https://doi.org/10.31891/2219-9365-2025-82-47
УДК 621.396.969.1

КОРЧИНСЬКИЙ Володимир
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vladkorchin@ukr.net
СЕМЕНКО Анатолій
Європейський університет
https://orcid.org/0000-0002-7043-7801
e-mail: setel@ukr.net
ЯРОВИЙ Роман
Європейський університет
e-mail: roman.yaroviy@e-u.edu.ua
ЗАГОРУЛЬКО Олександр
Європейський університет
https://orcid.org/0009-0008-7626-3874
e-mail: ozhrlko@ukr.net

АКТУАЛЬНІСТЬ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Важливою вимогою до роботи телекомунікаційних систем є скритність та прихованість передачі інформації, що складає одну з головних задач захисту інформації. При цьому найбільш небезпечним є несанкціонований доступ до одержання даних зловмисниками, що спричиняє велику шкоду для економіки та оборони країни. Зловмисник в першу чергу намагається виявити сигнал джерела інформації. Далі здійснюється спроба розкриття інформації, навіть використовуючи методи боротьби з завадами та вірусами. При позитивних результатах зусиль зловмисник одержить сигнал, створений з використанням таймерних сигнальних конструкцій, найбільш ефективного метод забезпечення скритності передачі інформації. Завдяки перебору великої кількості параметрів таймерної сигнальної конструкції- значущих моментів модуляції, кількості створених імпульсів , кількості елементарних часових відрізків та їх взаємному використанні при всіх можливих комбінаціях. При цьому буде досягнута потенційно мінімальна ймовірність прийому дійсного сигналу, що забезпечить практично неможливе розкриття інформації.

Ключові слова: Зловмисник, скритність, прихованість, джерело інформації, таймерна сигнальна конструкція, ймовірність приймання сигналу.

KORCHYNSKYI Volodymyr
State University of Intelligent Technologies and Telecommunication
SEMENKO Anatoliy, JAROVIY Roman, ZAHORULKO Oleksandr
European University

THE RELEVANCE OF CONFIDENTIALITY OF INFORMATION TRANSMISSION IN TELECOMMUNICATION SYSTEMS

An important requirement for the operation of telecommunication systems is the secrecy and concealment of information transmission, which is one of the main tasks of information security. At the same time, the most dangerous is unauthorized access to data by intruders, which causes great damage to the country's economy and defense. The violator first tries to detect the signal of the information source. Next, an attempt is made to disclose the information, even using anti-jamming and anti-virus methods. If the efforts are successful, the attacker will receive a signal created using timer signal constructions, the most effective method of ensuring the secrecy of information transmission. Due to the search for a large number of parameters of the timer signal construction - significant modulation moments, the number of generated pulses, the number of elementary time intervals and their mutual use in all possible combinations. At the same time, the potentially minimal probability of receiving a valid signal will be achieved, which will make it virtually impossible to disclose information.

The article proposes the use of Timer Signal Constructions (TSC) as an alternative to traditional Pulse Code Modulation (PCM) to enhance the structural concealment of the information signal. A study was conducted on the probability of signal structure disclosure depending on the number of pulses, significant modulation moments, and time parameters. Analytical calculations of the number of possible TSC signal realizations were presented, and the level of their structural concealment was evaluated.

Modeling was performed to analyze the dependence of the signal disclosure probability by an adversary under varying TSC parameters, demonstrating the potential to reduce this probability to the level of 10^{-50}. The impact of interference and the potential for signal cleansing by an adversary using antivirus tools were investigated. Special attention was given to the prospects of combining TSC with wideband signals, chaotic structures, pseudo-random sequences (PRS), and encryption methods (AES, 3-DES, SNOW), which allows for a comprehensive increase in telecommunication security. The proposed approaches are recommended for use in secure communication channels, particularly in conditions requiring resistance to technical intelligence threats.

Keywords. Violator, secrecy, concealment, information source, timer signal construction, bit error probability, probability of signal reception.

Стаття надійшла до редакції / Received 16.04.2025
Прийнята до друку / Accepted 11.05.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

В епоху розвитку інформаційних технологій велику цінність являє собою інформація, що використовується в багатьох видах діяльності людства. Тому в наукових дослідженнях і прикладних сферах особлива увага приділяється розробці і використанню методів і технічних засобів захисту інформації [1].

Загроза витоку інформації може призвести до порушення конфіденційного зв'язку з втратою важливої інформації. Зловмисник намагається поцупити інформацію для вигідного продажу та спричинення шкоди конкурентам, зокрема одержання доступу для новітніх технологій і особливо даних оборонного і стратегічного економічного значення.

Багаточисельна армія досвідчених фахівців - хакерів, що опанували новітні методи і засоби інформаційних технологій, в результаті шпіонської діяльності причиняє багатомільйонні втрати в економіці та оборонній галузі.

Тому при розробці та експлуатації телекомунікаційних систем особлива увага приділяється захисту інформації-прихованості передавання інформації.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Передана до каналу зв'язку інформація піддається впливу завад, що перешкоджають ефективній діяльності системи - забезпеченні приймання сигналу з мінімальною бітовою помилкою, зокрема сигналу керування військовими об'єктами. Також інформація може бути вражена вірусами [1].

При використанні розрядно-цифрового кодування двійковим сигналом ступінь прихованості передачі інформації визначається кількістю розрядів кодуючого двійкового сигналу, що може бути недостатньою [2]. Для збільшення структурної прихованості ТКС необхідно за можливістю розширювати ансамбль використовуваних сигналів.

Тому для підвищення ступеня прихованості передачі інформації доцільно використати таймерні сигнальні конструкції [3-6] .

ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

Зазвичай використовується розрядно-цифрове кодування (РЦК) для формування та обробки сигналу[1]. При цьому інформація визначається Найквістовим імпульсом, що не викликає міжсимвольної інтерференції (міжсимвольних спотворень) імпульсних сигналів:

$$t_{\text{н}} = \frac{1}{\Delta f} \quad , \tag{1}$$

де Δf – смуга пропускання каналу (і відповідно практична ширина спектру сигналу).

При використанні РЦС кількість реалізації сигналу визначається як:

$$N = 2^m, \tag{2}$$

де m-кількість розрядів кодової комбінації.

Наприклад, при перетворенні аналогового мовного сигналу в цифровий з m=8, кількість реалізацій, що відображають рівень амплітуди N=256.[2].

Кількість розрядів кодуючого двійкового сигналу буде визначати ступінь прихованості передачі інформаційного сигналу, що може бути недостатньою для забезпечення прихованості передачі інформаційного сигналу. Тому при створенні телекомунікаційних систем(ТКС) актуально використання таймерних сигнальних конструкцій (ТСК), що забезпечує набагато більшу прихованість передачі інформаційного сигналу[3].

В ТСК інформація закладена в тривалості декількох окремих часових відрізків t_{cx} на інтервалі конструкції $T_{\text{с1}}$ при обраній кількості значущих моментів модуляції (ЗММ) i, кількості створених імпульсів n, кількості елементарних часових відрізків s та їх взаємному положенні (рис. 1):

$$t_{cx} \geq t_0 + k\Delta, (k \in 0,\ 1,\ 2, \dots). \tag{3}$$

Зазвичай приймається тривалість базового елементу побудови ТСК:

$$\Delta = \frac{t_0}{s}, \tag{4}$$

де s-кількість підряд переданих одиниць або нулів.

Тоді:

$$t_0 = s\Delta \tag{5}$$

і тривалість елементарного імпульсу буде:

$$t_{cx} \geq s\Delta + k\Delta, (k \in 0,\ 1,\ 2, \dots). \tag{6}$$

Створені елементарні імпульси повинні мати тривалості t_{cx} і роміщуватись або окремо, або «в стик» із створенням суцільного імпульсу .

Кількість ЗММ і визначається в точках зміни полярності створених імпульсів, які розміщені окремо :

$$i = n_o - 1, \tag{7}$$

де n_o – кількість окремо розміщених імпульсів.

Загальну кількість реалізацій ТСК можна визначити як кількість поєднань за формулою [2]:

$$L = \frac{u!}{i!(u-i)!}, \tag{8}$$

де

$$u = ns - i(s-1). \tag{9}$$

Число реалізацій ТСК з урахуванням значень n, s при i=2наведено в табл.1 [3].

Таблиця 1.

Залежність кількості реалізацій від параметрів ТСК

$i = 2$							
s \ n	4	5	6	7	8	9	10
2	15	28	45	66	91	120	153
3	28	55	91	136	190	253	325
4	45	91	153	231	325	435	561
5	66	136	231	351	496	666	861
6	91	190	325	496	703	946	1225
7	120	253	435	666	946	1275	1653
8	153	325	561	861	1225	1653	2145
9	190	406	703	1081	1540	2080	2701
10	231	496	861	1326	1891	2556	3321

Наявність апріорної й апостеріорної невизначеності робить задачу визначення структури сигналу ймовірнісною, тому кількісною мірою структурної прихованості ТСК може служити ймовірність приймання дійсного сигналу p_c за умови, що сигнал уже виявлений.

Величину p_c можна визначати з урахуванням максимального ансамблю реалізацій $A_{тск}$, який потрібно проаналізувати методом повного перебору для знаходження ключів n, s та i при несанкціонованому доступі:

$$p_c = 1/A_{\text{ТСК.}} \tag{10}$$

Для розрахунків потенційної структурної прихованості сигналу ТСК максимальний ансамбль всіх реалізацій $A_{\text{ТСК.}}$ необхідно проаналізувати сигнал при всіх комбінаціях параметрів :

$$A_{тск} = \sum_{n=4}^{10} \sum_{s=2}^{7} \sum_{i=2}^{5} \frac{[(n\cdot s)-[(s-1)\cdot i]]!}{i!\cdot[[(n\cdot s)-[(s-1)\cdot i]]-i]!} \tag{11}$$

На рис. 1 наведена одержана в результаті проведених розрахунків за формулами (3), (4) залежність імовірності розкриття структури ТСК p_c від кількості імпульсі n при значеннях $S = 2 \div 12$, $n = 4 \div 10$ та $i = 1 \div 6$ [4].

Очевидно, величина p_c може сягати 10^{-50}, що забезпечить практично гарантовану прихованість сигналу для несанкціонованого зловмисника.

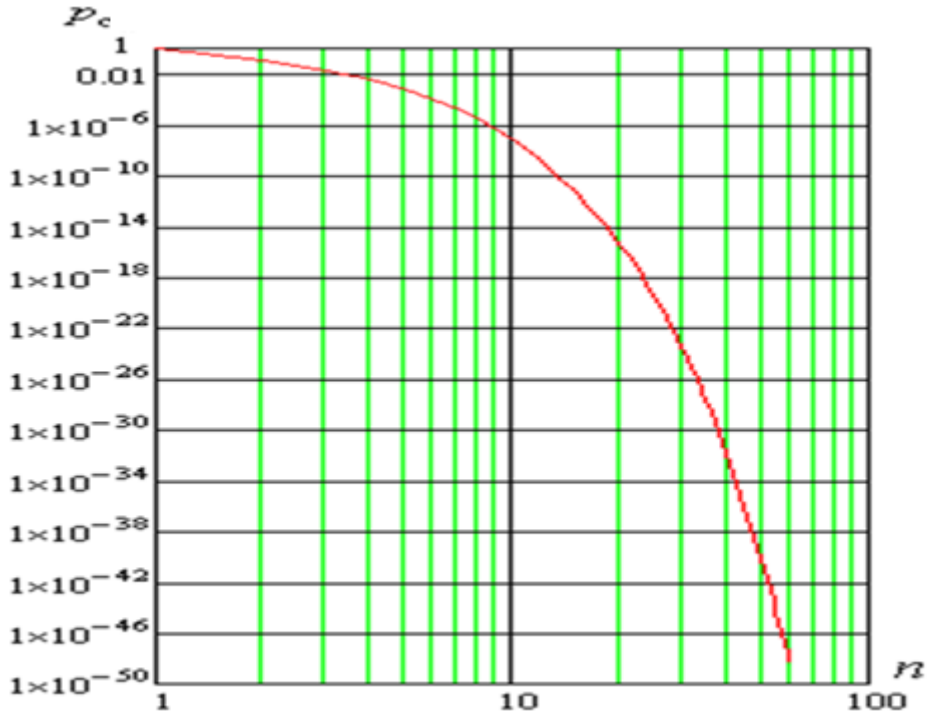

Рис1. Залежність імовірності розкриття структури ТСК p_c від кількості імпульсів *n* при значеннях S =1 ÷ 12 та i =1 ÷ 6

Для збільшення можливості розкриття інформації доцільно використати її шифрування - складного перетворення сигналу математичним методами. Найбільш поширене використання знайшли алгоритми шифрування AES, 3-DES, SNOW [5].

Реальний інформаційний сигнал може бути вражений завадами та вірусами [3,7].

Для зменшення рівня сигналу на вході розвідприймача зловмисника P_n доцільно використовувати широкосмуговий сигнал з потужністю [2] :

$$P_n = W\Delta f, \tag{12}$$

де W– щільність потужності; Δf – смуга пропускання розвідприймача.

Для підвищення прихованості передавання інформації з ТСК можна використати наступні методи [2]:

1.Спільне використання *ТСК і* ПВП - кодів, Голда, Касамі, Уолша для створення широкосмугового сигналу з базою:

$$B = T\Delta F = T/\tau >> 1, \tag{13}$$

де T – тривалість періоду сигналу;; ΔF – використовувана смуга частот; τ – тривалість елементарного імпульсу ПВП.

2.Спільне використання хаотичних сигналів та ТСК . При цьому ПВП створюються на основі хаосу за логічним, квадратичним або кубічним зображеннями.

3.Здійснення псевдовипадкової перебудови робочої частоти разом з використанням ТСК.

Зловмисник в своїй злочинній діяльності в першу чергу буде прагнути виявити надчутливим розвідприймачем сигнал від джерела інформації на максимальній відстані:

$$Д = \lambda / 4\pi \sqrt{PG_{пер.}G_{пр.}L \ / \gamma P_{пр.мін,}}, \tag{14}$$

де λ – довжина робочої хвилі; P – потужність передавача; $G_{пер.}$,$G_{пр.}$ - коефіцієнти підсилення антен передавача і приймача; L - загасання сигналу в атмосфері; γ - відношення сигнал/шум; $P_{пр.мін,}$ - чутливість приймача .

Зловмисник буде моніторити довжину хвилі сигналу та навколишній простір з відповідною вузькою діаграмою спрямованості антени.

Слід зазначити, що широкосмуговий сигнал буде сприяти скритності передачі інформації, особливо при використанні для розширення спектру сигналу псевдовипадкової послідовності (ПВП) на основі хаосу[2].

З метою підвищення рівня захищеності інформації доцільно застосовувати шифрування — складне математичне перетворення сигналу. Найбільш широке застосування отримали алгоритми AES, 3-DES і SNOW [5].

Реальний інформаційний сигнал може піддаватися впливу завад і вірусного програмного забезпечення [2,6].

Зловмисник попередньо може дешифрувати [7] та очистити сигнал від завад [2] і вірусів з використанням антивірусних програм, зокрема Dr.Web, Антивірус Касперського (AVP), AVG Free Edition, NOD32, NOD32, NORTON AntiVirus, Panda, Avira Free Antivirus [8] .

В результаті виконання вказаних вище дій зловмисник може одержати «чистий» сигнал, створений передавачем інформації з використанням ТСК, найбільш ефективних для підвищення прихованості передавання інформації [3]. Але враховуючи , що використання ТСК [9,10] забезпечить надзвичайно малу ймовірність розкриття сигналу до 10^{-50}, буде забезпечена практично гарантована неможливість одержання зловмиснику дійсного сигналу.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

1. Важливою вимогою до ТКС є забезпечення прихованості передавання інформації з метою уникнення несанкціонованого викрадення даних зловмисником.

2. Як перший крок злочинної діяльності зловмисник здійснить виявлення сигналу джерела інформації з використанням надчутливого розвідприймача шляхом моніторингу робочої частоти на навколишнього простору завдяки вузькій діаграмі спрямованості антени.

3. Зловмисник, опанувавши новітні досягнення інформаційних технологій, буде намагатись звільнити сигнал від попереднього пошкодження завадами та вірусами .

4. Завдяки виконаним вказаним попереднім заходам зловмисник може одержати «очищений» інформаційний сигнал і буде шляхом перебору великої кількості реалізацій ТСК намагатись розкрити інформацію, однак завдяки надзвичайно низькій ймовірності приймання реального сигналу йому досягнути позитивного результату буде практично неможливо.

5. Для забезпечення максимальної прихованості приймання сигналу доцільно використовувати таймерні сигнальні конструкції з параметрами : i =2, n=3, $s\leq 7$.

Перспективи подальших досліджень у даному напрямі забезпечення прихованості передавання інформації в ТКС передбачають розробку адаптивних таймерних сигнальних конструкцій з можливістю динамічної зміни параметрів у реальному часі, моделювання дій зловмисника з використанням машинного навчання, інтеграцію псевдовипадкових комутацій із частотним та фазовим перестроюванням сигналу, а також застосування когнітивного радіо для вибору малодоступних частот. Доцільно також дослідити використання квантових методів генерації ключів, створення математичних моделей ефективності захисту при різних типах атак, оптимізацію співвідношення між складністю сигнальної структури та енергоспоживанням, а також аналіз стійкості систем у розподілених середовищах зв'язку з можливістю синхронного моніторингу зловмисником.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах, Закон України № 80/94-ВР (1994) (Україна). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

2. Семенко, А., Бойко, Ю., Шпур, О., Стрелковська, І., Корчинський, В. & Яровий, Р. (2024). *Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія* (А. Семенко, Ред.). Європейський університет, Аграр Медіа Прінт. https://elar.khmnu.edu.ua/handle/123456789/17381.

3. Захарченко, М. (2009). *Системи передавання даних. Т. 1. Завадостійке кодування*. Фенікс.

4. Zakharchenko, N., Korchinskii, V., & Radzimovskii, B. (2011). Otsenka informatsionnoi skritnosti taimernikh signalnikh konstruktsii v sistemakh peredachi konfidentsialnoi informatsii. Zbirnik naukovikh prats ONAZ im.O.S.Popova, (1), 3–8.

5. *Шифрування*. (2023). https://www.kingston.com/ua/blog/data-security/what-is-encryption

6. *Віруси для ПК*. (2023). https://most-it.com.ua/top-10-najbilsh-rujnivnih-virusiv-chastina-persha-vid-mileniumu-do-2010-roku-a-120.html?srsltid=AfmBOoq6Raimvsgl

7. *Антивірусні програми*. (б. д.). https://www.itbox.ua/ua/blog/Naykraschi-bezkoshtovni-antivirusi-dlya-Windows-aktualni-u-2024-roci/?srsltid=AfmBOooEd8KZib-XTJf2IoUcUne79Jn00iNvMXKi7jKOyaH3PgGEfOVu

8. *Дешифрування*. (б. д.). https://elearn.nubip.edu.ua/pluginfile.php/190202/mod_assign/intro/Теоретичні%20положення.pdf

9. Семенко, А., Бойко, Ю., & Шпур, О. (2024). Комплексна оптимізація телекомунікаційної системи на основі модифікованої ПВП голда і RAKE-приймачів. *Measuring and computing devices in technological processes*, (3), 156–165. https://doi.org/10.31891/2219-9365-2024-79-20.

10. Бойко, Ю. М. (2015). Підвищення завадостійкості блоків оброблення сигналів супутникових засобів телекомунікацій на основі модифікованих схем синхронізації. *Вісник Національного технічного університету України Київський політехнічний інститут. Серія: Радіотехніка. Радіоапаратобудування*, (61), 91-107. https://doi.org/10.20535/RADAP.2015.61.91-107.

References

1. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh, Zakon Ukrainy № 80/94-VR (1994) (Ukraina). [Electronic resource]. – 1994. - Access mode: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
2. Semenko, A. I., Boiko, J. M., *et al*. (2024). Suchasni tekhnolohii infokomunikatsiinykh ta kompiuternykh merezh: Monohrafiia (A. I. Semenko, Red.). European University, Ahrar Media Print, 557 s. https://elar.khmnu.edu.ua/handle/123456789/17381.
3. Zakharchenko, M. (2009). Systemy peredavannia danykh. T. 1. Zavadostiike koduvannia. Feniks.
4. Zakharchenko, N., Korchinskii, V., & Radzimovskii, B. (2011). Otsenka informatsionnoi skritnosti taimernikh signalnikh konstruktsii v sistemakh peredachi konfidentsialnoi informatsii. Zbirnik naukovikh prats ONAZ im.O.S.Popova, *(1)*, 3–8.
5. Shyfruvannia. (2023). [Electronic resource]. – 2023. - Access mode: https://www.kingston.com/ua/blog/data-security/what-is-encryption
6. Virusy dlia PK. (2023). [Electronic resource]. – 2023. - Access mode: https://most-it.com.ua/top-10-najbilsh-rujnivnih-virusiv-chastina-persha-vid-mileniumu-do-2010-roku-a-120.html?srsltid=AfmBOoq6Raimvsgl
7. Antyvirusni prohramy. (b. d.). [Electronic resource]. – 2024. - Access mode:https://www.itbox.ua/ua/blog/Naykraschi-bezkoshtovni-antivirusi-dlya-Windows-aktualni-u-2024-roci/?srsltid=AfmBOooEd8KZib-XTJf2IoUcUne79Jn00iNvMXKi7jKOyaH3PgGEfOVu
8. Deshyfruvannia. (b. d.). [Electronic resource]. – 2024. - Access mode: https://elearn.nubip.edu.ua/pluginfile.php/190202/mod_assign/intro/Теоретичні%20положення.pdf
9. Semenko A., Boiko J., & Shpur O. (2024). Comprehensive optimization of telecommunication system based on modified PRS gold and RAKE receivers. *Measuring and computing devices in technological processes*, *(3)*, 156–165. https://doi.org/10.31891/2219-9365-2024-79-20.
10. Boiko, J. M. (2015). Increasing the noise immunity of signal processing units of telecommunications on the basis of the modified synchronization schemes. *Visnyk NTUU KPI Seriia-Radiotekhnika Radioaparatobuduvannia*, *61*, 91-107. https://doi.org/10.20535/RADAP.2015.61.91-107