

Вишнівський В.В., д.т.н.; Серих С.О., к.т.н.

ВИЗНАЧЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ СКЛАДНИХ СИГНАЛІВ КАНАЛІВ УПРАВЛІННЯ БЕЗПЛОТНИМИ АВІАЦІЙНИМИ КОМПЛЕКСАМИ

Vyshnivskiy V.V., Serykh S.O. **Determination of indicators of the effectiveness of complex signals of control channels of unmanned aircraft complexes.** The article discusses directions for improving the immunity of signals of control channels of unmanned aircraft complexes using complex signals. In order to implement the adaptation mode, it is proposed to use such devices for forming and processing signals of control channels that are rebuilt on command. This allows you to change: the parameters of a complex signal such as the base of a complex signal, the structure of the signal by pre-selecting it from the general ensemble, to perform a transition from one type of complex signal to another in accordance with the interference situation. These types of signal can be a discrete phase-manipulated signal, a discrete frequency-manipulated signal, i.e. with a pseudo-random frequency adjustment, or a combination thereof.

It was determined that various types of complex signals have excellent capabilities in the fight against intentional jamming, which realize such properties as counteracting the suppression of the signal by jamming and concealment of its transmission to prevent parameter reconnaissance and eliminate the possibility of targeting jamming.

To evaluate the effectiveness of complex signals, the selected indicator is the coefficient of suppression of interference by a complex signal based on the obtained analytical expressions for the values of the dispersion of the interference at the output of the correlation receiver after convolution of the complex signal.

The second indicator of efficiency is the entropy hiddenness of a complex signal, which also varies for different types of signals. Such an indicator determines both energy and structural stealth, which significantly affects the time of exploration of the parameters of a complex signal. A conclusion was made about the expediency of using two parametric efficiency criteria, which comprehensively evaluates the main properties of a complex signal and allows to compare the types of signals for use in modems of the most effective control channels.

Keywords: unmanned aircraft complex, unmanned aerial vehicle, ground control complex, complex signals, control channels, immunity, entropy stealth.

Вишнівський В.В., Серих С.О. Визначення показників ефективності складних сигналів каналів управління безпілотними авіаційними комплексами. В статті розглянуто напрямки підвищення заводо захищеності сигналів каналів управління безпілотними авіаційними комплексами із застосуванням складних сигналів. З метою реалізації режиму адаптації запропоновано використовувати такі пристрої формування і обробки сигналів каналів управління, що за командою перебудовуються. Це дозволяє здійснювати зміну: параметрів складного сигналу такого як база складного сигналу, структуру сигналу попередньо обираючи його із загального ансамблю, виконувати перехід від одного виду складного сигналу до іншого відповідно до заводої обстановки.

Визначено, що різні види складного сигналу мають відмінні здібності в боротьбі із навмисними заводами, які реалізують такі властивості як протидія придушенню сигналу заводою і скритність його передачі для перешкоджання розвідки параметрів і усунення імовірності застосування прицільної заводої.

Для проведення оцінки ефективності складних сигналів обраний показник – коефіцієнт придушення заводої складним сигналом на основі отриманих аналітичних виразів для значень дисперсії заводої на виході кореляційного приймача після згортки складного сигналу. Другим показником ефективності визначено ентропійну скритність складного сигналу, яка також для різних їх видів різниться. Такий показник визначає як енергетичну так і структурну скритність, що суттєво впливає на час розвідки параметрів складного сигналу. Зроблено висновок про доцільність застосування двох параметричного критерію ефективності, який комплексно оцінює головні властивості складного сигналу і дозволяє порівнювати види сигналу для застосуванню в модемах каналів управління найбільш ефективного.

Ключові слова: безпілотний авіаційний комплекс, безпілотний літальний апарат, наземний комплекс управління, складні сигнали, канали управління, заводо захищеність, ентропійна скритність.

Вступ

В умовах ведення бойових дій або підготовки до їх проведення, як показує сучасне становище, важливу роль відіграють безпілотні авіаційні комплекси (БАК) до складу яких входять — безпілотний повітряний апарат, пов'язані з ним пункт дистанційного пілотування або станція наземного керування, лінії керування і контролю та допоміжні елементи. Цей комплекс може охоплювати не один, а декілька безпілотних літальних апаратів.

Незалежно від принципів керування безпілотним літальним апаратом (БПЛА), які поділяють на: безпілотні некеровані, автоматичні, та дистанційно-пілотовані літальні апарати (ДПЛА). До складу БАК організаційно входять один або декілька пілотів, а залежно від призначення та завдання, що ним виконується екіпаж може також включати командира, оператора сенсорів, оператора вогневих засобів. Оцінка ринку безпілотників [1] показує, що саме ДПЛА після 2000 року отримали стрімке розширення за рахунок поширення кола вирішуваних задач. А це в свою чергу висуває значні вимоги до надійності каналів зв'язку, завадозахищеності сигналів каналів управління (КУ).

Зважаючи на складність виявлення БПЛА завдяки зменшенню їх розмірів і значного зниження рівня шуму двигунів вважати це демаскуючою ознакою можливо умовно. Знищення їх стрілецьким озброєнням скоріш випадковість. Застосування артилерійсько-ракетного впливу затратно в порівнянні із вартістю апарата, тобто тієї частини БАК, що найбільш наближена до противника. Більш актуальною в таких умовах альтернативою фізичному знищенню є придушення систем управління апаратом. Адже майже всі БПЛА керується оператором, а команди передаються по радіоканалам, коли випромінювання передавача і є ознакою присутності і демаскує місце знаходження. Таким чином, придушення каналу управління засобами радіоелектронної боротьби (РЕБ) здатне, як мінімум, перешкодити виконанню завдання. У разі обриву каналу зв'язку з оператором найсучасніші БПЛА мають відповідний режим роботи. При втраті сигналу від пульта автоматика повертає апарат у заданий район, де може зробити посадку. У такому випадку система керування ігнорує всі сигнали, а переміщення у вказану зону здійснюється за допомогою супутникової навігації. Використовуючи систему GPS або ГЛОНАСС, літальний апарат може визначити власне положення в просторі, напрям і дальність до оператора або аеродрому та повернутися до нього [2, 5]. Це продовжує життєвий цикл БАК. Щоб запобігти поверненню БПЛА, засоби радіоелектронної боротьби мають придушувати як канал управління, так і сигнали навігаційної системи. Інший режим самоліквідації у випадку приземлення на ворожий території закладено у окремих зразках техніки середньої і малої вартості перш за все тієї, що здійснює розвідку.

У якості доказу можна привести такі приклади. Середня тривалість "життя" безпілотника з нерухомим крилом на полі бою складає близько шести вильотів, звичайного квадрокоптера – лише три вильоти. Інший висновок – дрони як клас БПЛА грають життєво важливу роль передусім для розвідки, а не для ударних місій. Так, якщо у підрозділів без дронів час від виявлення до ураження цілей становить 30 хв. і більше, то наявність БПЛА із радіообміном скорочує його до 3-5 хв. [3, 4].

Таким чином у загальному вигляді підвищення завадозахищеності КУ є важливою і актуальною задачею, а застосування для цього складних сигналів [8] додатково збільшує скритність випромінювання і відповідно БПЛА.

Постановка задачі. Коли розв'язання завдання застосуванням комплексних методів підвищення завадозахищеності КУ неможливе чи обмежене, виникає необхідність використання інших неенергетичних методів, наприклад, сигнально-кодових [6]. Застосування складних сигналів простим екстенсивним шляхом – збільшенням бази сигналу

B_c дозволяє підвищити заводо захищеність КУ. Крім того швидка зміна виду сигналу та його параметрів із реалізацією адаптації до умов заводої обстановки може забезпечити додаткову скритність КУ. Обидва напрямки удосконалення актуальні але їх реалізація складна за умови необхідності реалізації пристроїв формування і обробки складних сигналів із змінними параметрами. Особливістю є те, що різні види складного сигналу володіють відмінною здатністю в забезпеченні заводо захищеності і скритності. Тому вибір більш ефективного в боротьбі із прицільними заводами виду складного сигналу є першочерговою задачею для досягнення визначених властивостей. А підвищення показників ефективності складних сигналів та значення критерію їх оцінки головною метою статті.

Додатковим напрямком слід вважати оцінку реалізації при визначенні моделі пристрою згортки складних сигналів, що дозволить зробити висновки про можливість мінімізувати пристрої формування та обробки сигналів КУ за рахунок програмно апаратного методу керування, зміни їх зворотних зв'язків та використання складеної структури сигналів.

Виклад основного матеріалу досліджень

Рішення завдання по підвищенню заводо захищеності КУ забезпечується завдяки використанню складних сигналів і розробки пристроїв їхньої обробки в модемах КУ [7]. Оптимальність вирішення залежить від вибору ефективного в боротьбі з заводами виду сигналу, визначення способу поєднання сигналів КУ з інформаційним сигналом (ІС), що реалізують найменший взаємний вплив.

Скориставшись розробленою методикою визначення показників ефективності модемів КУ, що наведена у [8] і порівнюючи способи об'єднання КУ із інформаційними каналами (ІК) за розрахованими показниками методики, запропоноване передавання складних сигналів КУ під ІС і розроблена методика визначення що до оптимального співвідношення їхньої потужності [7].

Різноманітність видів складних сигналів [9, 10] ускладнює завдання їхнього вибору. Проте оцінка доцільності їхнього застосування для вирішення конкретної задачі [7, 8, 10] підвищення заводо захищеності КУ, дозволяє зменшити кількість видів складних сигналів, що підлягають дослідженню до наступних - ДФМС, ДЧМС, ДЧДФМС [8]. Це пояснюється відносною простотою реалізації пристроїв їхнього формування і обробки, а головне, при використанні складової структури, простоті зміни виду сигналу за рахунок трансформації складового складного ДФМС в ДЧДФМС і ДЧМС відповідно, завдяки зміні параметрів, наприклад B_c у відповідності до умов заводої обстановки. Разом з тим ефективність їхнього використання в боротьбі з заводами не однакова і потребує оцінки за обґрунтовано обраними показниками.

Для вирішення завдань дослідження по підвищенню заводо захищеності каналів управління модемів КУ в БПЛА особливе значення відведено вибору виду складного сигналу, що повинен забезпечити максимальну заводостійкість і скритність передачі команд при простоті реалізації пристроїв формування і обробки сигналу, як початкової дії - синтезу. Для отримання кількісної оцінки ефективності необхідно застосовувати показники, що визначають головні властивості сигналів в боротьбі з заводами. Це відповідає меті дослідження.

Так як здатність опиратись дії потужних навмисних завод це властивість і головна вимога до сигналів КУ та до їхніх модемів, то крім апріорно відомих параметрів завод і сигналів необхідні відомості про [10, 11, 13] структуру самого складного сигналу. До того ж показник ефективності повинен оцінювати додаткову властивість сигналу – розвід захищеність, тобто враховувати такі параметри сигналу, які визначають їхню

енергетичну і структурну скритність [11]. Це дозволяє виключити з аналізу види складних сигналів з малою чи обмеженою в реалізації B_c , наприклад, сигнали Баркера [9] короткої довжини аперіодичної псевдовипадкової послідовності (ПВП). Щоб визначитись з показниками ефективності сигналів розглянемо загальну модель приймача складного сигналу [11] рис.1.

Модель складається з перемножувача, ідеального смугового узгодженого фільтра (УФ) і демодулятора сигналу керування.

$$S_{\Sigma}(t) = S_c(t) + S_{\Sigma_3}(t)$$

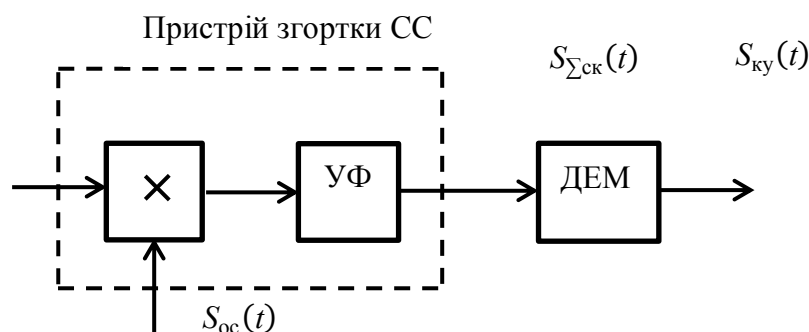


Рис. 1 Модель приймача складного сигналу

Перемножувач та УФ виконують операцію згортки складного сигналу $S_c(t)$, що потрапляє до входу приймача на частоті f_c разом з сумарною завадою - $S_{\Sigma_3}(t)$. Остання - це адитивна суміш навмисної завади потужності P_3 на частоті завади f_3 від постановника її та взаємної завади у вигляді ІС з потужністю P_{ic} , що передається над сигналом КУ в смузі ΔF_c , і флуктуаційного шуму. Шум апроксимується гаусовським випадковим процесом з нульовим середнім і рівномірною спектральною щільністю потужності N_0 . На інший вхід перемножувача поступає опорний сигнал $S_{oc}(t)$ частотою f_{oc} . В результаті множення $S_{\Sigma}(t)$ і $S_{oc}(t)$ трапляється стиснення спектру сигналу в $\Delta F_c / \Delta F_{ky}$ разів та виділення його на частоті - $f_p = f_c \cdot f_{oc}$.

Якщо СФ з імпульсною характеристикою - $h(t)$ в моделі рис. 1 має прямокутну АЧХ в смузі $\Delta F_{сф} = \Delta F_{ky}$, де ΔF_{ky} смуга сигналу КУ, то швидкість передачі команд R_{ky} узгоджена з ΔF_{ky} . Тоді передаточну функцію $K(f)$ фільтра можна записати:

$$K(f) = \int_{-\infty}^{\infty} h(t) e^{-j2\pi ft} dt = \begin{cases} 1, \text{ при } f \in (f_p \pm \Delta F_{ky}) \\ 0, \text{ при інших } f \end{cases} \quad (1)$$

Відомо [9], що завадостійкість модемів складних сигналів в умовах флуктуаційного шуму не залежить від виду сигналу і визначається:

$$h_{ш}^2 = \frac{E_c}{N_0} = \frac{P_c T_c}{P_{ш} / \Delta F_c} = (P_c / P_{ш}) B_c.$$

Помилково рахувати, що при $E_c = const$ збільшенням B_c можливо досягти зменшення $Q_{пкy}$ (підвищення $h_{ш}^2$), бо з розширенням ΔF_c пропорційно зростають шуми на вході демодулятора рис 1. А от в боротьбі з навмисними завадами і взаємною завадою від ІС це

дійовий спосіб [12, 13], що забезпечує досягнення значного рівня заводозахищеності КУ. При цьому вплив взаємної завади з відомими параметрами доцільно усувати компенсаційними методами боротьби з апріорно відомою заводою [9, 11]. Тому оцінку заводозахищеності прийому складних сигналів належить в першу чергу проводити по відношенню до імовірних найгірших навмисних завод, які складно прогножуються. Це дозволить визначитись з розміром B_c для конкретного виду складного сигналу для одночасної боротьби з навмисними заводами та ІС.

Так як операція згортки складного сигналу властива будь-якому пристрою їхньої обробітки [9], то модель рис.1 є узагальненою. Це дозволяє ввести також загальний показник ефективності - мінімальний коефіцієнт придушення навмисної завади за рахунок використання складного сигналу β_{min} [12]:

$$\beta_{min} = \frac{(P_3/P_c)_{вх}}{(P_3/P_c)_{вих}}, \quad (2)$$

де: $(P_3/P_c)_{вх}$ и $(P_3/P_c)_{вих}$ – відношення потужності завади-сигнал на вході перемножувача і виході СФ відповідно. В подальшому для стислості β_{min} - мінімальний коефіцієнт придушення завади. Ефективним буде сигнал з найбільшим β_{min} при однакових параметрах $(P_3/P_c)_{вх}$, ΔF_c , $\Delta F_{ку}$ сигналів, що порівнюються, а завади найнебезпечні для нього. На відміну від показника B_c , кращим в оцінці заводозахисту є β_{min} , бо дозволяє реально оцінювати ефективність складних сигналів безпосередньо в боротьбі з потужними навмисними заводами, як головною властивістю, що визначена метою дослідження.

Але застосування одного показника має недолік. Він полягає в наступному. При дії прицільних завод, співпадаючих з сигналом за усіма параметрами, включаючи структуру, оцінка ефективності втрачає сенс бо у цьому випадку $\beta_{min}=1$. Усунути недолік можна за рахунок використання додаткового показника, що визначає розвідзахищеність складного сигналу.

Для використання прицільної завади постановником завод імовірність розвідки параметрів сигналу Q_p повинна дорівнювати одиниці. На Q_p суттєво впливає скритність сигналу. З трьох складових скритності - енергетичної, структурної, інформаційної [8], перші два залежать від параметрів сигналу і визначають ентропійну скритність радіопередачі H_2 [10]. Інформаційна скритність досягається передачею формалізованих команд і на вибір сигналу не впливає.

Структурна скритність - це скритність множини змінних параметрів сигналу, що визначається:

$$H_A = -\sum_{i=1}^N Q(a_i) \log(a_i), \quad (3)$$

де $Q(a_i)$ - імовірність вибору для передачі деякого значення параметра a_i , з повної множини $\{a_i\}$, $i=1,2,\dots,N$ - ансамблю складного сигналу N .

Величину H_A з (3) можна розглядати як мінімально необхідне середнє число двійкових вимірювань або проб з рівно імовірними наслідками для розкриття невизначеності H_A , тобто [11], структур сигналів з N . Чим вище B_c , тим більше об'єм ансамблю сигналів. Не всі структури з N ефективні, тому потрібна розробка методики визначення раціонального об'єму ансамблю складного сигналу за рахунок оптимізації їхньої структурної складової, що є подальшим завданням дослідження.

Енергетична скритність - H_E характеризує ступінь невизначеності енергетичних параметрів складного сигналу КУ, що маскується завдяки передачі під ІС:

$$H_E = - \sum_{i=1}^N Q(a_i) \sum_{j=1}^N Q(a_j/a_i) \cdot \log(a_j/a_i), \quad (4)$$

де $Q(a_j/a_i)$ - умовна імовірність реєстрації структури складного сигналу a_j з ансамблю N , при передачі a_i , на яку впливають енергетичні показники визначені спектром складного сигналу. Оптимізація спектру складного сигналу КУ - це окреме завдання дослідження. Загальна H_Σ :

$$H_\Sigma = H_A H_E. \quad (5)$$

Методика визначення ефективності складного сигналу за показником скритності не обмежується розрахунком H_Σ за (5), H_A , H_E за (3), (4) відповідно і потребує додаткового дослідження N . Чим більше N , тим вище скритність. Але не всі сигнали з N доцільно використовувати. Потрібно провести визначення раціонального об'єму з ансамблю складних сигналів з гарними взаємкореляційними властивостями.

Проведений аналіз вибраних для підвищення заводо захищеності КУ складних сигналів [10] показує, що найбільш ефективним в боротьбі з навмисними завадами за показником β_{min} слід вважати ФМ ШПС [9, 11]. Але зважаючи на стрімкий розвиток засобів РЕБ і збільшення їх можливостей для розвідки параметрів і придушення сигналів для вибору ефективного виду сигналів із розглянутих слід на другому етапі дослідити їхню скритність саме за показником H_Σ , а раціональний вибір виду складного сигналу проводити відповідно по двох параметричному критерію $K = \{\beta_{min}, H_\Sigma\}$. Зміна режимів роботи КУ в напрямку підвищення його заводо захищеності - адаптація до зовнішніх впливів досягається збільшенням Бс. Тому при розгляді можливості реалізації слід враховувати яке максимальне значення цього параметру може забезпечити пристрій згортки вибраного виду сигналу і доцільність застосування складеної структури складного сигналу. При наближенні до реалізаційної межі бази ФМ ШПС подальше збільшення Бс досягається завдяки стрибкам по частоті, тобто застосуванням ППРЧ, що вказує на зміну виду сигналу, тобто перехід до застосування ППРЧ ФМ ШПС. На третьому етапі доцільно розглянути можливість сумісного передавання сигналів різних КУ в загальній смузі частот. Для розподілу сигналів доцільно використовувати структурну відмінність, а пріоритетність забезпечити зміною потужності при витриманні раціонального співвідношення сигналу КУ і ІС. Все це вказує на можливість розробки окремої методики вибору складного сигналу для реалізації адаптивної роботи пристроїв формування і обробки складних сигналів в БПЛА при використанні супротивником засобів РЕБ для придушення КУ і ІС. Доцільно також розглянути можливість застосування компенсаційних методів в окремих демодуляторах інформаційних і командних сигналів.

Висновки

Таким чином, аналіз ефективності сигналів доцільно проводити по двухпараметричному критерію $K = \{\beta_{min}, H_\Sigma\}$, який дозволить оцінити головні властивості складного сигналу КУ та обрати ефективний сигнал для боротьби з завадами. Для модему складного сигналу КУ заводо є навмисна завада і ІС. Для оцінки ефективності складного сигналу в боротьбі з кожною заводою потрібне окреме визначення β_{min} , бо структури завод і відповідно їхній вплив відрізняються. Доцільно при подовженні досліджень розробити методику оцінки і вибору складного сигналу КУ при передачі його під ІС.

Список використаної літератури:

1. БПЛА. Практические рекомендации. Защита элементов. [Електроний ресурс] (жовтень 2021 р.)
2. Новини ВПК. Матеріали спеціалізованої виставки UMEX-2018. Українські тактичні безпілотники зацікавили іноземних клієнтів [Електронний ресурс] // - Режим доступу: <http://milnavigator.com.ua>.

2. Слюсар В. М. (2013). Радиолінії зв'язу с БПЛА: приклади реалізації.. *Електроніка: наука, технологія, бізнес.* – 2010. - № 5. с. С. 56 – 60.
3. Перший народний комплекс БПЛА - People's Project.com [https:// \[Електронний ресурс\] //](https://peopleproject.com/pershij-narodnij-kompleks-bpla/) - Режим доступу: [http:// www.peoplesproject.com/pershij-narodnij-kompleks-bpla](http://www.peoplesproject.com/pershij-narodnij-kompleks-bpla).
4. Слюсар, В.И. Система досліджень НАТО по розвитку нелетального озброєння.. *Зб. матеріалів VI міжнародної науково-практичної конференції “Проблеми координації воєнно-технічної та оборонно-промислової політики в Україні. Перспективи розвитку озброєння та військової техніки”*. – Київ. 2018.- С. 306 – 309.
5. Комбінована система захищеного радіоуправління функціями БПЛА. Національний авіаційний університет. [Електронний ресурс] // - Режим доступу: <https://nau.edu.ua/ua/menu/science/naukovi-rozrobki/kombinovana-sistema-zahishchenogo-radioupravlinnya-funktsiyami-bpla.html>
6. Толюпа С.В. Підвищення ефективності систем радіозв'язу із OFDM за рахунок визначення оптимальних сигнально-кодових конструкцій. / С.В. Толюпа, В.С. Наконечний, Н.В. Цюпа // ЗВ'ЯЗОК. –2014. – № 3. – С. 37-40.
7. Серих С.О. Підвищення завадозахищеності каналів управління комплексів безпілотних літальних апаратів/ В.В. Вишнівський, С.О. Серих, Ю.І.Катков// Наукові записки УНДІЗ. – 2018. – №1(49).-С.23-30.
8. Серих С.О. Проблеми завадостійкості радіоліній з складними сигналами в умовах активних завад. // ЗВ'ЯЗОК. –2013. – № 4. – С. 32-37.
9. Серих С. О. Оцінка можливостей постановників завад та впливу їх енергетичних показників на функціонування засобів зв'язу / С.О.Серих, Ю.І. Катков // Сучасний захист інформації. - 2017. – №1. – С. 66-72.
10. Серих С.О. Скриптість повідомлень в мережах із радіодоступом та напрямки її підвищення / С.О. Серих // Сучасний захист інформації. – 2015. - №2. – С. 77-83.
11. Серых С.А. Методика выбора составных широкополосных сигналов для мобильных систем CDMA/ С.А. Серых, В. Р. Соловьев, О.В. Кокотов // Вісник ДУІКТ.- 2009. -№ 2.- С.112-117.
12. Tamil Esher (12 січня 2017). Diesel-Powered Drone Set Endurance Record (56 Hour Mission) for Small UAS. Defense Update. Архів оригіналу за 18 січня 2017. [Електронний ресурс]// - Режим доступу: [http://web.archive.org/web/20170118221638 /http://defenseupdate.com /20170112 _vanilla-uav.html](http://web.archive.org/web/20170118221638/http://defenseupdate.com/20170112_vanilla-uav.html).

Автори статті

Вишнівський Віктор Вікторович - доктор технічних наук, професор, завідувач кафедри Комп'ютерних наук Державний університет телекомунікацій, Київ, Україна.

Серих Сергій Олександрович - кандидат технічних наук, доцент, доцент кафедри Комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Vyshnivskiy Viktor Viktorovich – Sciences of Doctor (technic), professor, Head of the Department of Computer Science, State University of Telecommunications, Kyiv, Ukraine.

Sierykh Serhii Oleksandrovych – Candidate of Science (technic), associate professor of the Department of Computer Science, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 14.01.2022 р.

Рецензент: д.т.н., проф. В.Ф. Заїка