https://doi.org/10.31891/2219-9365-2025-82-25
УДК 004.056

КОРЧИНСЬКИЙ Володимир
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
РЯБУХА Олександр
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0001-7402-0395
e-mail: ryabukha@gmail.com
СТЕПАНОВ Вадим
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0001-0851-4220
e-mail: stepanovvadym333@gmail.com
ГОЛЕВ Денис
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-2899-4436
e-mail: d.v_holev@suitt.edu.ua
ЛІМАРЬ Ігор
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-8972-9935
e-mail: quantum.biology@outlook.com

ПРИСТРІЙ ЗАХИСТУ МОВНОГО АКУСТИЧНОГО СИГНАЛУ В УМОВАХ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

У статті розглядається проблема захисту мовної інформації, що передається по каналу зв'язку в умовах сучасних загроз, зокрема, перехоплення повідомлень, несанкціонованого доступу та аналізу акустичних сигналів. Запропоновано додатковий пристрій для радіостанції, який забезпечує підвищений рівень захисту мовного сигналу за рахунок його цифрового перетворення, шифрування та модифікації акустичних характеристик. Основний принцип роботи пристрою полягає у перетворенні акустичного сигналу в цифровий за допомогою аналого-цифрового перетворювача, подальшого шифрування та вставлення синхронізуючих сигналів у мовний потік. Це дозволяє забезпечити точне та коректне відновлення інформації в приймачі. Після обробки цифровий сигнал знову перетворюється в аналоговий та подається на телефонний капсуль, який активізує мікрофон радіостанції для організації сеансу передачі по радіоканалу. В умовах радіоелектронної боротьби запропонований пристрій надає додатковий захист інформації завдяки ускладненню процесу аналізу мовного сигналу у випадку його перехоплення через канал зв'язку. Наявність у цифровому потоку послідовності синхронізації дозволить зменшити вплив завад та забезпечити коректне поновлення мовного сигналу в приймачі. Надано аналіз і доведена доцільність використання кодів Баркера в якості сигналів циклової синхронізації. Розроблені структурні схеми пристроїв перетворення мовного сигналу. Метою роботи є розробка та аналіз принципу роботи додаткового пристрою для радіостанції, який забезпечує підвищений рівень захисту мовного сигналу шляхом його цифрового перетворення, шифрування та використання синхронізуючих сигналів для коректного прийому та відновлення інформації.

Ключові слова: захист мовної інформації, акустичний сигнал, радіостанція, шифрування, аналого-цифрове перетворення, синхронізація, радіоелектронна боротьба, несанкціонований доступ, перехоплення сигналу, цифрова обробка сигналів.

KORCHYNSKYI Volodymyr, RIABUKHA Oleksandr, STEPANOV Vadim,
HOLEV Denys, LIMAR Ihor
State University of Intellectual Technologies and Communications

DEVICE OF SPEECH ACOUSTIC SIGNAL PROTECTION IN THE CONDITIONS OF RADIO ELECTRONIC WARFARE

The article considers the issue of speech information, which is transmitted over the communication channel in the conditions of modern threats, particularly signal interception, unauthorized access and analysis of acoustic signals. An additional device for radio stations is proposed, which provides an increased level of speech signal protection due to its digital conversion, encryption and modification of acoustic characteristics. The basic principle of operation of the device is to convert the acoustic signal into digital using the analog-to-digital converter, further encryption and insertion of synchronizing signals into the speech stream. It allows to ensure exact and correct information recovery in the receiver. After processing, the digital signal is converted back into analog and fed to the telephone capsule, which affects the radio station microphone, ensuring the transmission of a protected speech signal over the radio channel. In the conditions of electronic warfare, the proposed device provides high efficiency due to the complexity of the process of analyzing the speech signal in the event of its interception through the communication channel. The presence of synchronization signals in the digital stream will allow to reduce the influence of interference and ensure correct renovation of the speech signal in the receiver. The analysis is given and the expediency of using Barker codes as cyclic synchronization signals is proven. Structural schemes of speech signal conversion devices are developed. The purpose of the work is to develop and analyse an additional device for radio station that provides increased level of speech signal protection by digital conversion, encryption, and the use of synchronization signals for correct reception and recovery of information.

Keywords: protection of speech information, acoustic signal, radio station, encryption, analog-to-digital conversion, synchronization, electronic warfare, unauthorized access, signal interception, digital signal processing.

Стаття надійшла до редакції / Received 11.04.2025
Прийнята до друку / Accepted 03.05.2025

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

У сучасних умовах військові та спеціальні підрозділи широко використовують радіозв'язок для оперативної координації дій [1]. Проте в умовах радіоелектронної боротьби (РЕБ) передача мовної інформації через радіостанції зазнає значних загроз [1, 2]. Основними з них є: глушіння або перехоплення сигналу; несанкціонований доступ (НСД) до повідомлень. У випадку перехоплення радіосигналу засобами радіоелектронної розвідки (РЕР) противник може отримати НСД доступ до мовного повідомлення шляхом прослуховування
радіоканалу [3]. Перехоплення сеансу радіозв'язку дає можливість модифікації або підміни переданих даних для дезінформації. Глушіння передаваного радіосигналу засобами РЕБ призводить до блокування процесу передання сигналів за допомогою потужних радіозавад. При аналізі акустичних сигналів використовуються методи спектрального аналізу для розпізнавання мовного повідомлення або відновлення його вмісту [1]. Слід відзначити, що традиційні методи криптографічного захисту, такі як шифрування даних, не завжди можуть бути застосовані через технічні обмеження апаратної бази мобільних радіостанцій та необхідність швидкої обробки сигналу. Також, запропонований метод перетворення мовного сигналу може бути додатковим засобом захисту інформації навіть при наявності шифрування даних у радіостанції.

В умовах активного використання засобів РЕБ застосування лише стандартних засобів шифрування часто є недостатнім. Сучасні методи захисту інформації в умовах РЕБ повинні відповідати таким вимогам: стійкість передаваного сигналу до перехоплення та захист його від аналізу сигналу; стійкість до глушіння. Стійкість до перехоплення передбачає забезпечення перетворення сигналу таким чином, щоб його було складно виявити, розпізнати або відновити. Це можливо шляхом розширення спектра сигналу та зменшення його амплітудних складових, що забезпечує так звану енергетичну прихованість сигнальних конструкцій. Оцінити умови забезпечення цього показника можливо за допомогою теореми Шеннона про пропускну спроможність каналу [4]:

$$C = \Delta F \log_2 \left(1 + \frac{P_{\text{с}}}{P_{\text{ш}}}\right) \tag{1}$$

де ΔF – смуга частот, яка призначена для передавання даних; $P_{\text{с}}$ – потужність сигналу на виході передавача; $P_{\text{ш}}$ – потужність завади в каналі. З (1) можна зробити висновок, що забезпечити енергетичну прихованість можливо за умови, що [4]:

$$\begin{cases} B_{\text{ш}} = T\Delta F \to \infty \\ P_{\text{с}}/P_{\text{ш}} \to 1 \end{cases} \tag{2}$$

За умови, що

$$P_{\text{с}}/P_{\text{ш}} < 1 \tag{3}$$

амплітуда передаваних сигналів буде менше шуму Гауса, що дасть змогу реалізації максимального рівня енергетичної прихованості сигнальних конструкцій [4]. Вочевидь, що умови (2) і (3) будуть мати силу у випадку забезпечення необхідної завадостійкості та швидкості передавання даних.

Захист від аналізу структури сигналу можливо за допомогою використання більш складних сигнально-кодових конструкцій (СКК). Прикладом таких СКК є хаотичні сигнали [9]. Стійкість до глушіння передбачає забезпечення можливості відновлення інформації навіть при наявності радіозавад, що можливо при розширенні спектра початкового вузькосмугового сигналу. Прикладом такого метода передавання сигналів є псевдовипадковий перескок робочої частоти (ППРЧ) [4]. Такий сигнал складніше заглушити в силу постійної зміни несущої частоти та вимагає використання широкосмугової завади стацією РЕБ противника. Цей метод розширення спектра лише частково задовольняє (1), тому що амплітуда сигналу не зменшується, а збільшується лише смуга частот передаваного сигналу. Також слід відзначити, що метод передавання ППРЧ в сучасних умовах радіоелектронного конфлікту виявляється SDR засобами спектрального аналізу радіочастотного спектра. Це суттєво спрощує визначення займаної смуги частот та дає противнику встановлювати відповідну широкосмугову заваду.

Запропонований у статті підхід передбачає використання додаткового пристрою, який інтегрується з радіостанцією та здійснює:

1) перетворення мовного сигналу в цифровий формат за допомогою аналого-цифрового перетворювача (АЦП);

2) шифрування сигналу відповідно до заданого алгоритму;

3) додавання до мовного сигналу синхронізуючих сигналів у паузах мовлення;

4) поновлення акустичного сигналу за допомогою цифро-аналогового перетворювача (ЦАП) для передачі його через мікрофон радіостанції.

На приймальній стороні здійснюється прийом акустичного сигналу, перетворення його в цифровий сигнал, розшифрування та відновлення мовного повідомлення. Використання такого методу ускладнює несанкціоноване прослуховування та аналіз структури сигналу, що значно підвищує рівень захищеності мовної інформації. У статті розглядається функціональна схема запропонованого пристрою, принципи його роботи, а також переваги використання в умовах можливого радіоелектронного придушення. Компактність і швидкодія додаткового пристрою захисту інформації передбачає можливість його інтеграції в існуючу систему зв'язку без значного ускладнення її роботи. Також, можливий варіант розробки додаткового пристрою захисту мовного сигналу, якій використовує гарнітуру радіостанції.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є розробка та аналіз принципу роботи додаткового пристрою для радіостанції, який забезпечує підвищений рівень захисту мовного сигналу шляхом його цифрового перетворення, шифрування та використання синхронізуючих сигналів для точного прийому та відновлення інформації.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Захист мовної інформації є одним із ключових напрямів у сфері інформаційної безпеки, особливо в умовах РЕБ [1]. Багато наукових досліджень присвячено методам забезпечення конфіденційності передаваних даних, зокрема через криптографічні та сигнальні технології [5, 6]. Різні дослідження висвітлюють заходи забезпечення безпеки мовного зв'язку, серед яких можна визначити: криптографічні методи [7, 8]; методи маскування сигналу. Найчастіше, для захисту мовних сигналів використовуються методи шифрування (AES, DES, RSA, потокові шифри) [8], що потребують потужних обчислювальних ресурсів. Методи маскування передавання орієнтовані на змішування кількох сигнально-кодових конструкцій, наприклад, мовного і шумового сигналу та інше. [9]. Такі підходи ефективні проти НСД, але можуть впливати на якість переданого сигналу.

Для забезпечення стабільної роботи системи зв'язку важливим є забезпечення її надійною системою синхронізації, яка відіграє важливу роль у цифровій обробці сигналів. У науковій праці [8] розглядається застосування синхросигналів для точного прийому та розшифрування мовних повідомлень, що особливо актуально при наявності завад та глушіння радіосигналів.

Захисту інформації в умовах РЕБ присвячено достатньо велика кількість публікацій, які зосереджені на підвищенні завадозахищеності радіозв'язку [9]. Завадозахищеність розглядає такі важливі питання як забезпечення прихованості та завадостійкості систем радіозв'язку. Для виконання таких завдань розглядається наступне:

– адаптивна фільтрація сигналів в приймачі для зменшення або усунення завад [8];

– хаотичні сигнали для ускладнення перехоплення мовних повідомлень [9, 10];

– розширення спектра інформаційного сигналу [4, 8];

– використання завадостійких кодів та систем шифрування [5, 7].

Отже, наявні дослідження підтверджують ефективність шифрування та методів маскування сигналу, однак проблема захисту мовної інформації в умовах РЕБ залишається актуальною. Запропонований у статті підхід поєднує цифрове перетворення мовного сигналу, його шифрування та використання синхронізуючих сигналів, що дозволяє покращити стійкість до перехоплення та аналізу.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Передача мовної інформації по радіоканалу завжди супроводжується ризиком її перехоплення та несанкціонованого доступу [1]. Умови РЕБ передбачають активне використання засобів радіоперехоплення, аналізу та глушіння сигналів. Отже, ефективний захист мовної інформації потребує комплексного підходу, що включає різні методи маскування, шифрування та синхронізації переданих даних [9]. У випадку радіоперехоплення передаваного сигналу є можливість запису його на носій інформації безпосередньо з радіоканалу за допомогою спеціальних приймачів. Після цього відбувається аналіз спектра сигналу і виділення мовних складових частот, що дає можливість відновити вміст повідомлень. В різних радіостанціях, як правило, для захисту інформації можуть використовувати системи шифрування, криптографічна стійкість яких залежить від довжини використовуваного ключа. Також слід відзначити, що деякі засоби зв'язку не мають необхідних вбудованих механізмів захисту інформації від НСД або методів розширення спектра

сигналів, які зменшують ймовірність виявлення та перехоплення передаваних повідомлень. Отже, в цьому випадку для таких засобів зв'язку доцільним є використання додаткових засобів захисту мовної інформації.

Запропонований пристрій є додатковим модулем для радіостанції, призначеним для захисту мовного сигналу від перехоплення в умовах РЕБ. На рис. 1 надана структурна схема пристрою перетворення мовного сигналу в передатчику, який складається з мікрофону (М), блоку попереднього підсилювача (П1), блоків АЦП та ЦАП, блоку шифрування (Ш), блоку сполучення цифрового мовного сигналу (СМС) з сигналами синхронізації, блоку формування сигналів синхронізації (ФСС), блоку підсилювача сигналу (П2) та телефонного капсуля (ТК).

Мікрофон забезпечує перетворення акустичного сигналу в змінний струм в ланцюгу підсилювача П1. За допомогою АЦП формується цифровий сигнал, який подається на пристрій шифрування. Далі зашифрований сигнал потрапляє на вхід блоку СМС, в якому в проміжках цифрового потоку вставляються кодові послідовності синхронізації, що поступають з пристрою ФСС. Сформований таким чином сигнал потрапляє на ЦАП для перетворення його в аналоговий сигнал, який через підсилювач П2 потрапляє на телефонний капсуль ТК. Слід зазначити, що блок ТК пристрою повинен щільно прилягати до тієї частини радіостанції, де знаходиться мікрофон. Для цього необхідно використовувати спеціальні кріплення на основі гумової прокладки з отворами для створення акустичного каналу між ТК та мікрофоном радіостанції. Це дозволить усунути місцевий ефект, коли частина акустичного сигналу через ТК може потрапляти на мікрофонний капсуль пристрою. Сформований таким чином акустичний сигнал поступає через мікрофон радіостанції по каналу.

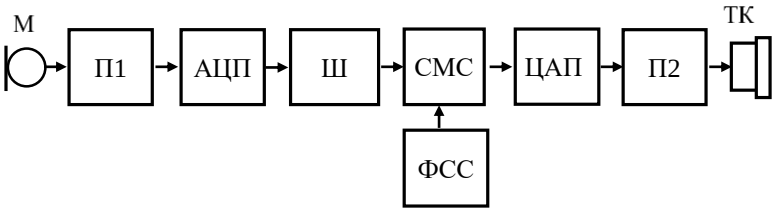

Рис. 1. Структурна схема пристрою перетворення мовного сигналу в передатчику

На рис. 2 надано структурну схему пристрою перетворення акустичного сигналу в приймачі. Акустичний сигнал з ТК радіостанції не може бути розпізнаним без додаткового перетворення.

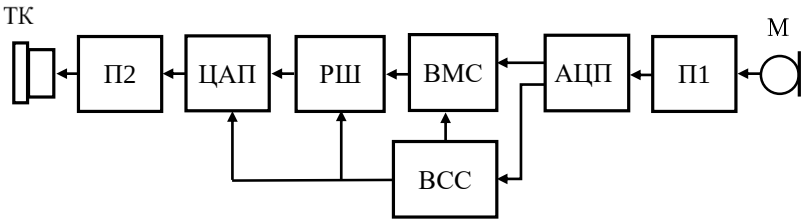

Рис. 2. Структурна схема пристрою перетворення мовного сигналу в приймачі

З виходу мікрофону електричний сигнал після підсилювання блоком П1 поступає на АЦП, з виходу якого цифровий потік подається на блок ВСС (виділення сигналів синхронізації). Блок ВСС формує цифровий потік сигналів синхронізації, за допомогою яких забезпечується узгоджена робота блоків ВМС (виділення мовних сигналів), РШ (розшифрування) та ЦАП. Блок ВМС забезпечує виділення тільки мовних цифрових сигналів за допомогою тактових імпульсів і циклових комбінацій, що надходять з блоку ВСС. По цикловим комбінаціям визначається початок і кінець фрагментів мовного цифрового сигналу. Блок РШ забезпечує перетворення закритого мовного цифрового потоку у відкритий. Далі цей цифровий потік подається на ЦАП. З виходу ЦАП сигнал потрапляє на підсилювач П2, а потім на ТК.

Потрібно відзначити, що мікрофонний капсуль повинен щільно прилягати через гумову прокладку з отворами до місця розташування акустичного каналу телефонного капсулю радіостанції. При реалізації даного пристрою важливим є забезпечення стабільної роботи системи тактової та циклової синхронізації, а також вирішення вибору розрядності блоків АЦП та ЦАП. Для забезпечення точного прийому та розшифрування сигналу в мовний потік вбудовуються спеціальні циклові сигнали синхронізації, що дає можливість визначати інтервали часу для відновлення послідовності. Для сигналів циклової синхронізації доцільним є використання кодів Баркера [8], що обґрунтовується унікальними їх властивостями: автокореляційна функція має максимальний пік при нульовому зсуві та мінімальні побічні пелюстки. Структури відомих кодів Баркера надано в табл. 1. Максимальне значення побічної (нецентральної) пелюстки (МЗПП) автокореляційної функції коду Баркера, нормалізоване відносно основного (центрального) піку.

Таблиця 1.

Структури кодів Баркера

Кількість біт в структурі коду	Код Баркера	МЗПП
2	+1, -1	0
3	+1, +1, -1	0
4	+1, +1, -1, +1	±1
5	+1, +1, +1, -1, +1	±1
7	+1, +1, +1, -1, -1, +1, -1	±1
11	+1, +1, +1, -1, -1, -1, +1, -1, -1, +1, -1	±1
13	+1, +1, +1, +1, +1, -1, -1, +1, +1, -1, +1, -1, +1	±1

Для вибору оптимального коду циклової синхронізації потрібно враховувати наступне:

– більша точність синхронізації забезпечується за рахунок довших кодів;

– більшу швидкість кореляційного пошуку можна досягти за рахунок коротших кодів;

– вищу завадостійкість забезпечують довші коди, які мають більшу енергетичну ефективність в умовах високого рівня шуму в каналі.

Отже, для короткочасної циклової синхронізації в умовах низького рівня завад та високої швидкості передачі доцільно використовувати коди Баркера 7 або 11. Для більш стійкої синхронізації в умовах РЕБ обгрунтованим є вибір коду Баркера 13, який має найкращі властивості по забезпеченню завадостійкості. На рис. 3 надано часові діаграми формування пакету при перетворенні аналогового мовного сигналу в цифровий сигнал.

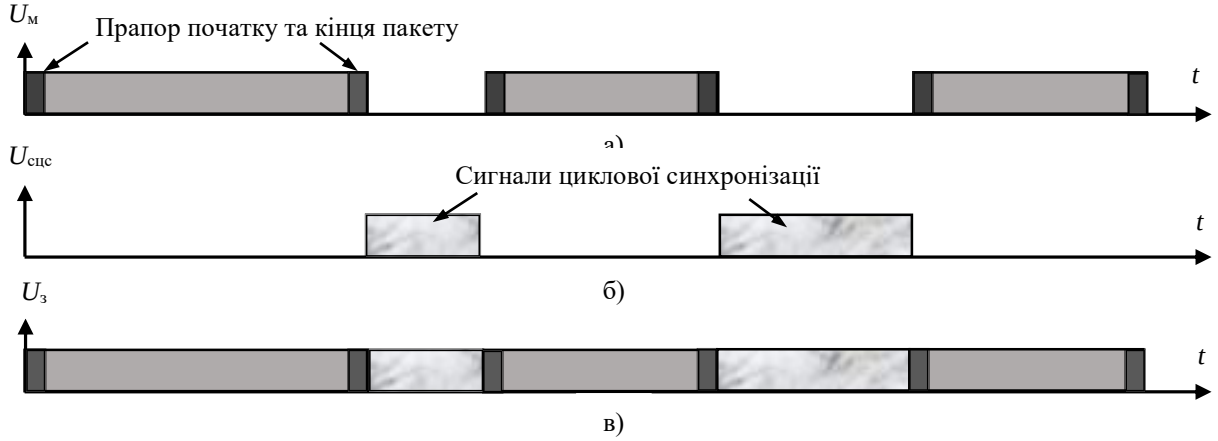

Рис. 3. Часові діаграми формування пакету при перетворенні аналогового мовного сигналу в цифрову послідовність: а) мовний цифровий сигнал з прапорами початку і кінця пакету на основі комбінації 01111110; б) синхросигнали з кодів Баркера (N13=13); в) сумарний цифровий сигнал для перетворення його в акустичний сигнал

Для позначення початку та кінця фрагментів мовного цифрового пакета пропонується використовувати двійкову комбінацію 01111110 (рис. 3 а). Для запобігання появі всередині пакета послідовності 01111110 потрібна процедура вставки додаткового нульового біта після п'яти поспіль передаваних біт логічного значення "1". У приймачі це враховується і після п'яти поспіль біт логічного значення "1", що приймаються, видаляється біт з нульовим значенням.. В якості сигналів циклової синхронізації (рис. 3 б) пропонується код Баркера (N_{13}=13), за допомогою якого заповнюється вільний інтервал між пакетами мовного сигналу (рис. 3 в).

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШОГО РОЗВИТКУ У ДАНОМУ НАПРЯМІ

Запропонований пристрій забезпечує захист мовного сигналу шляхом його цифрового перетворення: шифрування та модифікації акустичних характеристик. Це значно ускладнює дешифрування такого сигналу у випадку перехоплення сеансу передачі засобами радіоелектронної розвідки. Наявність сигналів циклової синхронізації в цифровому потоку дозволяє забезпечити стабільний прийом акустичного мовного сигналу. Пристрій може працювати з різними радіостанціями без їх модифікацій. Також, можлива реалізація даного пристрою з використанням гарнітури радіостанції, що спрощує процес перетворення даних та виключає необхідність додаткового акустичного перетворення мовного сигналу.

Література

1. Hordiichuk V., Snitsarenko P., Sarychev Y., Hrytsiuk V. War in cyberspace as a component of the Russian-Ukrainian hybrid war // Theoretical and applied aspects of the Russian-Ukrainian war: Hybrid aggression and national resilience / Koval M. (Ed.). – Kharkiv: Technology Center PC, 2023, pp. 183–208. – Режим доступу: DOI:10.15587/978-617-8360-00-9.

2. Герасимчук В. О. Захист мовної інформації у системах радіозв'язку. XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 11-12 травня 2023 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 125-127. – Режим доступу: https://ela.kpi.ua/handle/123456789/62380.

3. Конахович Г., Антонов В., Курушкін В. Концепція побудови обладнання захищеного радіотелефонного зв'язку для авіаційних застосувань [Електронний ресурс]. Безпека інформації. - 2014. - Т. 20, № 3. - С. 224-230. – Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2014_20_3_4.

4. Корчинський В.В. Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів / Корчинський В.В., Назаренко О.А., Степанов В.О., Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». No 2 (02) 2022, - С.25-31. – Режим доступу: https://visn-icct.uu.edu.ua/index.php/icct/article/view/86.

5. Гресь О.В., Верига А.Д., Політанський Р.Л., Дробик О.В. Апаратна реалізація пристрою шифрування мовної інформації. Сучасний захист інформації. № 3, 2014. С.71-77. – Режим доступу: http://nbuv.gov.ua/UJRN/szi_2014_3_14.

6. Гресь О. В., Розоріно Г. М., Іванчук М. М., Політанський Р. Л., Верига А. Д. Апаратна реалізація генератора хаотичних сигналів на основі дискретних відображень [Електронний ресурс] Зв'язок. - 2015. - № 3. - С. 35-40 . – Режим доступу: http://nbuv.gov.ua/UJRN/Zvjazok_2015_3_11.

7. Політанський Р. Л., Шпатар П. М., Гресь О. В., & Ляшкевич, В. Я. (2012). Шифрування інформації з використанням псевдовипадкових гаусових послідовностей. *Eastern-European Journal of Enterprise Technologies*, 2015. 6(11(60),С. 8-10. – Режим доступу: https://doi.org/10.15587/1729-4061.2012.5992.

8. Семенко А.І. Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія / А.І. Семенко, Ю.М. Бойко, О.М. Шпур, І. В. Стрелковська, В. В. Корчинський, Р. О. Яровий ; під заг. ред. А.І.Семенка. - Київ: Європейський університет, ФО-П Білецький Р.Г., 2024.- 557 с. ISBN 978-617-853-009-9. – Режим доступу: https://elar.khmnu.edu.ua/handle/123456789/17381.

9. Zakharchenko M., Korchynskii V., Kildishev V. Integrated methods of information security in telecommunication systems. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: http://ieeexplore.ieee.org/document/8095366/.

10. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// Наукові праці ОНАЗ. – Одеса: ОНАЗ, 2020. – № 2, – Р. – 65-69. URL: https://ojs.onat.edu.ua/index.php/sbornik_onat/issue/view/84.

11. Volodymyr Korchynskyi The generating random sequences with the increased cryptographic strength / Volodymyr Korchynskyi, Vitalii Kildishev, Oleksandr Riabukha, Oleksandr Berdnikov // IAPGOS, 1/2020, P. 20-23. URL: https://doi.org/10.35784/iapgos.916.

References

1. Hordiichuk V., Snitsarenko P., Sarychev Y., Hrytsiuk V. War in cyberspace as a component of the Russian-Ukrainian hybrid war // Theoretical and applied aspects of the Russian-Ukrainian war: Hybrid aggression and national resilience / Koval M. (Ed.). – Kharkiv: Technology Center PC, 2023, pp. 183–208. – Режим доступу: DOI:10.15587/978-617-8360-00-9.

2. Herasymchuk, V. O. Zakhyst movnoi informatsii u systemakh radiozviazku. XXI Vseukrainska naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh «Teoretychni i prykladni problemy fizyky, matematyky ta informatyky» (Ukraina, m. Kyiv, 11-12 travnia 2023 r.) : materialy konferentsii. – Kyiv : KPI im. Ihoria Sikorskoho, 2023. – S. 125-127. – Rezhym dostupu: https://ela.kpi.ua/handle/123456789/62380.

3. Konakhovych H., Antonov V., Kurushkin V. Kontseptsiia pobudovy obladnannia zakhyshchenoho radiotelefonnoho zviazku dlia aviatsiinykh zastosuvan [Elektronnyi resurs]. Bezpeka informatsii. - 2014. - T. 20, № 3. - S. 224-230. – Rezhym dostupu: http://nbuv.gov.ua/UJRN/bezin_2014_20_3_4.

4. Korchynskyi V.V. Metody pidvyshchennia prykhovanosti peredavannia informatsii na osnovi rozshyrennia spektra taimernykh syhnaliv / Korchynskyi V.V., Nazarenko O.A., Stepanov V.O., Al-Faiiumy Khaled // Naukovyi zhurnal «Infokomunikatsiini ta kompiuterni tekhnolohii» – Kyiv, «Vidkrytyi mizhnarodnyi universytet rozvytku liudyny «Ukraina». No 2 (02) 2022, S.25-31. – Rezhym dostupu: https://visn-icct.uu.edu.ua/index.php/icct/article/view/86.

5. Hres O.V., Veryha A.D., Politanskyi R.L., Drobyk O.V. Aparatna realizatsiia prystroiu shyfruvannia movnoi informatsii. Suchasnyi zakhyst informatsii. № 3, 2014. S.71-77. – Rezhym dostupu: http://nbuv.gov.ua/UJRN/szi_2014_3_14.

6. Hres O. V., Rozorino H. M., Ivanchuk M. M., Politanskyi R. L., Veryha A. D. Aparatna realizatsiia heneratora khaotychnykh syhnaliv na osnovi dyskretnykh vidobrazhen [Elektronnyi resurs] Zviazok. - 2015. - № 3. - S. 35-40 . – Rezhym dostupu: http://nbuv.gov.ua/UJRN/Zvjazok_2015_3_11.

7. Politanskyi, R. L., Shpatar, P. M., Hres, O. V., & Liashkevych, V. Ya. (2012). Shyfruvannia informatsii z vykorystanniam psevdovypadkovykh hausovykh poslidovnostei. Eastern-European Journal of Enterprise Technologies, 2015. 6(11(60),S. 8-10. – Rezhym dostupu: https://doi.org/10.15587/1729-4061.2012.5992.

8. Semenko A.I. Cuchasni tekhnolohii infokomunikatsiinykh ta kompiuternykh merezh: monohrafiia / A.I. Semenko, Yu.M. Boiko, O.M. Shpur, I. V. Strelkovska, V. V. Korchynskyi, R. O. Yarovyi ; pid zah. red. A.I.Semenka. - Kyiv: Yevropeiskyi universytet, FO-P Biletskyi R.H., 2024.- 557 s. ISBN 978-617-853-009-9. – Rezhym dostupu: https://elar.khmnu.edu.ua/handle/123456789/17381.

9. Zakharchenko M., Korchynskii V., Kildishev V. Integrated methods of information security in telecommunication systems. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: http://ieeexplore.ieee.org/document/8095366/.

10. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// Наукові праці ОНАЗ. – Одеса: ОНАЗ, 2020. – № 2, – Р. – 65-69. URL: https://ojs.onat.edu.ua/index.php/sbornik_onat/issue/view/84.

11. Volodymyr Korchynskyi The generating random sequences with the increased cryptographic strength / Volodymyr Korchynskyi, Vitalii Kildishev, Oleksandr Riabukha, Oleksandr Berdnikov // IAPGOS, 1/2020, P. 20-23. URL: https://doi.org/10.35784/iapgos.916.