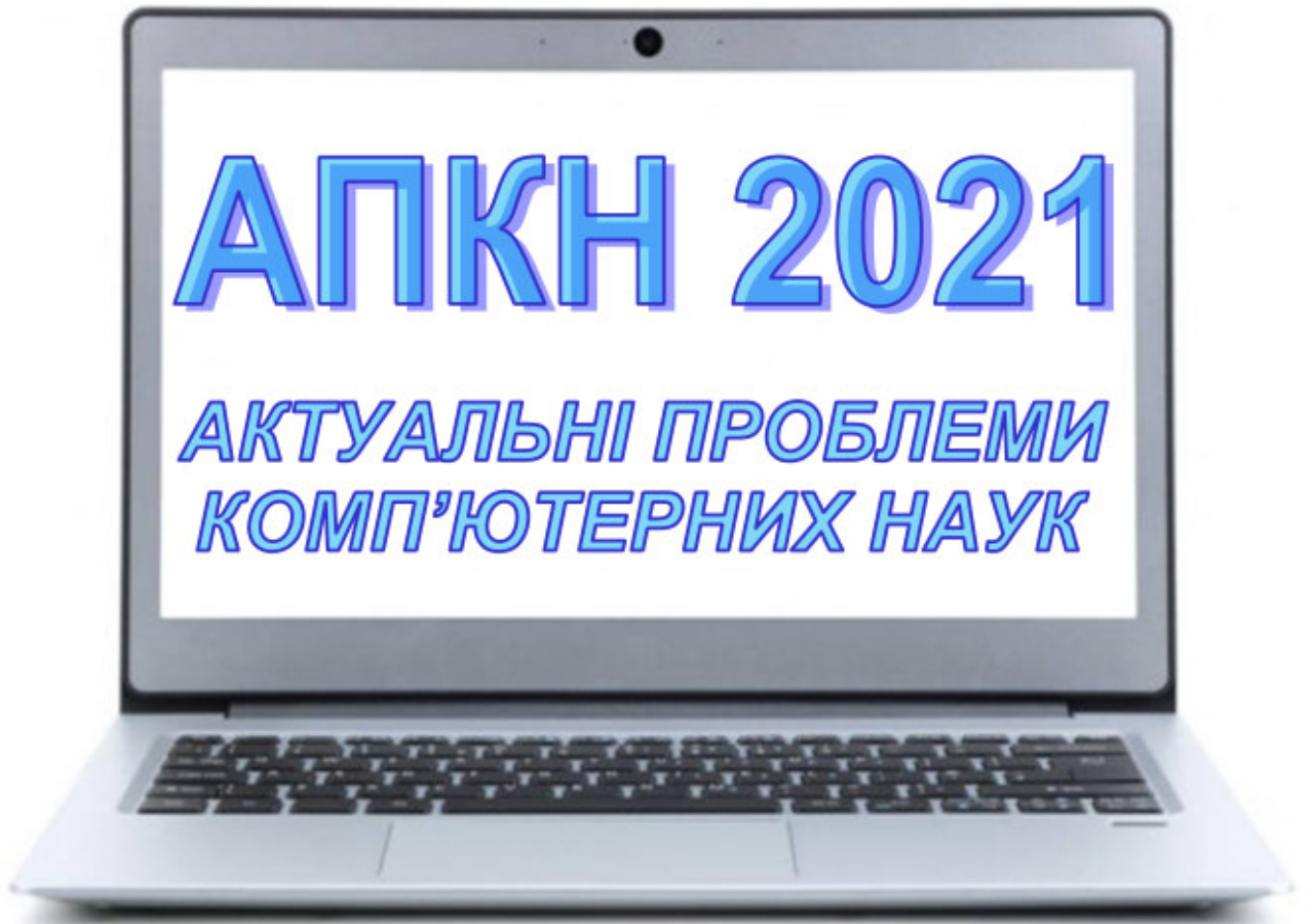


Міністерство освіти і науки України
Хмельницький національний університет



ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XIII Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2021»

15-16 жовтня 2021

Хмельницький 2021

УДК 004:37:001:62

Збірник наукових праць за матеріалами XIII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2021». Хмельницький – 2021. – 413с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів.

Участь у конференції та складові всіх її етапів (розгляд праць, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: apkt.khnu@gmail.com

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2021

XIII Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

Робочі мови конференції: українська, англійська

ОРГКОМІТЕТ:

СИНЮК О. М. голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

САВЕНКО О. С. заступник голови оргкомітету, декан факультету Інформаційних технологій ХНУ, доктор технічних наук, професор

БАРМАК О. В. заступник голови оргкомітету, завідувач кафедри Комп'ютерних наук ХНУ, доктор технічних наук, професор

ГОВОРУЩЕНКО Т. О. завідувач кафедри Комп'ютерної інженерії та інформаційних систем ХНУ, доктор технічних наук, професор

ВИСОЦЬКА О. В. доктор технічних наук, завідувач кафедри Радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», професор

ЛАВРОВ Є. А. доктор технічних наук, професор (Сумський державний університет)

ТІМОФЄЄВА Л. В. відповідальна за студентську науково-дослідну роботу ХНУ

МАЗУРЕЦЬ О. В. секретар конференції, к.т.н., доцент кафедри Комп'ютерних наук ХНУ

МОЛЧАНОВА М. О. секретар конференції, викладач кафедри Комп'ютерних наук ХНУ

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: apkt.khnu@gmail.com

Галкіна Р. І., Багрій Р. О., Скрипник Т. К. Застосування адаптивного підходу для реалізації системи опитувань та тестувань.....	306
Гринь С. С., Пивовар О. С., Таранчук А. А. Забезпечення прихованості дії та криптографічного захисту аналогових сигналів в хаотичній системі зв'язку.....	309
Данчук С. В., Багрій Р. О. Технологія автоматизованого отримання даних з веб-ресурсів для бізнес-аналітики.....	312
Длугунович Н. А. Інформаційна технологія фінансового моделювання для розвитку малого підприємництва.....	316
Дрозд А. І., Форкун Ю. В. Метод розподілу обчислювальних ресурсів для обробки розподілених потоків даних	319
Дудар О. В., Міхалевський В. Ц., Скрипник Т. К. Інформаційна система для забезпечення підтримки екологічної рівноваги.....	321
Єфімчук А. С., Скрипник Т. К., Мазурець О. В., Молчанова М. О. Автоматизований розподіл процесів при управлінні ІТ-проектами в складних критично-безпекових умовах.....	324
Житкевич В. В., Медведчук В. Ю. Метод відновлення пошкоджених растрових зображень.....	332
Заровний В. І., Скрипник Т. К. Методи шифрованої передачі даних між хмарними підпросторами	335
Кудрявцев В. В., Форкун Ю. В. Аналіз та застосування методів оптимізації швидкодії та відмовостійкості програмних продуктів	338
Курдибаха А. В., Мазурець О. В., Собко О. В., Молчанова М. О. Інформаційна технологія оцінювання діяльності сімейного лікаря за даними прийомів	340
Лавренцій А. А., Петровський С. С. Метод оцінювання наповненості дистанційних курсів предметів у школі	349
Левченко Т. В., Блажук В. Д., Молчанова М. О., Собко О. В. Метод оптимізації транспортних перевезень засобами біологічної метаевристики	352

УДК 623.519

Гринь С. С., Пивовар О. С., Таранчук А. А.

Хмельницький національний університет

ЗАБЕЗПЕЧЕННЯ ПРИХОВАНОСТІ ДІЇ ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ АНАЛОГОВИХ СИГНАЛІВ В ХАОТИЧНІЙ СИСТЕМІ ЗВ'ЯЗКУ

Розглянуто можливості одночасного забезпечення прихованості дії та криптографічного захисту в телекомунікаційних системах із застосуванням сигналів детермінованого хаосу та хаотичних методів їх обробки.

Possibilities of simultaneous provision of stealth of action and cryptographic protection in telecommunication systems with application of signals of deterministic chaos and chaotic methods of their processing are considered.

Захист інформації (ЗІ) – одне із найважливіших завдань прогресивного розвитку людства. Без забезпечення конфіденційності даних неможливе існування світової економіки в тому вигляді, що ми знаємо. Найкращим способом забезпечення проблематики ЗІ є прихованість дії, що забезпечує захист через неможливість виявлення навіть факту передачі [1].

Інший спосіб ЗІ – криптографічний, що передбачає застосування алгоритмів перетворення повідомлень таким чином, щоб за умови можливості виявлення факту передачі, забезпечувалась неможливість виявлення її інформаційного змісту. Поєднання захисту прихованістю дії та криптографічними перетвореннями дає найліпші результати загалом [1].

Останніми десятиліттями з'явилися вдалі спроби застосувати для захисту інформації методи хаотичної динаміки [2], що дозволяють одночасно вирішити як завдання прихованості дії, так і завдання криптографічного захисту.

Метою роботи є розробка концепції використання методів хаотичної динаміки для забезпечення захисту аналогових повідомлень від несанкціонованого доступу в телекомунікаційних каналах зв'язку.

Найбільш перспективним методом введення інформаційного сигналу в хаотичну піднесівну вважають метод параметричної модуляції хаотичного генератора (ХГ) [2], а найбільш завадостійким способом демодуляції є метод допоміжного ХГ на приймальному боці [3]. Основою роботи такої схеми передачі інформації є забезпечення односпрямованої хаотичної синхронізації та фіксація рівня її значення для через деякий критерій, який враховує відмінності між основним та допоміжним веденими ХГ [3].

Для розробки системи передачі із хаотичним ЗІ запропоновано застосувати такі підходи: за умови малої відмінності між параметрами веденого та ведучого ХГ режим хаотичної синхронізації встановлюється більш швидко; для передачі аналогових повідомлень слід застосовувати «силу» зв'язку між веденим та ведучим генераторами менше критичної; для детектування аналогових повідомлень із підвищеним криптографічним захистом на приймальному боці слід використати екстраполятор із керованими параметрами.

Дослідження застосування вказаних підходів реалізовувалось на базі ХГ Rucklidge, який має два параметри керування (a, k).

Якщо для визначення похибки синхронізації застосувати різницеву потужність сигналу однойменних фазових змінних основного та допоміжного ведених генераторів та логарифмічний масштаб то на залежності (рис.1) присутня значна лінійна ділянка, що може бути застосована як модуляційна характеристика в системі криптографічного захисту, а дія шумоподібного хаотичного сигналу та власне схема передачі забезпечуватиме прихованість дії.

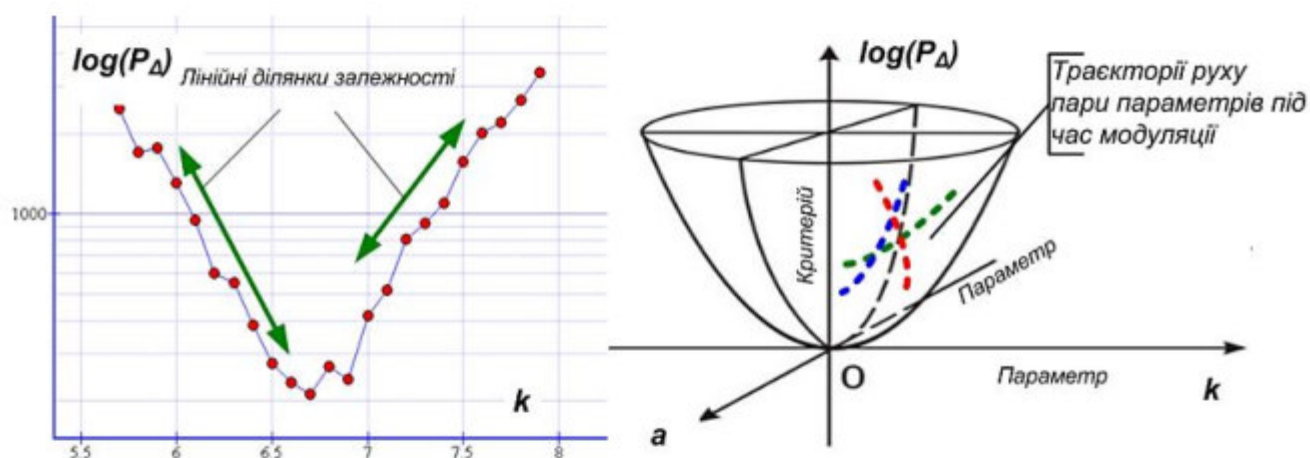


Рисунок 1 – Залежність похибки синхронізації від параметрів керування хаотичних веденого та ведучого генераторів

В такій системі прихованого зв'язку (рисунок 2) сукупність пар значень параметрів хаотичного генератора, які визначають середину лінійної ділянки, задають параметри криптографічного захисту, а характер їх функціональних – алгоритм шифрування (рисунок 1).

В схемі передачі (рис.2) за запропонованими принципами сумісний параметричний модулятор за допомогою ключів шифрування обирає траєкторію зміни параметрів під дією аналогового сигналу. На приймальному боці ведені ХГ починають синхронізуватись із ведучим генератором тим краще, чим ближче значення їх параметрів до поточних параметрів ведучого генератора встановлені екстраполятором. Дешифрування можливе лише за умови правильного вибору

значень параметрів, що забезпечується ключами шифрування на передавальному та приймальному боці.

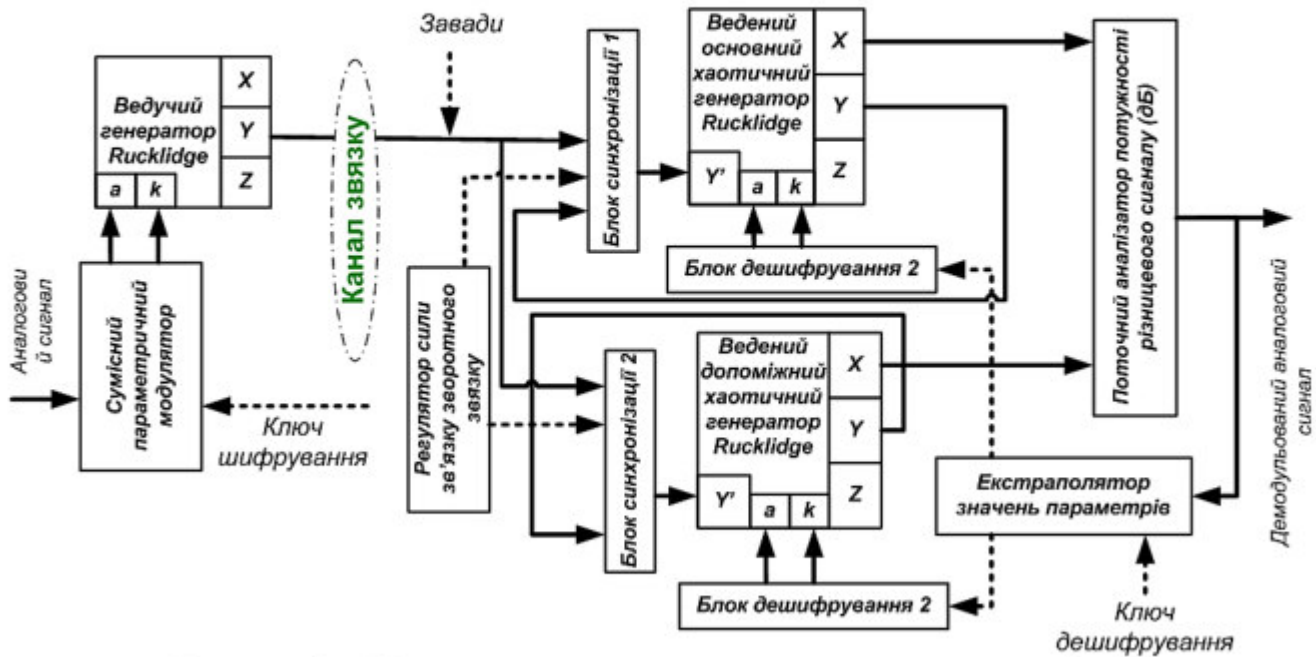


Рисунок 2 – Хаотична аналогова система прихованого зв'язку

Перевірка працездатності запропонованої схеми передачі реалізована в системі Matlab/Simulink. Рівень нелінійних спотворень під час передавання повідомлень не перевищував 5% за умови відношення сигнал-шум 10дБ.

Перелік посилань

1. Конахович Г.Ф. Захист інформації в телекомунікаційних системах /Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн, О.О. Горбунов //Навчальний посібник.– К.: НАУ,2009. – 380с.
2. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р. Л. Політанський; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів; Дрогобич : Коло, 2015. – 184 с.
3. Golevych.O, Pyvovar. O. Dumenko.P "Synchronization of non-linear dynamic systems under the conditions of noise action in the channel", Latvian Journal of Physics and Technical Sciences Открытый доступ Volume 55, Issue 3, 1 June 2018, Pages 70-76 DOI: <https://doi.org/10.2478/lpts-2018-0023>



АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК 2021

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Комп'ютерна верстка: Мазурець О.В.

Підписано до друку 14.10.2021.

Версія друку «APKN-2021 CorpusPaper v4mod3».

E-mail: apkt.khnu@gmail.com

ХНУ. м. Хмельницький, вул. Інститутська, 11.