та схема випробувального стенду для вимірювання Coupling Attenuation наведена у [8]. Якщо виробники пасивного обладнання ЛОМ будуть надавати інформацію про мінімальну величину Coupling Attenuation на фіксованих частотах, то проектувальники ЛОМ зможуть оцінити, який тип пасивного обладнання та від якого виробника їм треба обрати, щоб досягти потрібного ступеню захисту інформації.

На рис. 3 наведені результати вимірювань Coupling Attenuation в двох випадках – при прокладанні пасивного обладнання ЛОМ по бетонній підлозі (а) та при прокладанні пасивного обладнання ЛОМ під землею (б).

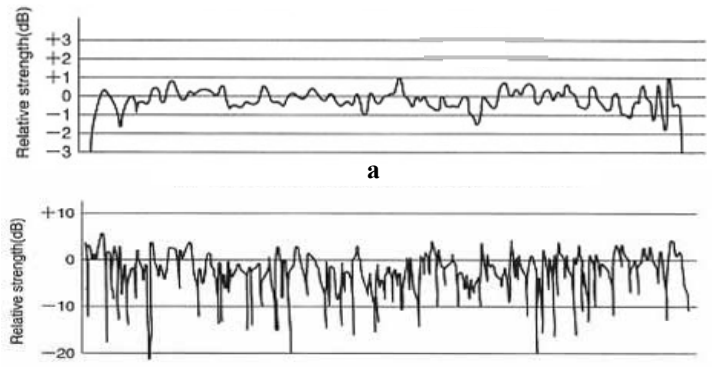


Рисунок 3 – Відносна нерівномірність величини Coupling Attenuation уздовж кабелю

Проте такий підхід теж має свої недоліки. Наприклад, за [9] Coupling Attenuation вимірюється в одній точці та на фіксованих частотах, але цього недостатньо для вирішення питання щодо вибору пасивного обладнання ЛОМ.

В реальних умовах прокладання пасивного обладнання ЛОМ існує відбита хвиля від неоднорідностей (стін, підлоги, стелі), що створює "флуктуації" електричного поля. Завдяки цим флуктуаціям не можна сказати, в якій точці пасивного обладнання ЛОМ та на якій частоті інформативного сигналу буде знаходитися мінімум Coupling Attenuation. Аналіз результатів вимірювань, наведених у [9] та [11] свідчить про те, що відносне зменшення абсолютної величини Coupling Attenuation із збільшенням частоти інформативного сигналу співпадає з відносною величиною флуктуацій величини Coupling Attenuation внаслідок впливу неоднорідностей.

Результати вимірювань випромінювання декількох структурованих кабельних систем різних класів у випробувальній лабораторії НДЦ "ТЕЗІС" наведені на рис. 4. Результати свідчать, що з ростом частоти якість екранування кабелем зростає, але вплив неоднорідностей вносить суттєві спотворення, особливо це помітно на низьких частотах. З рис. 4 видно, що величина випромінювання залежить не тільки від типу кабелю, а ще від багатьох факторів (зокрема, величини опору заземлення), які важко врахувати під час проведення випробувань. Це помітно якщо вимірювання одного і того самого кабелю провести декілька разів.

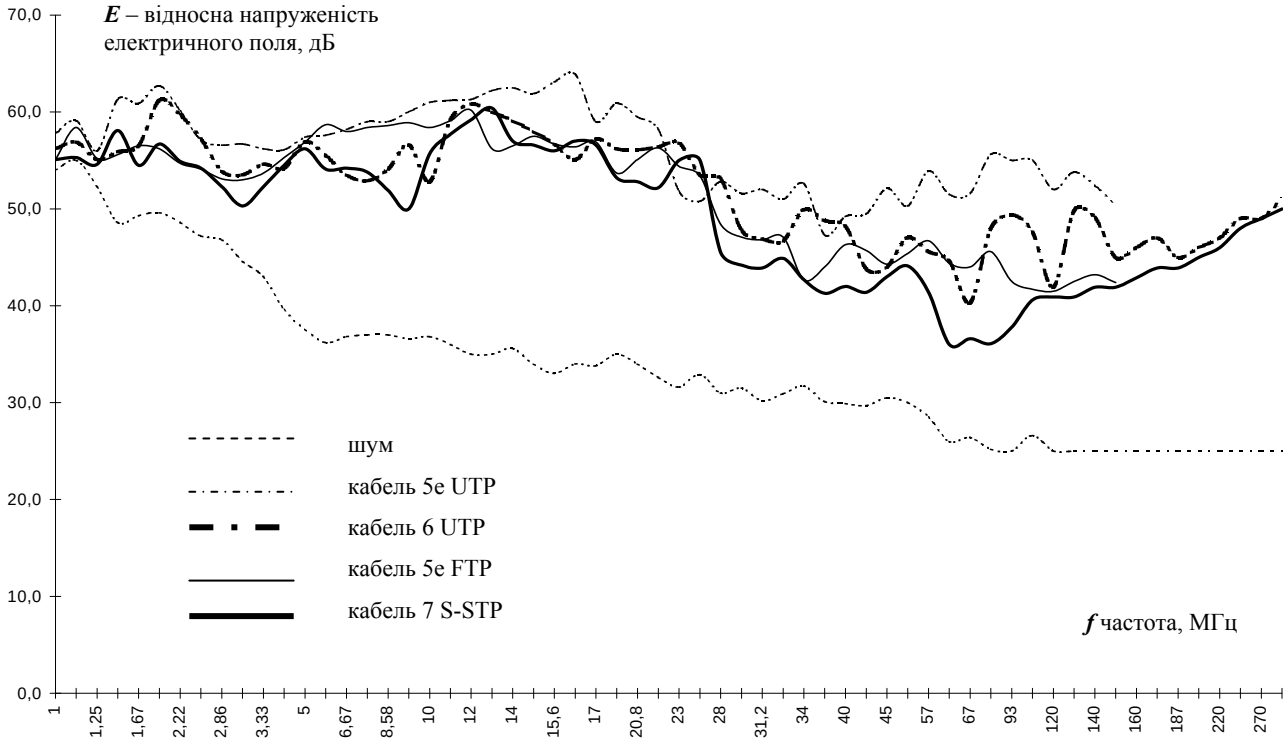


Рисунок 4 – Результати вимірювань випромінювання структурованих кабельних систем у випробувальній лабораторії НДЦ "ТЕЗІС"

III Висновки

Результати свідчать, що з ростом частоти якість екранування кабелем зростає, але вплив неоднорідностей вносить суттєві спотворення, особливо це помітно на низьких частотах. Величина випромінювання залежить не тільки від типу кабелю, а ще від багатьох факторів (зокрема величини опору заземлення), які важко врахувати під час проведення випробувань.

Для того, щоб результати випробувань були незалежні від використаного метода кодування інформації в ЛОМ та щоб мати можливість порівнювати ступінь захищеності інформації в ЛОМ різних виробників, краще як тестовий сигнал використовувати гармонічний сигнал.

Література: ***1.*** *Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної*

техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). ***2.*** *Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ -ПЕМВН-95).* ***3.*** *А А Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Принципы построения. // Компьютеры + программы – 1998. – № 3.* ***4.*** *А. А Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Защита от физического разрушения. // Компьютеры + программы. – 1998. – № 4.* ***5.*** *А. А. Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Защита от утечки информации по техническим каналам. // Корпоративные системы. – 1999. – № 2.* ***6.*** *А. А. Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Особенности реализации. // Корпоративные системы. – 1999. – № 3.* ***7.*** *Е. А. Зайцев. Резонанс экранированных систем. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., – 2002. – Вип. 5. – С. 207–210.* ***8.*** *http://www.mitsubishi-cable.co.jp/product/hikari/leakycl.html.* ***9.*** *ISO/IEC 1180. Second Edition. Information technology – Generic cabling for customer premises.* ***10.*** *А. Савчук. Проблемы технической защиты информации и электромагнитной совместимости для структурированных кабельных систем. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., – 2002. – Вип. 5. – С. 58–63.* ***11.*** *http://www.andrew.com.*

УДК 621.391.883

К ВОПРОСУ О ЗАЩИТЕ АБОНЕНТСКИХ ТЕЛЕФОННЫХ ЛИНИЙ УСТРОЙСТВАМИ КОМПЛЕКСНОЙ ЗАЩИТЫ

Владимир Луценко, Александр Архипов, Валерий Худяков*, Сергей Дедусенко**
НТУУ "КПИ", Физико-технический институт
**НИИ Электромеханических приборов, г. Киев*
***ЧП фирма "Бумекс", г. Киев*

Аннотация: **Рассматриваются вопросы технической защиты информационных потоков в абонентских телефонных линиях общего пользования. Сформулированы направления развития этих вопросов и проведен обзор существующих средств защиты телефонных аппаратов и линий. Определен круг наиболее дефицитных технических средств, проблемы, стоящие перед разработчиками и пользователями таких средств и возможные пути их решения.**

Summary: **The problems of technical protection of information flows in lines TLF of abonents of the general use. The directions are formulated, in which one it is necessary to develop activities for protection of the information against unauthorised users, the analysis of available and substantially created the hardware of protection. The circle of the most deficient means, systems in area of technical information protection, and possible paths of their creation as soon as possible is determined.**

Ключевые слова: **Защита информационных потоков, безопасность переговоров, активные и пассивные методы защиты.**

I Введение

Актуальность вопроса защиты телефонных линий и оконечных аппаратов телефонной связи в сетях общего пользования повышается из года в год. Важность вопроса не уменьшается по причине возрастания объемов оснащения различных структур импортной техникой, не прошедшей сертификации по технической защите информации (ТЗИ). И если процесс оснащения государственных структур в какой-то мере поставлен под контроль Департамента специальных телекоммуникационных систем и защиты информации (ДСТСЗИ) Службы безопасности Украины, то в остальных случаях этот процесс практически бесконтролен. Одной из причин такого положения дел является отсутствие целостной программы создания системы безопасности в рамках национальной системы ТЗИ. Кроме того, актуальность вопроса возрастает и в связи с интенсивным насыщением страны все более развитыми средствами связи, использующими "гибридные" каналы, аналоговые и цифровые, проводные и радиоканальные в единой системе связи. Это происходит на фоне неизбежных глобальных информационных процессов, характеризующихся повышенным вниманием к уязвимости информационных ресурсов и связных каналов коммерческих и государственных структур, страны в целом, что приводит к заметному возрастанию ущерба владельцев информационных ресурсов в результате объективной возможности утечки конфиденциальной информации.