

<https://doi.org/10.15407/knit2025.01.077>

УДК 621.396.99

**Ю. В. СТАСЄВ**, проф. кафедри, д-р техн. наук, проф.

ORCID 0000-0002-3893-0313

E-mail: stasev543@gmail.com

**Д. М. НЕПОКРИТОВ**, доцент кафедри

ORCID 0000-0003-1752-8496

E-mail: ndn\_ndn@ukr.net

**М. В. ПАРХОМЕНКО**, доцент кафедри, канд. техн. наук

ORCID 0000-0001-6062-7743

E-mail: maxpar76@gmail.com

**С. Г. ШИЛО**, доцент кафедри, канд. техн. наук, доцент

ORCID 0000-0001-5782-552X

E-mail: shilosg@i.ua

Харківський національний університет Повітряних Сил імені Івана Кожедуба

вул. Сумська 77/79, Харків, Україна, 61023

## МЕТОД ЗАХИСТУ КОСМІЧНИХ СИСТЕМ ЗВ'ЯЗКУ ТА КЕРУВАННЯ НА ОСНОВІ ДИНАМІЧНОЇ ЗМІНИ ФОРМ СКЛАДНИХ СИГНАЛІВ

*Досвід експлуатації космічних систем показує, що їхня ефективність суттєво залежить від якості функціонування системи зв'язку та керування космічним апаратом. Враховуючи, що космічні системи зв'язку та керування доступні для зловмисників, у таких системах реалізовано захист переданих команд та повідомлень з використанням криптографічних перетворень інформації та спеціальної апаратури. Реалізовані в таких системах алгоритми забезпечують пасивний захист системи керування космічним апаратом, при якому апаратура керування відмовляє в обробці команд при наявності потужних перешкод. Впровадження ефективних заходів стає ключовою складовою стратегій захисту космічних систем зв'язку та керування, оскільки технологічні можливості для атак на космічний апарат через радіоканал постійно розвиваються та стають все складнішими. Захист від потужних навмисних перешкод в таких системах здійснюється з використанням сигналів з частотною надмірністю. У статті розглядається метод динамічної зміни форм сигналів, який дозволяє забезпечити безпеку інформації на фізичному рівні. Виконується аналіз перешкодозахисту та імітостійкості космічних систем зв'язку та керування при використанні різних систем складних сигналів. Проаналізовано ансамблеві характеристики систем складних сигналів. Наведено результати досліджень імітостійкості при використанні різних систем сигналів. Визначено, що при реалізації динамічного режиму функціонування досягається вииграш у порівнянні з традиційними алгоритмами захисту космічних систем зв'язку та керування. Сформульовано умови практичної реалізації динамічного режиму функціонування космічних систем зв'язку та керування. Запропоновані системи сигналів, які дозволяють вирішити проблему безпеки передачі інформації в космічних системах зв'язку та керування на фізичному рівні.*

**Ключові слова:** космічні системи зв'язку та керування, перешкодозахист, імітостійкість, сигнали з частотною надмірністю.

Цитування: Стасєв Ю. В., Непокритов Д. М., Пархоменко М. В., Шило С. Г. Метод захисту космічних систем зв'язку та керування на основі динамічної зміни форм складних сигналів. *Космічна наука і технологія*. 2025. **31**, № 1 (152). С. 77—85. <https://doi.org/10.15407/knit2025.01.077>

© Видавець ВД «Академперіодика» НАН України, 2025. Стаття опублікована за умовами відкритого доступу за ліцензією CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

## ВСТУП

**Постановка проблеми.** Створення та застосування різноманітних космічних систем є перспективним напрямком практичного використання космічного простору. На сьогодні створені та успішно експлуатуються сотні різноманітних космічних систем військового та цивільного призначення [1—3, 12, 13, 15, 21—23, 25—27]. Рішення проблеми безпеки інформації, яка передається в космічних системах зв'язку та керування пов'язують з рішенням проблеми перешкодозахисту та імітостійкості [4—6, 12—15, 19]. Численні дослідження показують, що в теперішній час ці проблеми вирішуються окремо. Проблема перешкодозахисту розв'язується за рахунок енергетичних ресурсів космічних систем зв'язку та керування або за рахунок застосування на фізичному рівні сигналів з частотною надмірністю [13, 15, 19]. Потрібна імітостійкість забезпечується за допомогою перетворення дискретної інформації з використанням криптографічних перетворень інформації та спеціальної апаратури [4—6, 8, 11].

До теперішнього часу створено і успішно функціонує ряд космічних систем зв'язку та керування зі складними сигналами [2, 12—15, 21]. У цих системах для розширення спектру застосовуються сигнали з псевдовипадковою перебудовою робочою частотою (ППРЧ) [14], лінійні рекурентні послідовності максимальної довжини (ЛРПМ) [14], лінійні рекурентні послідовності з трирівневою функцією кореляції (ЛРПТ) [14] або сегменти цих послідовностей [10, 16, 24]. Однак ці послідовності мають незадовільні ансамблеві та структурні характеристики [14], що не дозволяє вирішити проблему безпеки інформації на фізичному рівні.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

В роботах [6, 8, 18] розглядаються методи захисту інформації на основі криптографічних перетворень інформації та відмови від прийому і обробки пакету інформації у випадку виявлення помилок у повідомленні. Такий підхід не є можливим для національних систем керування космічними апаратами, які працюють в умовах

жорсткого ліміту часу на передачу та прийом інформації.

У роботі [4] запропоновано метод динамічної зміни форм сигналів та визначено умови практичної реалізації цього методу, проте методики оцінки перешкодозахисту та імітостійкості космічних систем зв'язку та керування на фізичному рівні не наведено.

У роботах [5, 20] розроблено рекомендації з побудови систем керування літальними апаратами. В роботі [14] проведено аналіз властивостей дискретних сигналів для перешкодозахищених систем зв'язку та керування.

Розроблені в [4, 5, 20] рекомендації дозволяють оцінити граничні значення перешкодозахисту, імітостійкості та скритності в космічних системах зв'язку та керування без урахування енергетичних характеристик радіоліній.

Аналіз проведених досліджень показав, що на теперішній час відсутні методи оцінки безпеки інформації космічних системах зв'язку та керування на фізичному рівні.

**Мета статті.** Обґрунтування методу захисту інформації в космічних системах зв'язку та керування на фізичному рівні.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Рішення проблеми безпеки передачі інформації в космічних системах зв'язку та керування пов'язують з рішенням проблеми забезпечення перешкодозахищеності та імітостійкості. У роботі [5] сформульовано основні задачі системи та апаратури захисту інформації в космічних системах зв'язку та керування:

- забезпечення достовірності та цілісності переданої командно-програмної інформації,
- забезпечення конфіденційності даних та командно-програмної інформації,
- забезпечення ідентифікації та автентифікації об'єктів та суб'єктів процесу керування в системах керування космічними апаратами,
- захист від несанкціонованого доступу до системи керування космічними апаратами,
- забезпечення юридичної відповідальності користувачів за сформовані, передані, прийняті та виконані команди,
- керування спеціальними даними.

Ефективність функціонування космічних систем зв'язку та керування, як показали дослідження, багато в чому залежить від її завадо- та перешкодозахищеності, скритності та спроможності протистояти від несанкціонованого доступу до системи керування. Як правило, космічні системи зв'язку та керування функціонують в умовах впливу як природних, так і потужних навмисних перешкод [3, 7, 17].

Для забезпечення стійкості роботи космічних систем зв'язку та керування в цих умовах необхідно прийняти цілий комплекс заходів, спрямованих на досягнення необхідних значень імітостійкості каналу зв'язку, а також забезпечити необхідний доступ інформації та команд керування об'єктами, які передані по каналу зв'язку, що запобігає витоку інформації і обмежує доступ до енергетичних ресурсів радіолінії. Ефективність функціонування космічних систем зв'язку та керування визначається багатьма факторами, зокрема [12, 20]:

- здатністю протистояти природнім і навмисним перешкодам,
- здатністю забезпечити високу структурну скритність сигналів,
- забезпеченням високої пропускну здатності,
- забезпеченням скритності радіолінії керування космічним апаратом,
- забезпеченням ефективного перекриття каналів витоку інформації.

Застосуванням цих заходів в комплексі можливо досягти стійкої роботи системи зв'язку та керування космічним апаратом. Однак в такій концепції захисту інформації, як показали дослідження [4–6, 18, 20], не реалізуються потенціальні можливості захисту космічних систем зв'язку та керування, які досягаються за рахунок динамічної передачі сигналів, при який відповідність «інформаційний символ сигнал-переносник» змінюється в часі по псевдовипадковому закону.

Реалізація режиму динамічної передачі сигналів дозволяє на фізичному рівні вирішити проблему захисту від несанкціонованого доступу до каналу, а також забезпечує приховування змісту переданих повідомлень.

У нашій роботі [4] було розроблено теоретичні основи побудови та реалізації режиму динамічної передачі сигналів у космічних системах зв'язку та керування. На основі сформульованих теоретичних положень були розроблені технічні рішення щодо забезпечення безпеки інформації в космічних системах зв'язку та керування [5, 14]. В основу розроблених технічних рішень покладено обґрунтовані вимоги до апаратури імітозахисту і запропоновано структуру команд [6].

Аналіз особливостей функціонування космічних систем зв'язку та керування [4, 5, 14], а також врахування перерахованих вище факторів показує, що найповніше забезпечує ефективність функціонування такий протокол обміну даними:

$$P = \{S_k, B_n, K_n\}, \quad (1)$$

де  $S_k$  — процес синхронізації кореспондентів за частотою та затримкою,  $B_n$  — процес встановлення автентичності та повноважень кореспондентів,  $K_n$  — процес передачі команд і спеціальних радіоданих.

Зупинимось детальніше на несанкціонованому доступі до радіолінії керування космічним апаратом. Аналіз особливостей функціонування радіолінії керування космічним апаратом [5] показує, що можливість несанкціонованого доступу залежить, з одного боку, від здатності зловмисника нав'язати захищену команду, а з іншого боку — нав'язати складні сигнали.

Кількісно стійкість системи керування щодо несанкціонованого доступу до радіолінії керування космічним апаратом можна обчислити з використанням виразу [14]

$$I = P_{\text{нав.ком}} P_{\text{нав.сигн}}, \quad (2)$$

де  $P_{\text{нав.ком}}$  — ймовірність нав'язування хибної команди,  $P_{\text{нав.сигн}}$  — ймовірність нав'язування помилкового сигналу.

Відзначимо, що  $P_{\text{нав.ком}}$  визначає несанкціонований доступ до радіолінії керування космічним апаратом на дискретному рівні і залежить від алгоритмів формування дискретних захищених команд.  $P_{\text{нав.сигн}}$  визначає несанкціонований доступ до радіолінії керування і зв'язку на фізичному рівні і залежить від особливостей функціонування радіолінії, системи використання сигналів, енергетичних характеристик.

Зупинимось детальніше на несанкціонованому доступі до радіолінії керування на фізичному рівні. Наведений аналіз показує, що ймовірність нав'язування команди визначається виразом [14]

$$P_{\text{нав.ком}} = P_{\text{нав.інф.бл}} P_{\text{нав.нд}}, \quad (3)$$

де  $P_{\text{нав.інф.бл}}$  — ймовірність нав'язування стандартного інформаційного блоку довжиною  $m$  біт,  $P_{\text{нав.нд}}$  — ймовірність можливості здійснювати нав'язування хибних команд зловмисником.

Ймовірність нав'язування інформаційного блоку залежить від його довжини і визначається виразом [6]:

$$P_{\text{нав.інф.бл}} = 2^{-m}, \quad (4)$$

де  $m$  — довжина стандартного інформаційного блоку, який використовується в радіолінії керування.

Оцінимо несанкціонований доступ до радіолінії керування космічним апаратом в умовах впливу зловмисника на систему. Спочатку розглянемо випадок, коли інформаційним символам відповідають одні і ті ж форми складних сигналів. Тоді несанкціонований доступ радіолінії керування безпілотним літальним апаратом залежить від енергетичних співвідношень сигналів і перешкод; від взаємного розташування радіопередавальних і радіоприймальних пристроїв; від характеристик антенних систем; чутливості прийомних пристроїв; від умов поширення електромагнітних хвиль; від видів випромінювання і способів обробки сигналів; від робочої частоти і бази сигналів. Якість функціонування таких систем залежить від можливостей зловмисника формувати структурні та імітаційні перешкоди.

З огляду на той факт, що форми складних сигналів, які використовуються для передачі інформаційних символів, не змінюються в часі, зловмисник має реальну можливість сформувати структурну перешкоду, максимально корельовану з корисним сигналом. Це призводить до зниження відношення енергії сигналу  $E_c$  до спектральної щільності перешкоди  $N_0$ , що визначається співвідношенням

$$\frac{E_c}{N_0} = \frac{P_c}{P_n} \cdot T_c \cdot \Delta F_c (1 - R_{\sigma \max}), \quad (5)$$

де  $T_c$  — тривалість сигналу,  $\Delta F_c$  — ширина спектра сигналу,  $R_{\sigma \max}$  — рівень бічних пелюсток функції взаємної кореляції корисного і перешкоджаючих сигналів.

При оцінці перешкодозахищеності радіолінії керування космічним апаратом необхідно розглядати два режими роботи: режим виявлення (синхронізації) і режим розрізнення складних сигналів.

Режим виявлення складних сигналів характеризується ймовірністю хибної тривоги  $P_{\text{хт}}$  й ймовірністю пропуску сигналу  $P_{\text{пр}}$ . Число інтервалів невизначеності при пошуку дорівнює  $N$ , запишемо вираз, що зв'яже ймовірності  $P_{\text{хт}}$  й  $P_{\text{пр}}$  з енергетичними характеристиками сигналу [15]:

$$P_{\text{пр}} = \Phi \left( \sqrt{\frac{E_c}{N_0}} - \sqrt{2 \ln \frac{N}{P_{\text{хт}}}} \right), \quad (6)$$

де  $\Phi(x)$  — інтеграл ймовірності,  $E_c / N_0$  — відношення енергії сигналу до спектральної потужності перешкоди.

Вираз (6) враховує випадок, коли фаза сигналу точно відома. Очевидно, що при наявності невизначеності по фазі ймовірність виявлення погіршується, і це можна розглядати як втрати енергії сигналу. У роботі [14] показано, що для сигналу з випадковою фазою необхідне відношення  $E_c / N_0$  при заданих  $P_{\text{хт}}$  і  $P_{\text{пр}}$  визначається виразом

$$\frac{E_c}{N_0} = \left[ \sqrt{\ln \frac{N}{P_{\text{хт}}}} + \sqrt{\ln \frac{1}{P_{\text{пр}}} - 1.4} \right]^2, \quad (7)$$

У режимі розрізнення складних сигналів якість розрізнення сигналів характеризується ймовірністю помилки  $P_{\text{пом}}$  й визначається співвідношенням [9, 14]

$$P_{\text{пом}} = 1 - \Phi \left( \sqrt{\frac{2E_c}{N_0}} \right) \quad (8)$$

при когерентній обробці сигналу та

$$P_{\text{пом}} = 0.5 \exp[-E_c / (2N_0)] \quad (9)$$

при некогерентній обробці сигналу.

Вирази (6)–(9) дозволяють оцінити перешкодозахищеність космічних систем зв'язку та керування при впливі загороджувальних і зосереджених по спектру перешкод. Водночас аналіз особливостей функціонування космічних

систем зв'язку та керування показує, що поряд із загороджувальними й зосередженими по спектрі перешкодами на радіолінії можуть впливати потужні структурні перешкоди. У цьому випадку перешкодозахищеність системи зв'язку й керування залежить від взаємної кореляції корисного сигналу та завади, а ймовірність прийому хибного сигналу з урахуванням дії в радіоканалі шуму і сигналів-перешкод запишеться у вигляді [14, 20]

$$P_x = P_{\pi}(P_m + P_c) + (1 - P_{\pi})P_{\text{пом}}, \quad (10)$$

де  $P_{\pi}$  — апіорна ймовірність потрапляння сигналу-перешкоди в розрізнений у даний момент часу частотний діапазон,  $P_m$  — умовна ймовірність прийому хибного сигналу при дії на вимисної перешкоди в каналі, де сигнал відсутній,  $P_c$  — умовна ймовірність перейменування сигналу при дії на нього сигналу перешкоди та шуму,  $P_{\text{пом}}$  — ймовірність помилки через дію шуму.

Оцінимо імітостійкість і скритність системи зв'язку й керування при використанні квазіоптимальних, складних і похідних квазіортогональних систем сигналів, вважаючи, що в системі зв'язку й керування реалізується динамічний режим «швидкий код», причому зміна форм складових сигналів здійснюється через інтервали часу, які дорівнюють тривалості сигналу.

У табл. 1 наведені результати досліджень порівняльного аналізу ймовірності імітації сигналу в системі зв'язку й керування при використанні традиційних ЛРПМ, ЛРПТ, квазіортогональних [10, 16, 24] та синтезованих авторами похідних квазіортогональних і складових систем сигналів [14]. Аналіз табл. 1 показує, що синтезовані системи сигналів дозволяють забезпечити імітостійкість системи зв'язку й керування на фізичному рівні. Не менш важливою характеристикою системи зв'язку й керування є ймовірність нав'язування одержувачу хибної інформації.

У табл. 2 наведені значення ймовірності нав'язування і-біт хибної інформації при  $L = 256$ .

Аналіз табл. 1 та табл. 2 дозволяє зробити висновки, що реалізація в системі зв'язку й керування динамічного режиму і використання синтезованих систем сигналів дозволяє на фізичному рівні розв'язувати задачу імітостійкості і перешкодозахищеності.

При практичній реалізації динамічного режиму функціонування забезпечити наведені в таблицях значення можливо тільки при виконанні умов [4]:

- ймовірність передачі сигналу не повинна залежати від передавальних інформаційних символів і переданих раніше сигналів;

Таблиця 1. Порівняльний аналіз ймовірності імітації складового сигналу при реалізації динамічного режиму

| Системи сигналів                   | 127                 | 255                 | 511                 | 1 023               |
|------------------------------------|---------------------|---------------------|---------------------|---------------------|
| ЛРПМ                               | $4.3 \cdot 10^{-4}$ | $2.5 \cdot 10^{-4}$ | $4 \cdot 10^{-5}$   | $1.6 \cdot 10^{-5}$ |
| ЛРПТ                               | $6.2 \cdot 10^{-5}$ | $2.5 \cdot 10^{-4}$ | $3.8 \cdot 10^{-6}$ | $9.6 \cdot 10^{-7}$ |
| Квазіортогональні системи сигналів | $9.2 \cdot 10^{-6}$ | $1.3 \cdot 10^{-6}$ | $3.5 \cdot 10^{-7}$ | $7 \cdot 10^{-8}$   |
| Похідні квазіортогональні сигнали  | $2.5 \cdot 10^{-6}$ | $4.6 \cdot 10^{-7}$ | $1.6 \cdot 10^{-7}$ | $1.6 \cdot 10^{-9}$ |
| Складні системи сигналів           | $2.6 \cdot 10^{-6}$ | $4.3 \cdot 10^{-7}$ | $3.9 \cdot 10^{-8}$ | $1.4 \cdot 10^{-9}$ |

Таблиця 2. Ймовірність нав'язування і-біт хибної інформації

| Системи сигналів                   | 1                   | 2                    | 3                    | 4                    | 5                    | 6                    |
|------------------------------------|---------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| ЛРПМ                               | $2.5 \cdot 10^{-4}$ | $6.2 \cdot 10^{-8}$  | $1.6 \cdot 10^{-11}$ | $3.9 \cdot 10^{-15}$ | $9.8 \cdot 10^{-19}$ | $2.4 \cdot 10^{-22}$ |
| ЛРПТ                               | $2.5 \cdot 10^{-4}$ | $6 \cdot 10^{-8}$    | $1.6 \cdot 10^{-11}$ | $3.9 \cdot 10^{-15}$ | $9.8 \cdot 10^{-19}$ | $2.4 \cdot 10^{-22}$ |
| Квазіортогональні системи сигналів | $9.2 \cdot 10^{-6}$ | $9.2 \cdot 10^{-11}$ | $8.8 \cdot 10^{-16}$ | $8.6 \cdot 10^{-21}$ | $8.2 \cdot 10^{-26}$ | $7.8 \cdot 10^{-31}$ |
| Похідні квазіортогональні сигнали  | $2.5 \cdot 10^{-6}$ | $6.2 \cdot 10^{-12}$ | $1.6 \cdot 10^{-17}$ | $3.9 \cdot 10^{-23}$ | $9.8 \cdot 10^{-29}$ | $2.4 \cdot 10^{-34}$ |
| Складні системи сигналів           | $2.5 \cdot 10^{-6}$ | $6.7 \cdot 10^{-12}$ | $1.8 \cdot 10^{-17}$ | $4.6 \cdot 10^{-23}$ | $1.2 \cdot 10^{-28}$ | $3.1 \cdot 10^{-34}$ |



- розмір ансамблю використовуваних сигналів повинен задовольняти вимогу з іміто- і перешкодозахищеності;
- стійкість керівної множини, яка задає динамічний режим функціонування, не повинна знижуватися у випадках, коли зловмисникам відомий засіб реалізації динамічного режиму;
- надлишковість, що міститься в інформації про множини, яка задає динамічний режим функціонування, повинна бути мінімальною.

## ВИСНОВКИ

Аналіз властивостей складових систем сигналів показав, що вищі значення перешкодозахищеності, імітостійкості та скритності космічних систем зв'язку та керування досягаються при використанні сегментів похідних систем сигналів.

Імовірність нав'язування хибного сигналу залежить від енергетичних співвідношень сигналу та завади і ступеня їхньої кореляції. Отже, перешкодозахищеність та імітостійкість космічних систем зв'язку та керування досягається за рахунок використання слабкорельованих систем сигналів, які мають розширений ансамбль сигналів та невизначеності для зловмисника конкретної форми сигналу.

Таким чином, розв'язання задачі підвищення перешкодозахищеності та імітостійкості космічних систем зв'язку та керування на фізичному рівні досягається використанням сигналів з поліпшеними ансамблевими, кореляційними, структурними характеристиками і застосуванням алгоритмів динамічної зміни сигнальних конструкцій.

## ЛІТЕРАТУРА

1. Александров С., Туров Д. Перспективные системы и средства радиосвязи тактического звена управления ВС США. *Зарубежное военное обозрение*. 2018. № 11. С. 42—48. URL: [http://pentagonus.ru/publ/perspektivnye\\_sistemy\\_i\\_sredstva\\_radiosvjazi\\_takticheskogo\\_zvena\\_upravlenija\\_vs\\_ssha\\_2018/11-1-0-2868](http://pentagonus.ru/publ/perspektivnye_sistemy_i_sredstva_radiosvjazi_takticheskogo_zvena_upravlenija_vs_ssha_2018/11-1-0-2868) (дата звернення: 26.08.24).
2. Бабак В. П., Конін В. В., Харченко В. П. *Супутникова радіонавігація*. К.: Техніка, 2004. 328 с.
3. Білий О. А., Шолудько В. Г., Малих В. В., Гай Ю. І. Перспективи розвитку системи супутникового зв'язку ЗС України. *Зб. наук. праць ВІТІ*. 2018. Вип. 2. С. 6—15.
4. Горбенко І. Д., Стасев Ю. В. Безопасность информации в космических системах связи и управления. *Космична наука і технологія*. 1996. 2, № 5/6. С. 64—68.
5. Горбенко І. Д., Стасев Ю. В., Потій А. В., Ткачев А. М. Предложения по обеспечению безопасности информации в единой спутниковой системе передачи информации. *Космична наука і технологія*. 1998. 4, № 5/6. С. 62—66.
6. Горбенко І. Д. *Криптографічний захист інформації*: монографія. Харків: ХНУРЕ, 2016. 356 с.
7. Горностаев Ю. М., Соколов В. В., Невдяев Л. М. *Перспективные спутниковые системы связи*. М.: Изд-во Горячая линия - Телеком, 2000. 132 с.
8. Гришук Р. В., Даник Ю. Г. Синергія інформаційних та кібернетичних дій. *Тр. ун-ту*. 2014. № 6 (127). С. 132—143.
9. Жук А. П., Орел Д. В. Об оценке помехозащищенности спутниковых радионавигационных систем. *Инфокоммуникационные технологии*. 2012. С. 83—88.
10. Замула А. А. Ансамблевые свойства характеристических дискретных сигналов. *Системы обработки информации*. 2013. № 8 (115). С. 213—216.
11. Коркішко Т. А., Мельник А. О., Мельник В. А. *Захист інформації в комп'ютерних і телекомунікаційних мережах. Алгоритми та процеси симетричного блокового шифрування*. Львів: БАК, 2003. 168 с.
12. Лаврич Ю. М., Бистров М. І., Присяжний В. І., Пясковський Д. В. Реалізація технології подвійного використання засобів контролю космічного простору. *Космична наука і технологія*. 2023. 29, № 4. С. 127—140.
13. Макаренко С. И. Использование космического пространства в военных целях. *Системы управления, связи и безопасности*. 2016. № 4. С. 181.
14. Науменко М. І., Стасев Ю. В., Кузнецов О. О., Євсєєв С. П. *Теорія сигнально-кодкових конструкцій*: монографія. Харків: ХУПС, 2008. 541 с.
15. Ніколаєнко Б. А., Пелешок Є. В. *Сучасні супутникові системи зв'язку*. Київ: ІСЗІ КП ім. Ігоря Сікорського, 2022. 146 с.
16. Приходько С. І., Гусєв С. А., Зубенко В. А. Розробка каскадних кодкових конструкцій з покращеними властивостями. *Системы обработки информации*. 2011. № 2 (92). С. 119—128.

17. Руденко В. І., Зінченко М. О., Яковчук О. В., Лазута Р. Р. Модель системи супутникового зв'язку та передачі даних спеціального призначення. *Modern Inform. Technologies in the Sphere of Security and Defence*. 2024. 1(49). С. 45—58.
18. Семко В. В., Бурячок В. Л., Толюпа С. В., Складанний П. М. Модель управління захистом інформації в інформаційно-телекомунікаційній системі. *Вісник Нац. ун-ту «Львівська політехніка». Сер. Радіoeлектроніка та телекомунікації*. 2015. 818. С. 151—155.
19. Смірнов А. А., Сай В. Н., Коваленко А. В. Аналіз перспективних напрямів в удосконаленні радіо систем управління та зв'язку з можливістю множинного доступу. *Системи озброєння і військова техніка*. 2012. № 3 (31). С. 218—226.
20. Стасєв Ю. В., Серов С. С., Дядюн В. О. Умови побудови радіолінії управління безпілотним літальним апаратом в умовах радіoeлектронної протидії. *Системи озброєння і військова техніка*. 2018. № 3 (55). С. 95—99. <https://doi.org/10.30748/soivt.2018.55.13>.
21. Agency leads NATO team in tough cyber exercise. URL: <https://www.ncia.nato.int/NewsRoom/Pages/20190408-Lock-Shields.aspx> (дата звернення: 26.08.24).
22. ETSI TS 125 211 v. 7.2.0 (2007-05). Universal Mobile Telecommunications System (UMTS). Physical channels and mapping of transport channels onto physical channels (FDD). 3GPP TS 25.211 version 7.2.0 Release 7. Route des Lucioles, European Telecommunications Standards Institute, 2007. 55 p. URL: [https://www.etsi.org/deliver/etsi\\_ts/125200\\_125299/125211/07.02.00\\_60/ts\\_125211v070200p.pdf](https://www.etsi.org/deliver/etsi_ts/125200_125299/125211/07.02.00_60/ts_125211v070200p.pdf) (дата звернення: 26.08.24).
23. Fritz D. A., Doshi B. T., Oak A. C., Jones S. D., Burbank J. L., Miller H. L., Oetting J. D., Collins R. M., Gonzalez L. A., Nichols R. A. Military satellite communications: space-based communications for the global information grid. *Johns Hopkins APL technical digest*. 2006. 27. No. 1. P. 32—40.
24. Karpenko O., Kuznetsov A., Sai V., Stasev Yu. Discrete Signals with Multi-Level Correlation Function. *Telecommunications and Radio Engineering*. 2012. No. 1(71). P. 91—98.
25. Kumar R., Taggart D., Monzingo R., Goo G. Wideband gapfiller satellite (WGS) system. *IEEE Aerospace Conf.*, Big Sky, MT, USA, 2005. P. 1410—1417. doi: 10.1109/AERO.2005.1559431.
26. Rice M., Giles T., Wong V., Shakeel I., Mein D. Ground Mobile WGS Satcom for Disadvantaged Terminals. *J. Battlefield Technology*. 2009. 13 (1). P. 13—19.
27. WGS 1, 2, 3 (WGS Block I). Gunter's Space Page, 2023. URL: [https://space.skyrocket.de/doc\\_sdat/wgs-11.htm](https://space.skyrocket.de/doc_sdat/wgs-11.htm) (дата звернення: 26.08.24).

## REFERENCES

1. Aleksandrov S., Turov D. (2018). Advanced systems and means of radio communication tactical management of the US armed forces. *Foreign military review*, No. 11, 42—48. URL: [http://pentagonus.ru/publ/perspektivnye\\_sistemy\\_i\\_sredstva\\_radiosvjazi\\_takticheskogo\\_zvena\\_upravlenija\\_vs\\_ssha\\_2018/11-1-0-2868](http://pentagonus.ru/publ/perspektivnye_sistemy_i_sredstva_radiosvjazi_takticheskogo_zvena_upravlenija_vs_ssha_2018/11-1-0-2868) (Last accessed: 26.08.24) [in Russian].
2. Babak V. P., Konin V. V., Kharchenko. V. P. (2004). *Sputnikova radionavigation*. Kyiv: Tekhnika, 328 p. [in Ukrainian].
3. Biliy O. A., Sholudko V. G., Malikh V. V., Gai Yu. I. (2018). Prospects for the development of the satellite communication system of the Ukrainian satellite system. *Collection of scientific works MITI*, No. 2, 6—15 [in Ukrainian].
4. Horbenko Y. D., Stasev Yu. V. (1996). Security in Space Communication and Control Systems. *Space Science and Technology*, 2, № 5/6, 64—68 [in Russian].
5. Horbenko Y. D., Stasev Yu. V., Potij A. V., Tkachev A. M. (1998). Proposals for ensuring the security of information in a single satellite information transmission system. *Space Science and Technology*, 4, № 5/6, 62—66 [in Russian].
6. Horbenko I. D. (2016). *Cryptographic protection of information*: monograph. Kharkiv: Kharkiv Nat. Univ. of Radioelectronics, 356 p. [in Ukrainian].
7. Gornostaev Yu. M., Sokolov V. V., Nevdyayev L. M. (2000). *Perspective satellite communication systems*. M.: Publ. house Hot line, 132 p. [in Russian].
8. Grischuk R. V., Danik Yu. G. (2014). Synergy of information and cybernetic activities. *Proc. Univ.*, No. 6 (127), 132—143 [in Ukrainian].
9. Zhuk A. P., Orel D. V. (2012). On the assessment of noise immunity of satellite radionavigation systems. *Infocommunication technologies*, No. 2 (10), 83—88 [in Russian].
10. Zamula A. A. (2013). Ensemble properties of characteristic discrete signals. *Scientific and technical J. Inform. processing systems*, No. 8 (115), 213—216 [in Russian].
11. Korkishko T. A., Mel'nyk A. O., Mel'nyk V. A. (2003). *Information Protection in Computer and Telecommunication Networks: Algorithms and Processors of Symmetric Block Encryption*. L'viv: BAK, 168 p. [in Ukrainian].
12. Lavrich Yu. M., Bistrov M. I., Prisyazhny V. I., Pyaskovsky D. V. (2023). Implementation of the technology of underground vibration control of space control. *Space Science and Technology*, 29, No. 4, 127—140 [in Ukrainian].

13. Makarenko S. I. (2016). Use of outer space for military purposes. *Control, communications and security systems*, No. 4, 181 [in Russian].
14. Naumenko M. I., Stasiev Yu. V., Kuznetsov O. O., Yevsieiev S. P. (2008). *Theory of signal-code constructions*: monograph. Kharkiv: Ivan Kozhedub Kharkiv National Air Force University, 541 p. [in Ukrainian].
15. Nikolaenko B. A., Peleshok E. V. (2022). *Current satellite systems communication*: Kyiv: ISZZI KPI im. Igor Sikorsky, 146 p. [in Ukrainian].
16. Prikhodko S. I., Gusev S. A., Zubenko V. A. (2011). Development of cascading code structures with reduced authorities. *Inform. processing systems*, No. 2(92), 119–128 [in Russian].
17. Rudenko V. I., Zinchenko M. O., Yakovchuk O. V., Lazut R. R. (2024). Model of a system for satellite communication and transmission of data for special purposes. *Modern Inform. Technologies in the Sphere of Security and Defense*, No. 1(49), 45–58 [in Ukrainian].
18. Semko V. V., Buryachok V. L., Tolyupa S. V., Folded P. M. (2015). Model for managing the security of information in the information and telecommunications system. *Bull. Nat. Univ. "Lvivska Pol". Ser.: Radioelectronics and telecommunications*, No. 818, 151–155 [in Ukrainian].
19. Smirnov A. A., Sai V. N., Kovalenko A. V. (2012). Analysis of promising directions in advanced radio control systems and connection with the possibility of multiple access. *Armorsystems and military equipment*, No. 3 (31), 218–226 [in Ukrainian].
20. Stasiev Yu. V., Sierov S. S., Diadiun V. O. (2018). Conditions for constructing a radio control line for an unmanned aerial vehicle in conditions of electronic countermeasures. *Armorsystems and military equipment*, No. 3 (55), 95–99 [in Ukrainian].
21. Agency leads NATO team in tough cyber exercise. URL: <https://www.ncia.nato.int/NewsRoom/Pages/20190408-Lock-Shields.aspx> (Last accessed: 26.08.24).
22. ETSI TS 125 211 v. 7.2.0 (2007-05). Universal Mobile Telecommunications System (UMTS). Physical channels and mapping of transport channels onto physical channels (FDD). 3GPP TS 25.211 version 7.2.0 Release 7. Route des Lucioles, European Telecommunications Standards Institute, 2007. 55 p. URL: [https://www.etsi.org/deliver/etsi\\_ts/125200\\_125299/125211/07.02.00\\_60/ts\\_125211v070200p.pdf](https://www.etsi.org/deliver/etsi_ts/125200_125299/125211/07.02.00_60/ts_125211v070200p.pdf) (Last accessed: 26.08.24).
23. Fritz D. A., Doshi B. T., Oak A. C., Jones S. D., Burbank J. L., Miller H. L., Oetting J. D., Collins R. M., Gonzalez L. A., Nichols R. A. (2006). Military satellite communications: space-based communications for the global information grid. *Johns Hopkins APL technical digest*, 27, No. 1, 32–40.
24. Karpenko O., Kusnetsov A., Saj V., Stasiev Yu. (2012). Discrete Signals with Multi-Level Correlation Function. *Telecommunications and Radio Engineering*, No. 1(71), 91–98.
25. Kumar R., Taggart D., Monzingo R., Goo G. (2005). Wideband gapfiller satellite (WGS) system. *IEEE Aerospace Conf.*, Big Sky, MT, USA, 1410–1417. doi: 10.1109/AERO.2005.1559431.
26. Rice M., Giles T., Wong V., Shakeel I., Mein D. (2009). Ground Mobile WGS Satcom for Disadvantaged Terminals. *J. Battlefield Technol.*, 13, No. 1, 13–19.
27. WGS 1, 2, 3 (WGS Block I). Gunter's Space Page, 2023. URL: [https://space.skyrocket.de/doc\\_sdat/wgs-11.htm](https://space.skyrocket.de/doc_sdat/wgs-11.htm) (Last accessed: 26.08.24).

Стаття надійшла до редакції 26.08.2024

Після доопрацювання 25.11.2024

Прийнято до друку 25.11.2024

Received 26.08.2024

Revised 25.11.2024

Accepted 25.11.2024



*Y. Stasiev*, Doctor of Technical Sciences, Prof., Prof. of Department

<https://orcid.org/0000-0002-3893-0313>

*D. Nepokrytov*, Associate Professor

<https://orcid.org/0000-0003-1752-8496>

*M. Parkhomenko*, Candidate of Engineering Sciences (Ph. D.), Associate Professor

<https://orcid.org/0000-0001-6062-7743>

*S. Shylo*, Candidate of Engineering Sciences (Ph. D.), Docent, Associate Professor

<https://orcid.org/0000-0001-5782-552X>

Ivan Kozhedub Kharkiv National Air Force University

77/79 Sumska Str., Kharkiv, 61023 Ukraine

#### A METHOD FOR PROTECTING SPACE COMMUNICATION AND CONTROL SYSTEMS BASED ON DYNAMIC CHANGE OF COMPLEX SIGNAL SHAPES

The experience of operating space systems shows that the effectiveness of such systems significantly depends on the quality of the spacecraft communication and control system. Given that space communication and control systems are accessible to intruders, such systems protect transmitted commands and messages using cryptographic information transformations and special equipment. The algorithms implemented in such systems provide passive protection of the spacecraft control system, where the control equipment refuses to process commands in the presence of powerful interference. Implementation of effective measures is becoming a key component of strategies to protect space communication and control systems, as technological capabilities for attacks on a spacecraft via a radio channel are constantly evolving and becoming more complex. Protection against powerful intentional interference in such systems is carried out using signals with frequency redundancy. The article discusses the method of dynamic change of signal shapes, which enhances the security of information at the physical level. The analysis of interference protection and imitation resistance of space communication and control systems using various systems of complex signals is carried out. The ensemble characteristics of complex signal systems are analyzed. The results of studies of imitation resistance when using different signal systems are presented. It is determined that the implementation of the dynamic mode of operation achieves a gain in comparison with traditional algorithms for protecting space communication and control systems. The conditions for the practical implementation of the dynamic mode of operation of space communication and control systems are formulated. Signal systems are proposed that can provide the solution to the problem of security of information transmission in space communication and control systems at the physical level.

**Keywords:** space communication and control systems, interference protection, imitation resistance, signals with frequency redundancy.