КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023. 2022.18.197204
УДК 621.3

Крючкова Лариса Петрівна
доктор технічних наук, доцент, професор кафедри систем інформаційного та кібернетичного захисту
Державний університет телекомунікацій, м.Київ, Україна
ORCID ID: 0000-0002-8509-6659
alara54@ukr.net

Цмоканич Іван Володимирович
аспірант
Державний університет телекомунікацій, м. Київ,Україна
ORCID: 0000-0002-5085-8457
ivakobor@ukr.net

МЕТОДИЧНІ АСПЕКТИ ВИЗНАЧЕННЯ ПАРАМЕТРІВ ЗАХИСНИХ ВПЛИВІВ НА ЗОНДУВАЛЬНІ СИГНАЛИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

Анотація. Розглянуто процеси формування технічних каналів витоку мовленнєвої інформації методами високочастотного «нав'язування», новий метод технічного захисту інформації від перехоплення цими методами, сутність якого полягає у застосуванні комбінованої активної завади, що змінює властивості зондувального сигналу. Мета роботи — розгляд методичних аспектів визначення параметрів захисних впливів на зондувальний сигнал для забезпечення надійного блокування каналу витоку інформації. Головні завдання експериментальних досліджень — забезпечення максимального ступеню ефективності запропонованого методу технічного захисту, визначення максимального рівня цієї ефективності та визначення оптимальних параметрів захисних сигналів. Основні параметри системи захисту, що підлягають визначенню в результаті експерименту: визначення смуги частот максимально ефективного впливу для кожного виду модуляції, що використовується при перехопленні інформації, та визначення рівнів сигналів максимально ефективного впливу для кожного виду модуляції. Подано результати імітаційних досліджень, проведених для знаходження параметрів захисних сигналів, здатних забезпечити максимально можливу руйнацію інформативних параметрів небезпечного сигналу, і, як результат, створення протидії перехопленню конфіденційної інформації зацікавленими особами.

Ключові слова: захист інформації; перехоплення інформації; метод високочастотного нав'язування; зондувальний сигнал; небезпечний сигнал; завадовий захисний сигнал; параметри захисних сигналів; імітаційне моделювання; LabVIEW.

ВСТУП

Постановка проблеми. У загальній проблемі забезпечення безпеки інформації питання захисту кофіденційної інформації є одним із найважливіших. Ефективними методами перехоплення конфіденційної інформації на об'єктах інформаційної діяльності є методи високочастотного «нав'язування» (ВЧ-нав'язування, ВЧН) [1–5]. Під високочастотним «нав'язуванням» розуміється спосіб несанкціонованого отримання інформації, при якому відбувається зондування радіосигналом приміщення або його струмопровідних комунікацій, в якому відбуваються переговори. В результаті взаємодії з технічними засобами або спеціально впровадженими пристроями відбувається модуляція зондувальних сигналів мовленнєвими. Якщо в зазначених колах є елементи, параметри яких (індуктивність, ємність або опір) змінюються під дією низькочастотних сигналів, то в навколишньому просторі буде створюватися вторинне поле високочастотного випромінювання, модульованого низькочастотним сигналом.

У даний час застосовуються два способи перехоплення інформації каналами ВЧН:

– 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.

У роботі [6] авторами запропоновано новий метод технічного захисту інформації від перехоплення методами ВЧН, сутність якого полягає у застосуванні комбінованої активної завади, що змінює властивості зондувального високочастотного сигналу. В основі методу лежить відоме фізичне явище виникнення биття між коливаннями близьких частот.

Оскільки при перехопленні інформації методами ВЧН можуть виникати як амплітудна, так частотна і фазова модуляція перевипроміненого сигналу, то необхідно вжити заходів до блокування можливості одержання інформації при використанні будь-якої з цих модуляцій.

Завадою для сигналів з фазовою модуляцією буде зміна фази результуючого коливання в момент переходу його амплітуди через нуль. Але якщо такі моменти зберегти постійними (тобто вибрати постійну частоту захисного коливання), то систему перехоплення інформації можна легко адаптувати до такої завади. Тому має сенс частоту захисного коливання зробити хитною в певних невеликих межах, які забезпечують виникнення явища биття. Для цього можна хитати частоту вліво і вправо від середнього значення, наприклад, за лінійним законом. А для внесення хаотичності в процес хитання частоти, основний (задавальний) лінійний керуючий сигнал можна скласти з випадковим низькочастотним сигналом, що забезпечить захист і від частотно-модульованого, і амплітудно-модульованого перехоплення інформації.

Для остаточного зашумлення акустичної інформації, випромінюваний захисний сигнал можна скласти з іншим випадковим сигналом малого рівня (щоб зберегти основну частоту захисного гармонічного сигналу), що перекриває звуковий діапазон частот. Таким чином, в середовище, що використовується для подачі зондувального коливання, буде введена активна завада, яка перетворює сигнал ВЧ-нав'язування в сигнал, фаза, частота і амплітуда якого носять випадковий характер, і робить його непридатним для перехоплення мовленнєвої інформації. Слід зазначити, що при певному виборі середньої частоти захисного коливання і діапазону її зміни можна досягти захоплення цієї частоти генератором ВЧ-нав'язування.

Описаний спосіб захисту мовленнєвої інформації є об'єктом інтелектуальної власності (Патент України № 95365 [7]).

Мета та завдання дослідження. Мета роботи — розгляд методичних аспектів визначення параметрів захисних впливів на зондувальний сигнал для забезпечення надійного блокування каналу витоку інформації. Отримання таких експериментальних даних дозволить забезпечити практичну реалізацію запропонованого методу захисту інформації від витоку каналами ВЧН.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Головними завданнями експериментальних досліджень є забезпечення максимального ступеню ефективності запропонованого методу, визначення максимального рівня цієї ефективності та визначення оптимальних параметрів захисних сигналів.

Питання організації постановки експерименту щодо визначення вихідних параметрів запропонованої авторами системи захисту інформації від її несанкціонованого перехоплення методами ВЧ-нав'язування розглянуто в [8].

Основні параметри системи захисту, що підлягають визначенню в результаті експерименту:

1. Визначення смуги частот максимально ефективного впливу для кожного виду модуляції, що використовується при перехопленні інформації;
2. Визначення рівнів сигналів максимально ефективного впливу для кожного виду модуляції.

Схема побудови експерименту залежить від вибраного критерію ступеню ефективності запропонованого методу. При цьому критерій повинен відповідати вимогам простоти проведення експерименту з використанням стандартизованих радіовимірювальних приладів і однозначності отриманих результатів.

Вважається доцільним будувати експеримент на синусоїдальних сигналах звукового діапазону частот, а в якості критерію оцінки ефективності рівня захисту, забезпечуваного системою, використовувати відношення спектрів потужностей небезпечного сигналу, виміряних у приймачі до і після впливу запропонованої завади [8].

Оскільки поставлені завдання необхідно вирішити для всіх видів модуляції, що виникають при ВЧН, пропонується застосувати метод суперпозиції для кожного з них, що забезпечить однозначність трактування отриманих результатів і достатню для подальшого проектування повноту досліджень.

Узагальнену схему проведення експериментальних досліджень подано на рис. 1 [8].

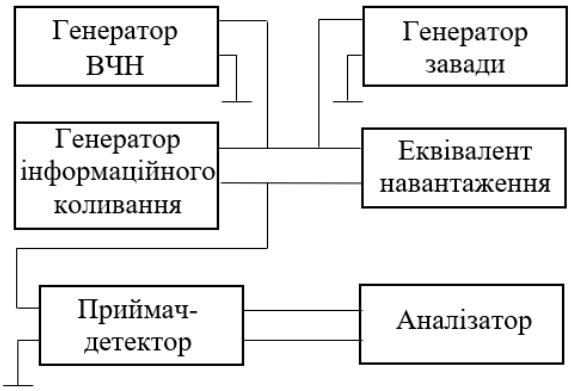

Рис. 1. Узагальнена схема проведення експериментальних досліджень

Функції генератора завади:

1. Формувати і змінювати частоту основного коливання впливу на сигнал ВЧН;
2. Змінювати діапазон управління частотою хитання і рівнем основної частоти;
3. Змінювати діапазон швидкості хитання основної частоти;
4. Формувати і змінювати параметри шумових сигналів;
5. Змінювати загальний рівень сигналу завади;
6. Здійснювати ці зміни незалежно одне від одного;
7. Використовувати кожний з видів зміни сигналу завади при відключенні решти факторів впливу.

Для вимірювання параметрів зондуючого сигналу і сигналу завади можуть бути використані стандартні осцилограф, частотомір і вольтметр (на схемі ці прилади не показано).

Еквівалент навантаження повинен забезпечувати три різні види модуляції зондуючого коливання небезпечними сигналами.

ISSN 2663 - 4023

Основні вимоги до еквіваленту навантаження:

1. Забезпечення можливості перетворення небезпечного сигналу в АМ, ЧМ та ФМ незалежно один від одного;
2. Забезпечення можливості регулювання рівня глибини модуляції для кожного з її видів.

Очевидно, що найбільш прийнятним шляхом реалізації такого пристрою буде створення трьох окремих перетворювачів, що забезпечить простоту проведення експерименту.

Такі ж вимоги та методи побудови слід віднести і до побудови схем приймачів-детекторів.

Враховуючи, що перехоплення інформації може здійснюватись як на основній частоті, так і на гармоніках небезпечного сигналу, формування захисних сигналів слід здійснювати не тільки відносно основної частоти, а й відносно гармонік небезпечного сигналу [9]. Таким чином, явища «биття» і «качання» небезпечних сигналів буде прослідковуватись і на основній частоті, і на гармоніках, що унеможливить перехоплення інформації.

Нами проведено імітаційні дослідження для всіх видів модуляції з використанням пакету LabVIEW версії 20.0.1. [10]. Дослідження проводились за робочими блок-схемами, що складаються з трьох основних частин: група генераторів, що в сумі сигналів генерують небезпечний сигнал (відмічена позначкою 1); група генераторів, що в сумі сигналів генерують захисний сигнал (відмічена позначкою 2); група контрольних пристроїв для спостереження за сигналами (відмічена позначкою 3).

Блок-схему дослідження впливу захисних сигналів на небезпечні сигнали з амплітудною та кутовою модуляціями подано на рис. 2.

Фрагмент результатів моделювання сигналів наведено на рис. 3.

Беручи до уваги дані, отримані в результаті дослідження, а саме зображення результуючого сигналу (рис. 3. d), можна зробити висновок, про ефективне руйнування інформаційної складової небезпечного сигналу з частотною модуляцією.

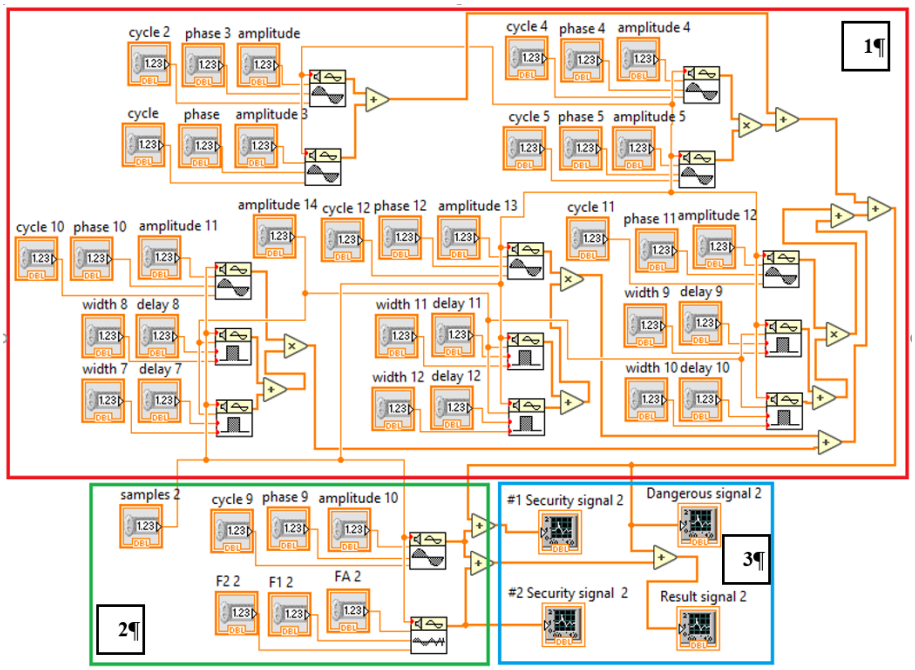

Рис. 2 Блок-схема дослідження впливу захисних сигналів на небезпечні сигнали з амплітудною та кутовою модуляціями

ISSN 2663 - 4023

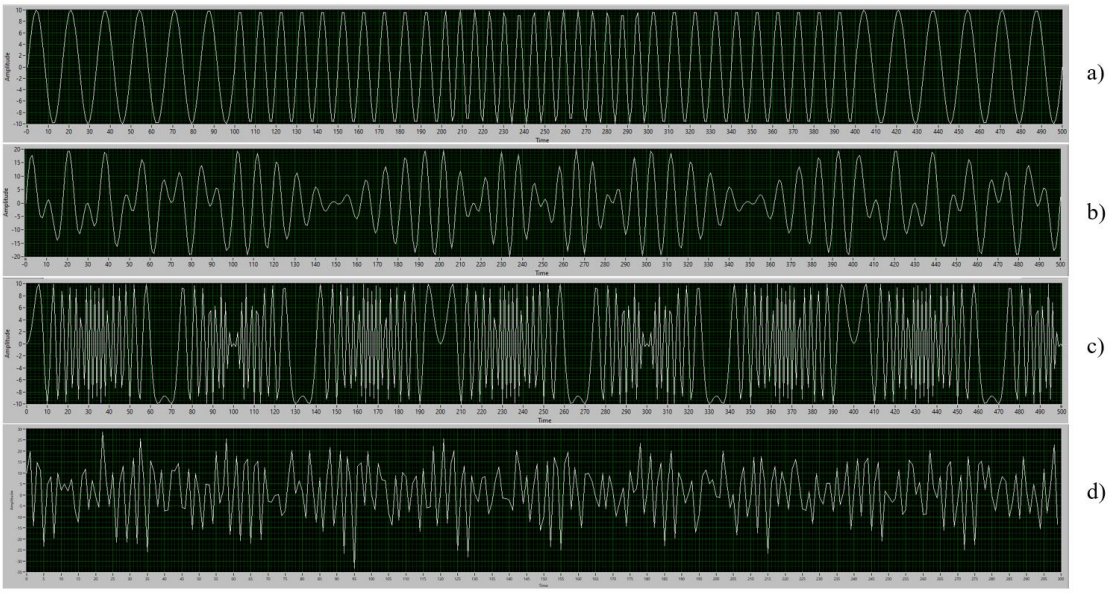

Рис. 3. Зображення сигналів дослідження впливу захисних сигналів на частотно-модульований небезпечний сигнал. (a — зображення небезпечного сигналу з частотною модуляцією, b — зображення результуючої небезпечного сигналу та першого захисного сигналу, c — зображення другого захисного сигналу, d — зображення результуючого сигналу)

ВИСНОВКИ

Визначено загальні завдання і методика проведення експериментального дослідження, необхідного для розробки технічного завдання на проектування нової системи захисту інформації від високочастотного «нав'язування».

Доцільно будувати експеримент на синусоїдальних сигналах звукового діапазону частот, а в якості критерію оцінки ефективності рівня захисту, забезпечуваного системою, використовувати відношення спектрів потужностей небезпечного сигналу, виміряних в приймачі до і після впливу запропонованої завади.

Оскільки поставлені завдання необхідно вирішити для всіх видів модуляції, що виникають при високочастотному «нав'язуванні», пропонується застосувати метод суперпозиції для кожного з них, що забезпечить однозначність трактування отриманих результатів і достатню для подальшого проектування повноту досліджень.

Формування захисних сигналів слід здійснювати не тільки відносно основної частоти, а й відносно гармонік небезпечного сигналу. Таким чином, явища «биття» і «качання» небезпечних сигналів буде прослідковуватись і на основній частоті, і на гармоніках, що унеможливить перехоплення інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Каторин Ю., Куренков Е., Лысов А., Остапенко А. (2000). *Большая энциклопедия промышленного шпионажа*. ООО «Издательство Полигон».
2. Ленков С., Перегудов Д., Хорошко В. (2008). *Методы и средства защиты информации. Том 1. Несанкционированное получение информации*. Арий.
3. Ленков С., Перегудов Д., Хорошко В. (2008). *Методы и средства защиты информации. Том 2. Информационная безопасность*. Арий.

4. Провозін О., Железняк В., Хорошко В. (2015). Особливості захисту інформації від витоку по каналу, створеному за рахунок застосування методу високочастотного «нав'язування». *Сучасні інформаційно-телекомунікаційні технології: Матеріали міжнародної науково-технічної конференції, Том IV. Сучасні технології інформаційної безпеки*, 28–30.
5. Крючкова Л., Провозін О. (2017) Перехоплення мовленнєвої інформації методами високочастотного «нав'язування». *Сучасний захист інформації*, 3(31), 74–80.
6. Ленков С., Рибальський О., Хорошко В., Крючкова Л. (2009). Принципы блокирования съема информации способами ВЧ-навязывания. *Вісник Київського національного університету ім. Тараса Шевченка. Військово-спеціальні науки*, 22, 36–39.
7. Рибальський О., Хорошко В., Крючкова Л., Джужа О., Орлов Ю. (2011) *Спосіб захисту інформації* (Патент України №95365).
8. Рибальський О., Хорошко В., Крючкова Л. (2009). Экспериментальные исследования нового метода защиты от ВЧ-навязывания. *Вісник Східноукраїнського національного університету ім. В. Даля*, 6 (136), 94–96.
9. Крючкова Л., Цмоканич І. (2021). Удосконалений метод захисту інформації від витоку каналами високочастотного нав'язування. *Збірник тез доповідей XIII Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології»*, 62–63.
10. Kriuchkova L., Vovk M., Tsmokanych I., & Tarasenko D. (2022). Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition. In: *Cybersecurity Providing in Information and Telecommunication Systems*, 3188(2), 265–272.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

Larysa Kriuchkova
doctor of Technical Sciences, docent,
professor of the Department of Information Systems and Cybernetic Protection
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-8509-6659
alara54@ukr.net

Ivan Tsmokanych
postgraduate
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0002-5085-8457
ivakobor@ukr.net

METHODOLOGICAL ASPECTS OF DETERMINING THE PARAMETERS OF PROTECTIVE EFFECTS ON PROBING SIGNALS OF HIGH-FREQUENCY IMPOSITION

Abstract. The methods of high-frequency "imposition" are effective methods of intercepting confidential information on objects of information activity. The publication examines the processes of forming technical channels for the leakage of speech information by methods of high-frequency "imposition", a new method of technical protection of information from interception by these methods, the essence of which is the application of combined active interference that changes the properties of the probing signal. The purpose of the work is to consider the methodological aspects of determining the parameters of protective effects on the sounding signal to ensure reliable blocking of the information leakage channel. Obtaining such experimental data will allow for the practical construction of the proposed systems.

The main tasks of experimental research are to ensure the maximum degree of efficiency of the proposed method of technical protection, to determine the maximum level of this efficiency and to determine the optimal parameters of protective signals. The main parameters of the protection system to be determined as a result of the experiment: determination of the frequency band of maximum effective influence for each type of modulation used in the interception of information, and determination of signal levels of maximum effective influence for each type of modulation.

It is considered appropriate to build an experiment on sinusoidal signals of the audio frequency range, and as a criterion for evaluating the effectiveness of the level of protection provided by the system, use the ratio of power spectra of the dangerous signal measured in the receiver before and after the impact of the proposed interference. Since the tasks must be solved for all types of modulation that occur during high-frequency "imposition", it is proposed to apply the superposition method for each of them, which will ensure the unambiguous interpretation of the obtained results and the completeness of research sufficient for further design.

The results of simulation studies, which were carried out to find the parameters of protective signals capable of ensuring the maximum possible destruction of the informative parameters of a dangerous signal, and, as a result, creating countermeasures against the interception of confidential information by interested parties, are presented.

Keywords: information protection; interception of information; method of high-frequency imposition; probing signal; dangerous signal; nuisance protective signal; parameters of protective signals; simulation modeling; LabVIEW.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Katorin J., Kurenkov E., Lysov A., Ostapenko A. (2000). *Great encyclopedia of industrial espionage*. Polygon Publishing House LLC.
2. Lenkov S., Peregudov D., Horoshko V. (2008). *Methods and means of information security, Volume 1. Unauthorized acquisition of information*. Arius.
3. Lenkov S., Peregudov D., Horoshko V. (2008). *Methods and means of information security, Volume 2. Information security*. Arius.

4. Porovozin O., Zheleznyak V., Horoshko V. (2015). Peculiarities of information protection against leakage through a channel created by using the high-frequency "imposition" method. *Modern information and telecommunication technologies: Materials of the international scientific and technical conference, Volume IV. Modern information security technologies*, 28–30.
5. Kriuchkova L., Porovozin O. (2017) Interception of speech information by methods of high-frequency "imposition". *Modern information protection*, 3(31), 74–80.
6. Lenkov S., Rybalskyj O., Horoshko V., Kriuchkova L. (2009). Principles of blocking information collection using HF-jamming methods. *Bulletin of Kyiv National University named after Taras Shevchenko. Military special sciences*, 22, 36–39.
7. Rybalskyj O., Horoshko V., Kriuchkova L., Dzhuzha O., Orlov J. (2011) *Method of information protection* (Patent of Ukraine №95365).
8. Rybalskyj O., Horoshko V., Kriuchkova L. (2009). Experimental studies of a new method of protection against HF-interference. *Bulletin of the Eastern Ukrainian National University named after V. Dalya*, 6 (136), 94–96.
9. Kriuchkova L., Tsmokanych I. (2021). An improved method of protecting information from leakage through channels of high-frequency imposition. *Collection of abstracts of reports of the XIII International Scientific and Practical Conference "Computer Systems and Network Technologies"*, 62–63.
10. Kriuchkova L., Vovk M., Tsmokanych I., & Tarasenko D. (2022). Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition. In: *Cybersecurity Providing in Information and Telecommunication Systems, 3188(2)*, 265–272