RS Global Journals

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773
Tel: +48 226 0 227 03
Email: editorial_office@rsglobal.pl

JOURNAL	International Journal of Innovative Technologies in Social Science
p-ISSN	2544-9338
e-ISSN	2544-9435
PUBLISHER	RS Global Sp. z O.O., Poland

ARTICLE TITLE	ОГЛЯД МЕТОДІВ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ, СФОРМОВАНИМИ ВИСОКОЧАСТОТНИМИ НАВ'ЯЗУВАННЯМИ
AUTHOR(S)	Крючкова Лариса Петрівна, Цмоканич Іван Володимирович
ARTICLE INFO	Kriuchkova Larysa, Tsmokanych Ivan. (2021) Overview of Methods of Protection of Acoustic Information Against Leaks by Channels Formed by High-Frequency Impositions. International Journal of Innovative Technologies in Social Science. 3(31). doi: 10.31435/rsglobal_ijitss/30092021/7685
DOI	https://doi.org/10.31435/rsglobal_ijitss/30092021/7685
RECEIVED	07 August 2021
ACCEPTED	14 September 2021
PUBLISHED	17 September 2021
LICENSE	This work is licensed under a **Creative Commons Attribution 4.0 International License.**

ОГЛЯД МЕТОДІВ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ, СФОРМОВАНИМИ ВИСОКОЧАСТОТНИМИ НАВ'ЯЗУВАННЯМИ

Крючкова Лариса Петрівна, *д.т.н., доцент, професор кафедри систем інформаційного та кібернетичного захисту Державного університету телекомунікацій, Київ, Україна,*
ORCID ID: https://orcid.org/0000-0002-8509-6659
Цмоканич Іван Володимирович, *аспірант кафедри систем інформаційного та кібернетичного захисту Державного університету телекомунікацій, Київ, Україна,*
ORCID ID: https://orcid.org/0000-0002-5085-8457

DOI: https://doi.org/10.31435/rsglobal_ijitss/30092021/7685

ARTICLE INFO

Received 07 August 2021
Accepted 14 September 2021
Published 17 September 2021

KEYWORDS

high-frequency imposition, technical information leakage channel, method of acoustic information protection, dangerous signal, parasitic modulation, dangerous signal parameters, protective signal.

ABSTRACT

The existing methods of information protection from leakage by high-frequency imposition channels are considered. The main differences between them, their general advantages and disadvantages, as well as the main methods of high-frequency imposition are described. The ways of using methods, their complex combination to ensure full protection of information are analyzed. The types of signals that may be present at the facility where critical information is processed are described. The channels of information leakage are described both in the power supply and grounding channels and through the dielectric (air). The main components of the signal that need to be considered when assessing the electromagnetic environment at the facility are also considered. Examples of application of passive, active and complex measures to ensure information protection are studied. The purpose of further research is to study the parameters of the hazardous signal, improve existing methods of information protection to ensure high-quality information protection and develop an algorithm for rapid response to changes in the electromagnetic environment at the facility to ensure faster response to prevent information leakage. The priority tasks are mathematical and experimental study of the parameters of the dangerous signal in order to identify opportunities for the destruction of its basic parameters in order to reduce its level of informativeness, as well as finding an algorithm for rapid response to changes in the electromagnetic environment. Both the positive aspects and the difficulties that may occur during the above research are outlined.

Citation: Kriuchkova Larysa, Tsmokanych Ivan. (2021) Overview of Methods of Protection of Acoustic Information Against Leaks by Channels Formed by High-Frequency Impositions. *International Journal of Innovative Technologies in Social Science*. 3(31). doi: 10.31435/rsglobal_ijitss/30092021/7685

Вступ. На даний момент у світі прослідковується процес глобальної інформатизації суспільства. Реальна безпека держави багато в чому залежить від безпеки її інформаційних ресурсів і технологій, а забезпечення безпеки інформації залежить від захисту конфіденційної інформації. Саме тому захист національної конфіденційної інформації є одним з головних пріоритетів державної політики.

Одним з ефективних методів перехоплення конфіденційної інформації, що циркулює в апаратурі основних технічних засобів і систем (ОТЗС) або наводиться у допоміжних технічних засобах і системах (ДТЗС), є метод високочастотного нав'язування (ВЧН).

Канали витоку інформації формуються за рахунок акустоелектричних перетворень, що утворюються при одночасному впливі на елементи технічних засобів конфіденційних мовленнєвих сигналів та зондуючого високочастотного сигналу, якщо не було вжито радикальних заходів, що перешкоджають проникненню струмів високої частоти всередину технічних засобів [1].

Огляд методів захисту інформації від витоку каналами, сформованими високочастотним нав'язуванням, є актуальним, адже до сьогодні не знайдено методу, здатного повноцінно захищати конфіденційну інформацію від перехоплення методами ВЧН. В публікації розглянуто доступні авторам методи захисту інформації від перехоплення методами ВЧН з метою їх вдосконалення і подальшого ефективного використання на об'єктах інформаційної діяльності.

Матеріали та методи.

В даний час застосовуються два методи високочастотного нав'язування:

- за допомогою контактного або індукційного введення високочастотного сигналу в електричні кола, які мають функціональні або паразитні зв'язки з основним технічним засобом;
- шляхом опромінення високочастотним електромагнітним сигналом джерела інформації і прийняття відбитого модульованого сигналу.

Якість перехоплення інформації за допомогою ВЧН залежить від ряду факторів [2]:

• характеристик і просторового положення джерела сигналу;

• наявності в контрольованому приміщенні нелінійного елемента (пристрою), параметри якого (геометричні розміри, положення в просторі, індуктивність, ємність, опір і т. д.) змінюються за законом сигналу;

• характеристик зовнішнього джерела, яке задає небезпечний сигнал;

• типу приймача відбитого сигналу.

Загальне уявлення про розмаїття методів такого перехоплення дає наступна класифікація:

Таблиця 1.

1. За діапазоном частот:	радіо, оптичні
2. За середовищем поширення:	струмопровідними комунікаціями, через діелектрик (повітря)
3. За використанням спеціально впроваджених на об'єкті пристроїв	з впровадженням, дистанційні
4. За оперативністю отримання інформації	в реальному масштабі часу, з часовою затримкою.

На сьогодні використовуються пасивні, активні та комбіновані методи захисту інформації від перехоплення. Також існує поділ на організаційні та технічні методи захисту інформації.

До основних організаційних заходів відносять [3]:

1. Залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ);
2. Категорування й атестацію об'єктів ОТЗС та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;
3. Використання на об'єкті сертифікованих ОТЗС та ДТЗС;
4. Встановлення КЗ навколо об'єкта;
5. Залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;
6. Організацію контролю та обмеження доступу на об'єкти ОТЗС та у виділені приміщення;
7. Введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;
8. Відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Серед загальновідомих методів захисту інформації від перехоплення за допомогою високочатотного нав'язування можна вказати наступні: встановлення додаткових конструкцій екранування на початкових етапах розробки апаратури, яка буде використовуватись; встановлення додаткового екранування конструкції; встановлення фільтрації високочастотних зондуючих сигналів в усіх підключених до апаратури електричних колах і лініях зв'язку. Однак вказані пасивні методи не забезпечують повноцінного захисту інформації.

Мета пасивних і активних методів захисту – зменшення відношення сигнал / шум на межі контрольованої зони до величин, які забезпечують неможливість виділення засобом розвідки зловмисника небезпечного інформаційного сигналу. В пасивних методах захисту зменшення відношення сигнал/шум досягається шляхом зменшення рівня небезпечного сигналу, в активних методах – шляхом збільшення рівня шуму [4].

Як пасивні, так і активні засоби захисту мають свої характерні переваги і недоліки.

Як зазначають автори І.С. Антясов, А.П. Яресько та А.Н. Соколов, перевагами пасивних засобів захисту є:

• Малі габарити, проста електрична схема;

• Зовнішнє електроживлення не потрібно;

• вони включаються в розрив ланцюгів і тому вихід з ладу деяких елементів електричної схеми виявляється в процесі експлуатації;

• невисока вартість щодо інших типів засобів.

Водночас, активні засоби захисту, в порівнянні з пасивними, мають більш складну будову, високу вартість, а також вимагають зовнішнього джерела електроживлення. Але, незважаючи на ці недоліки, часто виявляється, що ефективність активних засобів захисту вище, ніж у пасивних. Відповідно комбіновані засоби захисту побудовані на основі комбінації пасивних і активних засобів. До найбільш широко застосовуваних пасивних методів захисту відносяться:

• обмеження сигналів малої амплітуди;

• фільтрація сигналів високочастотного нав'язування

• відключення перетворювачів (джерел) сигналів. [5]

Слід зауважити, що у даній статті розглядається проблематика захисту інформації від перехоплення в телефонних лініях. Серед перелічених методів відсутній такий, який впливав би безпосередньо на параметри небезпечного сигналу, який генерується з метою перехоплення інформації.

С.І. Лізунов та К.І. Розумовський зазначають, що використання активних засобів має певні недоліки [6]:

- При зміні розташуванні джерела інформаційного сигналу (наприклад, перестановки ПК або додавання нових), загальний рівень сигналу в приміщенні можуть змінитися таким чином, що сигнали можна виявити поза приміщенням, незважаючи на зашумлення.

- Необхідно зашумлювати сигнали в широкому діапазоні частот. Межі цього діапазону не завжди можна чітко визначити із-за биття кількох сигналів, а також можливого зовнішнього ВЧ впливу.

- Наявність пригнічуючих випромінювань демаскує об'єкт і може перешкоджати роботі інших чужих пристроїв за межами контрольованої зони.

- Використання активних засобів передбачає постійні додаткові дії (наприклад, підготовка комплексу до роботи, включення, виключення, профілактика, постійна перевірка його практики та тому подібне).

- Необхідні додаткові джерела живлення. Іноді це приводить до обмеження працездатності генераторів шуму в часі.

Автори О.К. Барановський та А.Ф. Мельник у своїй статті [7] зробили висновок, що метод перехоплення інформації високочастотного нав'язування складний для виявлення тому, що має широкий діапазон допустимих частот, в той час пристрої, робота яких спрямована на виявлення високочастотного нав'язування, мають змогу здійснювати перевірку тільки у вузькому діапазоні частот.

В цій статті пропонується варіант захисту інформації від перехоплення шляхом організації каналу в певній полосі частот. В такому разі передача даних буде здійснюватись з певними спотвореннями. Відповідно зловмиснику буде потрібно періодично повторювати параметри свого небезпечного сигналу, що на практиці дуже важко реалізувати. Однак навіть у

такому випадку у зловмисника є можливість аналізувати весь спектр, який утворюється від високочастотного нав'язування, накопичувати варіації сигналів та виділяти важливі для себе частини. Тому цей метод також не гарантує повноцінного захисту інформації, якщо навіть не враховувати складність його реалізації.

Одним із найбільш дієвих методів захисту інформації можна вважати метод, який базується на генеруванні сигналів завади. У статті В.В. Ткаченка та В.В. Єрмошина [8] розглядається поняття моделі сигналу ВЧН та пропонується використовувати різні моделі сигналів завади, так як від моделі залежить ефективність її використання задля захисту інформації від перехоплення.

Згідно цієї роботи при оцінці електромагнітної обстановки потрібно враховувати три складові:

1. ВЧ-сигнал
2. Завади
3. Внутрішні або власні шуми приймача сигналу.

Відповідно до цього в сумі організовується так звана адитивна суміш, яка має наступний вигляд:

$$U_{Bx_i}(x,t) = U_v(x,t,\beta_h) + n(x,t) \text{ при } t = 0$$

$$U_{Bx_i}(x,t) = U_{31}(x,t,\alpha_3,\beta_3) + U_v(x,t,\beta_c) + n(x,t) \text{ при } t = 1,$$

де $U_{31}(x,t,\alpha_3,\beta_3)$ – сигнал ВЧ-нав'язування,

$U_v(x,t,\beta_h)$ – сигнал завади, який є непередбаченим,

$n(x,t)$ – власні шуми приймаючого пристрою, перераховані до входу приймача.

Корисні сигнали відрізняються один від одного параметрами, на кількість яких вказує індекс і-го класу сигналу. Велика кількість видів корисних сигналів та сигналів завади систематизуються шляхом введення типових моделей або типових видів сигналів.

Такими сигналами є детерміновані, квазідетерміновані і випадкові (складні) корисні сигнали, детерміновані, квазідетерміновані, випадкові і групові сигнали завади. В якості видової ознаки типових моделей сигналів і завад виступають амплітуда та початкова фаза.

Детерміновані сигнали і завади мають невипадкові амплітуди і початкові фази (із умови нормування амплітуди беруться рівними одиниці).

Квазідетерміновані сигнал і завада мають випадкові амплітуди та (або) початкові фази. При цьому типовим видом є сигнали із випадковими амплітудами і випадковими початковими фазами, які характеризуються найбільшим ступенем випадковості в цьому вигляді сигналів і найбільш часто зустрічаються на практиці. Але у відношенні сигналів завади потрібно також використовувати і модель з невипадковою амплітудою і випадковою початковою фазою, яка адекватна непередбачуваній заваді, яка створюється при умові близького розташування джерела і рецептора завад. При невипадковій амплітуді її значення приймають рівним одиниці, а при випадковій амплітуді остання нормується таким чином, що її другий початковий момент, який є нормованим множником потужності сигналу, був рівним одиниці.

Випадкові сигнали на відміну від детермінованих і квазідетермінованих сигналів, які відносяться до простих сигналів, є складними. Вони характеризуються наявністю послідовності в часі і (або) просторі ряду квазідетермінованих сигналів. Кожен з таких сигналів називається елементарним і має незалежні від інших елементарних сигналів випадкові несуттєві параметри (амплітуду і початкову фазу). До числа складних відносяться випадкові шумові і не шумові сигнали. Тому складні сигнали часто називають випадковими.

Аналогічним чином визначаються детерміновані, квазідетерміновані і випадкові сигнали завади. Додатковим видом до цього відноситься групова завада, яка представляє собою суму сигналів завади перших трьох типів, які накладаються один на одного в часі та (або) в просторі [4].

Підсумовуючи вищесказане, слід зауважити, що на об'єктах, де обробляється критично важлива інформація, можуть бути присутні різні види сигналів та завад. У варіанті, коли системи з непорушними антенами знаходяться на близьких відстанях одна від одної, сигнали завади мають постійні або відомі несуттєві параметри. В таких умовах роботою є модель детермінованої завади.

В.В. Хома [9] описує вплив високочастотного нав'язування на абонентські телефонні лінії. Серед варіантів вирішення питання захисту інформації від перехоплення пропонується

використання загороджувальних фільтрів. Амплітудно-частотна характеристика таких фільтрів має забезпечувати так звану «прозорість» в інтервалі каналу тональної частоти (300 – 3400 Гц) і якомога більше згасання на частотах позазвукового діапазону.

Найпростішим варіантом загороджувального фільтра є конденсатор, встановлений у мікрофонне коло телефонного апарата або у коло електромагнітного дзвінка виклику. Ємність конденсатора вибирають так, що зашунтувати зондувальні сигнали високочастотного нав'язування і разом з тим істотно не впливати на корисні сигнали.

Складнішим варіантом розглядається можливість використання активних засобів. Він полягає у накладанні захисного шуму на небезпечний сигнал. Розрізняють низькочастотні маскувальні сигнали в діапазоні від 100 Гц до 10 кГц та високочастотні широкосмугові – від 20 кГц до 30 МГц. Внаслідок ефекту маскування не вдається засобами технічної розвідки виділити інформативні параметри сигналів витоку.

На нашу думку, ідею застосування активних засобів можна реалізувати не тільки для захисту інформації в телефонних каналах, але й для захисту акустичної інформації. Складність реалізації полягає в тому, що маскувальні сигнали, як вже зазначалось вище, повинні бути змінними відносно того, як змінюється небезпечний сигнал. В цьому полягає недолік даного методу.

В [1] зазначається, що в загальному випадку лініями зв'язку при високочастотному нав'язуванні можуть служити не лише реальні низькочастотні лінії, але і паразитні лінії, утворені будь-якими іншими провідниками. Враховуючи це, підвищуються шанси перехоплення інформації у зловмисника, адже збільшується варіативність використання методу перехоплення інформації шляхом високочастотного нав'язування.

У простому випадку в якості зондуючого коливання супротивником може бути застосоване гармонічне (синусоїдальне) коливання. Аналітичне вираження таких коливань в загальному випадку має вигляд:

$$F(t) = A_0 \cos(w_0 t + \varphi_0),$$

де A_0 – амплітуда коливання,

$(w_0 t + \varphi_0)$ – фаза коливання.

При постійних значеннях параметрів A_0 і $(w_0 t + \varphi_0)$ коливання, що визначається вказаним співвідношенням, не несе ніякої смислової інформації про стан об'єкта спостереження. Якщо ж в такт з керуючим низькочастотним (НЧ) сигналом (небезпечним сигналом) змінюватимуться основні параметри цього коливання, то результуюче коливання може бути представлене у вигляді:

$$F(t) = A(t) \cos \phi(t).$$

Тобто, зондуюче коливання в цьому випадку характеризуватиметься двома основними величинами, що змінюються в часі: амплітудою $A(t)$ і фазовим кутом $\phi(t)$. Процес, який полягає в тому, що параметри зондуючого коливання змінюються в часі згідно з оброблюваними в ОТЗС сигналами низької частоти (небезпечними сигналами), є процесом небажаної (паразитної) модуляції. В даній статті рекомендується застосування комплексного підходу до захисту інформації, а саме: розробка спеціальних вимог і рекомендацій для розробників апаратури ОТЗС і ДТЗС, використання пасивних і активних засобів захисту інформації, виконання вимог по екрануванню, фільтрації і розв'язках в широкому діапазоні частот (від 10 кГц до 30 МГц і більше). Ці методи суттєво зменшують ймовірність витоку інформації, але також не унеможливлюють даний процес. Серед питань, які також потрібно розглядати при такому комплексному підході, на нашу думку, є розробка і впровадження методів щодо швидкого виявлення небезпечного сигналу. Це дозволить швидше зреагувати та не допустити витік інформації.

Підсумовуючи аналіз вищезгаданих статей, робимо висновок, що наявна в них інформації переважно описує конкретно певний метод захисту інформації від витоку каналами високочастотного нав'язування. Загальним недоліком всіх методів, на нашу думку, є неможливість швидкого аналізу зміни спектру частот, що свою чергу може призвести до витоку інформації. Також мало уваги приділено параметрам небезпечного сигналу, від зміни яких може якісно відрізнятись можливість зловмисника отримати доступ до інформації.

Отже, огляд методів захисту інформації від витоку каналами високочастотного нав'язування дає нам чітке розуміння та систематизацію основних переваг та недоліків як загальних, так і окремо взятих методів та дозволяє сформувати мету подальшого дослідження,

яке буде висвітлено у наступних статтях, а саме удосконалення наявних методів захисту інформації від перехоплення методом високочастотного нав'язування.

Результати дослідження.

На сьогоднішній день в основному пропонуються наступні методи щодо захисту інформації від витоку шляхом високочастотного нав'язування:

1. Створення контрольованої зони не меншої за Зону 2, яка розраховується з врахуванням небезпечного сигналу на кратних гармоніках підсилювачів, організації режиму доступу до контрольованої зони.

2. Екранування ОТЗС, унеможливлення «паразитної» високочастотної генерації підсилювачів ОТЗС (локального екранування підсилювачів, оцінювання випромінювань та блокування роботи ОТЗС у разі виявлення «паразитної» модуляції, оцінювання, індикації та сигналізації відхилення параметрів підсилювачів та блокування роботи ОТЗС при виявленні позитивного зворотного зв'язку тощо).

3. Просторового електромагнітного зашумлення на об'єкті [13].

Результати, отримані в ході аналітичного огляду публікацій, свідчать про те, що методи захисту інформації не забезпечують повноцінної безпеки інформації, тому мають підлягати удосконаленню. Пропонується використання наявних методів, але з урахуванням особливостей параметрів небезпечного сигналу та сигналу, який повинен руйнувати його, дослідження поведінки вищезгаданих сигналів при зміні їх параметрів з метою виявлення оптимальних. Дослідження можливості швидкого реагування на зміну в оточуючому середовищі, тим самим попереджуючи перехоплення інформації.

Обговорення результатів проведеного дослідження.

Огляд наявної інформації дозволив систематизувати знання та загальновідомі дані про методи захисту інформації від високочастотного нав'язування. Наступним етапом буде математичне та експериментальне дослідження методів захисту інформації з метою знаходження можливості удосконалення.

Пріоритетними питаннями є детальне дослідження параметрів небезпечного та захисного сигналів та можливість швидкого реагування на зміни у оточуючому середовищі. Серед труднощів слід зазначити складність практичної реалізації, потребу поглибленого та трудомісткого вивчення тематики та правильну організацію експериментального дослідження. Але, незважаючи на це, при правильному підході можна розробити програму вдосконалення наявного методу захисту інформації та забезпечити повноцінний захист від перехоплення.

Висновки. Станом на сьогодні задля захисту інформації від перехоплення каналами високочастотного нав'язування використовують активні, пасивні та комбіновані методи захисту інформації. Жоден з існуючих методів не забезпечує прийнятного рівня захисту інформації, тим самим даючи можливість зловмиснику дізнатись критично важливу інформацію. Аналітичний огляд показав, що при високочастотному нав'язуванні канали витоку інформації утворюються як в колах електроживлення та заземлення, так і в оточуючому середовищі. Це додає зловмиснику варіативності та збільшує шанси на перехоплення інформації. Водночас це зобов'язує забезпечувати комплексний підхід при побудові системи захисту інформації.

Відомі методи дозволяють забезпечувати захист інформації, але всі вони здебільшого вузькоспеціалізовані та не універсальні. Тому пріоритетним завданням є удосконалення одного з наявних методів з можливістю більш універсального застосування та для підвищення захищеності інформації. Визначено потенційні способи удосконалення методу та позначено мету наступних досліджень. Окреслено як позитивні моменти, так і ймовірні труднощі при проведенні досліджень.

REFERENCES

1. Krjuchkova L. P., Provozin O. P. (2017), «Interception of speech information by high-frequency «imposition». Modern information protection, 3(31). P. 74-80.
2. Katoryn Ju.F., Razumovskyj A.V., Spyvak A.Y. (2012), Protection of information by technical means: textbook. SPb: NYU YTMO. 416 p.
3. Jarutich A.O. (2019), «Protection of information from leakage through technical channels». Science online: International electronic scientific journal, 1.
4. Vorona V.A., Kostenko V.O. (2016), «Methods and means of protection of information from leakage through technical channels». Computational nanotechnology, 3. P. 208-223.

5. Sokolov A. N., Antjasov Y. S., Jaresjko A. P. (2015), «Protection of information in the room from leakage through technical channels. UrFO newspaper. Information security, 3(17). P. 12-16.
6. Lizunov S.I., Rozumovsjkyj K.I. (2019), «The use of shielding structures to protect information». Science Week 2019. Faculty of Radio Electronics and Telecommunications. Abstracts of reports of the scientific-practical conference. Zaporizhzhja, 15–19 kvitnja 2019 r. Redkol. V. V. Naumyk (vidpov. red.). Zaporizhzhja: ZNTU, P.112-115.
7. Baranovskyj O. K., Meljnyk A. F. (2007), «Analysis of the threat of information leakage in electrical channels of digital data transmission due to «RF imposition». EB BSU: SOCIAL SCIENCES: Informatics. Proceedings of the conferences of the Faculty of Applied Mathematics and Informatics 2005-2007. Network computer technologies. P. 181-184.
8. Ermoshyn V. V. Tkachenko V. V. (2010), «Model of high-frequency imposition signal». Scientific and technical journal «MODERN INFORMATION PROTECTION», 2. P. 68-72.
9. Khoma V.V. (2009), «Methods and means of technical protection of information on subscriber telephone lines». Automation, measurement and control. L.: Vyd-vo Nac. un-tu «Ljviv. Politekhnika», 639. P. 87-93.
10. Lenkov S.V., Rybaljsjkyj O.V., Khoroshko V.A., Krjuchkova L.P. (2009), «Principles of blocking information retrieval by HF-imposition methods». Bulletin of Taras Shevchenko National University of Kyiv. Military special sciences, 22. P. 36-39.
11. Patent 95365 Ukraine, IPC (2011.01) H04K 3/00. Method of information protection / Rybaljsjkyj O.V., Khoroshko V.O., Krjuchkova L.P., Dzhuzha O.M., Orlov Ju.Ju.; applicant and patent owner National Academy of Internal Affairs. - № a200913327; declared 22.12.2009; 55 publ. 25.07.2011, Bull. № 14.
12. Patent 103546 Ukraine, IPC (2013.01) H04K 3/00. Method of information protection / Rybaljsjkyj O.V., Khoroshko V.O., Ghryshhuk R.V.; applicant and patent owner Ghryshhuk R.V. - № a201202038; declared 22.02.2012; publ. 25.10.2013, Bull. № 20.
13. S. O. Ivanchenko, O. V. Ghavrylenko, O. A. Lypsjkyj [ta in.] (2016), Technical channels of information leakage. The order of creation of complexes of technical protection of information: the textbook of NTUU «KPI». Kyjiv: NTUU «KPI». 104 p.