Застосування широкосмугових сигналів у телекомунікаційних мережах систем відеоспостереження об'єктів інформаційної діяльності

А. М. Котенко[1], А. М. Зідан[1], С. В. Бодров[1], В. В. Собчук[2]

[1]Державний Університет телекомунікацій, Київ, Україна
[2]Східноєвропейський національний університет імені Лесі Українки, Луцьк, Україна
Corresponding author. E-mail: dutkotenko@gmail.com

Paper received 22.03.19; Accepted for publication 03.03.19.

https://doi.org/10.31174/SEND-NT2019-200VII24-14

Анотація. У статті проведено порівняльний аналіз застосування широкосмугових та вузькосмугових сигналів для передачі інформації у телекомунікаційних мережах. Показано переваги по таким показникам як енергетична скритість, завадостійкість, та параметрична скритість. На підставі цього зроблено висновок про доцільність використання широкосмугових сигналів у телекомунікаційних мережах систем відеоспостереження об'єктів інформаційної діяльності.

Ключові слова: *відеоспостереження, канал витоку інформації, інформація з обмеженим доступом, широкосмуговий сигнал, об'єкт інформаційної діяльності.*

Вступ. В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України, яка часто є об'єктом зовнішньої інформаційної експансії та руйнівного інформаційного вторгнення. Вся ця безліч загроз структурується у наступні групи загроз: витоку інформації матеріально-речовим каналом, несанкціонованих дій з інформацією, знищення матеріальних носіїв інформації під впливом зовнішніх фізичних полів [1]. Безліч загроз інформаційній безпеці вимагають відповідних методів та засобів, для ефективної протидії їм. Одним із засобів ефективної протидії витоку інформації з об'єктів інформаційної діяльності матеріально-речовим каналом є системи відеоспостереження (СВС) [2], що дуже важливо для забезпечення інформаційної безпеки. На сьогодні існує безліч типів СВС, але всі вони побудовані за одною загальною схемою (рис.1).

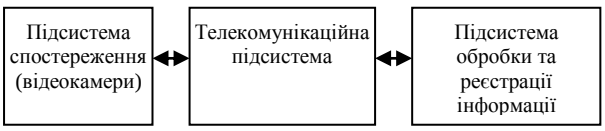

Рис. 1. Склад системи відеоспостереження

Короткий огляд публікацій. Сучасні системи відеоспостереження представляють собою програмно-апаратний комплекс призначений для запису відеоінформації та передачі її до місця перегляду чи зберігання [3]. Для цього використовують відеозапис на спеціалізовані пристрої, які можуть робити як у безперервному режимі, так і в режимі покадрового запису із заданим інтервалом часу між кадрами, з обов'язковим записом поточного часу й дати. Самою критичною ланкою СВС, яка власно й визначає основні характеристики системи у цілому, є телекомунікаційна підсистема. На сьогодні для побудови телекомунікаційних підсистем СВС використовуються два підходи. Перший (класичний) полягає у застосуванні дротового зв'язку, другий (інноваційний) базується на використанні радіозв'язку. Перевага застосування дротового зв'язку – можливість забезпечити завадозахищеність інформації, недоліки – великі монтажні витрати як часу так і грошей; у деяких випадках ускладненість самого процесу монтажу, та неестетичність. Переваги застосування радіозв'язку існуючих СВС – малі монтажні витрати, малий час розгортання СВС, естетичність, іноваційність; недоліки – низька завадозахищеність інформації під час її передачі у мережі, що є неприйнятним у питаннях інформаційної безпеки. Низька завадозахищеність обумовлена застосуванням вузькосмугових сигналів (ВСС) у телекомунікаційних підсистемах існуючих СВС, або розробник взагалі не вказує тип радіосигналу і застосування таких систем для захисту інформації на об'єктах інформаційної діяльності теж несе певний ризик. Вузькосмуговий сигнал легко розвідати, придушити, зімітувати. Таким чином аналіз існуючих підходів, що застосовуються для організації передачі інформації у телекомунікаційних підсистемах СВС показує, що вони не дозволяють у повній мірі вирішити задачу передачі інформації у системах безпеки об'єктів інформаційної діяльності. Тому, завдання щодо удосконалення методів передачі інформації у сучасних СВС є актуальним.

Мета. Обґрунтування використання для передачі інформації у телекомунікаційній підсистемі СВС широкосмугових сигналів (ШСС), як одного із можливих шляхів щодо забезпечення високої завадозахищеності передачі інформації при збереженні інших позитивних якостей застосування радіозв'язку. Для досягнення зазначеної мети необхідно зробити порівняльний аналіз використання ШСС та ВСС у телекомунікаційній мережі СВС.

Матеріали та методи. Для досягнення поставленої мети проведено аналіз науково-методичної літератури, застосовано системний підхід, теорію передачі інформації.

Результати та їх обговорення. Перше – більша енергетична скритність. Енергетична скритність передачі ШСС полягає у зменшені дальності його розвідки Rp технічними засобами спостереження противника. Відомо що дальність розвідки пропорційна кореню квадратному з потужності Pc (енергії) сигналу, що випромінюється, іншими словами $R \sim \sqrt{P_c}$. Враховуючи, що широкосмуговий сигнал можна представити як композицію *n* вузькосмугових, то при однакової енергії ШСС і ВСС, та за умовою що закон внутрішньоімпульсної модуляції (маніпуляції) ШСС є невідо-

мим противнику, відношення дальності розвідки ВСС та ШСС визначається виразом [4]:

$$\frac{R_{шсс}}{R_{всс}} = \frac{\sqrt{\frac{P_c}{n}}}{\sqrt{P_c}} = \frac{1}{\sqrt{n}} .(1)$$

Тобто, дальність розвідки ШСС є у $\sqrt{n}$ разів меншою ніж ВСС. Крім того, при досить великому n можливо забезпечити передачу сигналу з питомою щільністю енергії меншою ніж питома щільність природних шумів. В цьому випадку розвідка сигналу взагалі можлива лише за умов знання його внутрішньої структури.

Друге – параметрична скритність інформаційного обміну. Параметрична скритність інформаційного обміну ШСС забезпечується достатньо складним кодуванням сигналу його елементарними складовими [4]. Навіть при фіксації факту передачі ШСС, для виділення з нього інформації необхідно знати параметри цього кодування. Це являється дуже складною задачею, якщо врахувати, що при достатньо великій базі сигналу кількість можливих значень сигналу *k* буде визначатися за відомим виразом розрахунку кількості можливих перестановок [5]:

$$k=n^m .(2)$$

де *n* – кількість дискрет у ШСС;

m – кількість значень, які може приймати сигнал у дискреті в залежності від потужності алфавіту сигналів.

Третє – висока завадостійкість. Завадостійкість, при використанні ШСС, обумовлюється, підсиленням в n разів ШСС на виході узгодженого приймача. У [4] наведена формула, яка пов'язує відношення сигнал/шум (q^2) на виході приймача з відношенням сигнал/шум на вході ρ^2 і базою сигналу *B*:

$$q^2 = 2B\,\rho^2 .(3)$$

де $\rho^2 = P_c/P_ш$ (P_c, $P_ш$ – потужності ШСС та завади);

$q^2 = 2E/N_ш$, *E* – енергія ШСС, $N_ш$ - спектральна щільність шуму у смузі ШСС.

Відношення сигнал-шум на виході q^2 визначає робочі характеристики прийому ШСС, а відношення ρ^2 - енергетику сигналу та шуму. Необхідна величина q^2 може бути отримана навіть якщо $\rho^2<<1$. Для цього достатньо лише вибрати ШСС з досить великою базою. Виграш по завадостійкості при використанні ШСС обумовлюється невідомим для противника законом розподілу енергії сигналу в частотній та часової областях. Відношення γ сигнал/завада у цьому випадку буде мати вигляд:

$$\gamma = \frac{\int_{t_c}\int_{f_c} E_c(f,t)dfdt}{\int_{t_c}\int_{f_c} E_з(f,t)dfdt} .(4)$$

де: E_c, $E_з$ - енергія сигналу та енергія завади відповідно;

t_c, f_c - часова та частотна області відповідно, в яких відбувається передача сигналу.

Враховуючи те, що для противника є невідомими області t_c та f_c відношення сигнал/завада за однакових умов для ШСС буде кращим ніж для ВСС.

Висновки. Підводячи підсумок проведеного дослідження, можна сказати, що існуючі телекомунікаційні підсистеми СВС не у повному обсязі задовольняють сучасним вимогам. Розв'язати протиріччя між вимогами щодо забезпечення малих монтажних витрат, малого часу розгортання СВС, естетичності та високої скритності, завадозахищеності, імітостійкості дозволяє застосування у телекомунікаційній підсистемі ШСС. Таким чином застосування ШСС у телекомунікаційної підсистемі СВС, дозволяє створити систему передачі даними яка задовольняє сучасним вимогам.

Приведені результати можуть бути використані при проектуванні та розробці телекомунікаційних підсистем СВС об'єктів інформаційної діяльності.

ЛІТЕРАТУРА

1. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
2. Котенко А.М. Запобігання витоку інформації матеріально-речовим каналом за рахунок використання систем відеоспостереження // Збірник наукових праць "Сучасний захист інформації." Державний університет телекомунікацій. Київ. Вип. 1, 2017. – С. 48 – 53.
3. Гедзберг Ю. М. Охранное телевидение. - М.: Горячая линия-Телеком, 2005. -312 с.
4. Варакин Л. Е. Системы связи шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.
5. Вентцель Е.С. Теория вероятностей. - М.: Государственное издательство физико-математической литературы, 1962.-564с.

REFERENCES

1. ND TZI 3.7-003-05 The order of work on creation of complex system of information security in the information and telecommunication system.
2. Kotenko A.M. Prevention of information leakage through the material channel through the use of video surveillance systems. // Collection of scientific works " Modern information protection." State University of Telecommunications. Kyiv. Iss. 1, 2017. – P. 48 – 53.
3. Gedzberg U. M. Security television. - M.: Hot line -Telekom, 2005. -312 p.
4. Varakin L. E. Noise-like communication systems. – M.: Radio and communication, 1985. – 384 p.
5. Ventcel E. S. Probability theory. - M.: State Publishing House of Physics and Mathematics - 1962. - 564 p.

Application of broadband signals in telecommunication networks of video surveillance systems of information activity objects

A. N. Kotenko, A. M. Zidan, S. V. Bodrov, V. V. Sobchuk

Abstract. The article provides a comparative analysis of the application of broadband and narrowband signals for the transmission of information in telecommunication networks. The advantages are shown by such indicators as energy concealment, noise immunity, and parametric concealment. Based on this, it was concluded that the use of broadband signals in telecommunication networks of video surveillance systems of information activity objects.

Keywords: *video surveillance, information leakage channel, restricted access information, broadband signal, information activity object.*