УДК 621.391 DOI: 10.30748/soivt.2018.56.08

А.В. Северілов, В.В. Васьковський, В.М. Волосенко, І.А. Шуварін

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

АНАЛІЗ АНАЛОГОВИХ МЕТОДІВ СКРЕМБЛЮВАННЯ, ЩО ЗАСТОСОВУЮТЬСЯ В СИСТЕМАХ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ

У роботі проведено аналіз аналогових методів скремблювання, які використовуються в системах військового ультракороткохвильового радіозв'язку, а саме: частотна інверсія сигналу, розбиття смуги частот мовного сигналу на декілька піддіапазонів, розбиття сигналу на мовні сегменти і їх перестановки в часі. Розглянуто принципи функціонування та показано основні переваги та недоліки наведених методів аналогового скремблювання. Проведено аналіз якості розбірливості відновленого мовного повідомлення в залежності від рівня сигнал / шум в каналі радіозв'язку та способу обраного методу аналогового скремблювання.

Ключові слова: *радіозв'язок, аналогове скремблювання, інверсія, часовий інтервал, несанкціонований спостерігач, шифрування, смуга частот.*

Вступ

Постановка проблеми. Досвід проведення Операції об'єднаних сил (ООС) свідчить про те, що основною складовою системи управління військами в тактичній ланці управління залишається система ультракороткохвильового (УКХ) радіозв'язку [1], особливо на глибині взводний опорний пункт – ротний опорний пункт. Особливо це є актуальним у випадках, коли бойова обстановка не дозволяє розгорнути проводові лінії зв'язку. При цьому часто виникає потреба забезпечити захист інформації, що передається в мережах УКХ радіозв'язку. Це пов'язано насамперед з тим, що підрозділи радіоелектронної розвідки противника здійснюють постійний моніторинг радіоефіру. Це дозволяє здійснювати ефективне перехоплення мовної інформації та нейтралізацію всієї системи зв'язку, зокрема системи УКХ радіозв'язку. За даними розвідки в армії РФ дуже ефективно застосовуються комплекси радіоелектронної боротьби (РЕБ) "Борисоглібськ-2" та "Торн". Комплекс "Борисоглібськ-2" був зафіксований в Луганській області та в самому Луганську взимку 2015 року. Комплекс РЕБ "Торн" [2] був зафіксований біля Донецького аеропорту у 2015 році.

Аналіз останніх досліджень і публікацій. Аналіз літератури [3–4] свідчить, що безпека зв'язку при передачі мовних повідомлень базується на використанні великої кількості різних методів шифрування повідомлень, що змінюють властивості повідомлення таким чином, що воно стає незрозумілим та, відповідно, недоступним для несанкціонованого спостерігача, що здійснює моніторинг радіоканалу. Порядок реалізації методів шифрування мовного повідомлення обирається в залежності від конкретних завдань, що покладені на систему передачі інформації та особливостей побудови технічного каналу передачі даних [3].

Найбільш розповсюдженим та бюджетним методом, що забезпечує захищену передачу мовних повідомлень в системах УКХ радіозв'язку можна вважати скремблювання [5]. Це процес частотного та часового перетворення мовного сигналу на передавальній стороні для того, щоб зробити це повідомлення незрозумілим на приймальній стороні. Необхідною властивістю такого перетворення є зворотнє перетворення для відновлення мовного повідомлення на приймальній стороні.

Тому **метою роботи** є аналіз існуючих методів скремблювання, що застосовуються в системах УКХ радіозв'язку.

Виклад основного матеріалу

На сьогоднішній день можна виділити два напрямки шифрування мовних сигналів – це скремблювання аналогових сигналів та перетворення мовного повідомлення в дискретний вигляд з подальшим шифруванням [6]. Аналогові скремблери перетворюють вихідний мовний сигнал (без переведення його в цифрову форму) таким чином, щоб при прослуховуванні радіоканалів за допомогою радіостанцій, що не оснащені подібними пристроями, були створені суттєві труднощі для розбірливості переданої інформації [4]. При цьому при скремблюванні перетворений мовний сигнал, що володіє властивостями нерозбірливості і невпізнанності, займає таку ж смугу частот спектра, що і вихідний сигнал. У цифрових пристроях захисту інформації мовні компоненти перетворюються в цифровий потік даних і

змішуються з деякою псевдовипадковою послідовністю, що виробляється ключовим генератором [7]. Сформоване таким способом мовне повідомлення з передавальної сторони через лінію радіозв'язку потрапляє до приймальної сторони, де за допомогою однакових алгоритмів здійснюється дескремблювання мовного повідомлення.

Основними технічними характеристиками скремблерів, які необхідно оцінювати при виборі конкретного типу пристрою захисту інформації, є [6–8]: рівень шифрування інформації, залишкова розбірливість, якість відновлення сигналу, вплив на параметри радіостанцій, рівень технічного виконання (маса, габарити, споживання електроенергії, можливість встановлення в різні типи станцій і т. п.), вартість.

Найбільш важливою характеристикою скремблера є ступінь шифрування повідомлення [8]. Однак, необхідно пам'ятати, що дане поняття носить умовний характер через те, що на даний момент відсутні будь-які керівні документи, що регламентують це визначення.

Разом з тим, умовно можна розділити всі пристрої захисту інформації на засоби захисту інформації від ненавмисного перехоплення [4] (тобто від прослуховування особами, які не використовують спеціальні засоби перехоплення чужих переговорів) і засоби захисту інформації від несанкціонованого доступу [5–6] (тобто від прослуховування можливими конкурентами, метою яких є саме перехоплення чужих переговорів, і оснащених для цього спеціальними технічними засобами). Звичайно, що засоби захисту інформації від несанкціонованого доступу, в свою чергу, можна розділити на кілька рівнів, що забезпечують різний рівень захисту переговорів в залежності від ступеня оснащеності противника. У літературі [3] часто зустрічається класифікація пристроїв захисту інформації за часом дешифрування інформації після її запису. Однак така класифікація більше підходить для складних криптографічних систем, а не для мереж УКХ радіозв'язку де небезпеку становить, як правило, тільки перехоплення переговорів в реальному масштабі часу. Тому в якості критерію рівня закриття інформації для засобів УКХ радіозв'язку більш доцільно використовувати залишкову розбірливість повідомлення та вартість технічних засобів, що забезпечують перехоплення повідомлень в реальному масштабі часу.

Під залишковою розбірливістю [6] розуміють міру можливості відновлення мовного повідомлення при його прослуховуванні за допомогою технічних засобів, не обладнаних даним типом пристрою захисту інформації. Певною мірою залишкова розбірливість є складовою частиною характеристики рівня закриття інформації, однак, залишкова розбірливість характеризує ступінь нерозбірливості повідомлень при їх прослуховуванні без застосування спеціальних засобів. Рівень закриття інформації показує захищеність переговорів і при навмисному перехопленні з використанням спеціальної апаратури. Кількісно залишкова розбірливість може бути оцінена відсотком відновлених фрагментів повідомлення при прослуховуванні переговорів за допомогою радіозасобів, не оснащених даним типом пристроїв захисту інформації [4; 7]. Слід відзначити, що найбільший ступінь захисту інформації забезпечують скремблери з мінімальною залишковою розбірливістю [5]. Слід, однак, відзначити, що практично всі відомі аналогові мовні скремблери не в змозі в повному обсязі позбавитись розбірливості. В закодованому скремблером мовному повідомленні зберігається інформація про швидкість та особливості мовного повідомлення. Тому, несанкціонований спостерігач має змогу ідентифікувати (в залежності від наявності відомостей про тематику переговорів, що ведуться) від 10 до 50% інформації, що передається [8].

Якість відновлення мовного повідомлення є найважливішим тактико-технічним показником скремблера [6]. Даний показник вираховується спираючись на процентне співвідношення спотвореного повідомлення до загального об'єму повідомлення. Як правило, він виражається через розбірливість відновленої мови. Допустимою якістю відновленого повідомлення вважається, коли на приймальній стороні може бути ідентифікований голос особи, що передавала повідомлення, та інформаційна складова.

Крім того, слід відзначити, що вплив скремблерів на параметри радіостанцій проявляється, перш за все, в погіршенні чутливості приймача за рахунок зменшення співвідношення сигнал / шум на вхідному колі приймача [3; 5; 8].

По друге, під час часового скремблювання мовного повідомлення, необхідно забезпечити заданий часовий інтервал для здійснення синхронізації скремблерів на передавальній та приймальній стороні. А це суттєво збільшує сеанс радіообміну за часом.

По третє, за рахунок зменшення залишкової розбірливості відбувається погіршення, як якості відновлення сигналу, так і технічних параметрів радіостанцій.

Для портативних засобів УКХ радіозв'язку військового призначення відіграє суттєву роль спосіб конструктивної реалізації скремблерів. Оскільки конструктивно скремблери уявляють собою малогабаритні мікроелектронні вузли, які встановлюються всередину корпусу радіостанції, кращий вибір для аналогових пристроїв захисту інформації є пристрої з мінімальними габаритами і енергоспоживанням [4]. Звичайно, що мінімізація габаритів дозволяє розширити можливість застосування скремблерів, а тому

забезпечується можливість їх установки в більшу кількість радіозасобів.

Підрозділи Збройних Сил України, як правило, оснащаються професійними засобами УКХ радіозв'язку зарубіжних виробників таких, як Motorola, Kenwood, Icom та ін. [9], які мають можливість використовувати аналогові види модуляції мовного повідомлення (частотні або фазові).

Для подібного роду радіозасобів, в переважній більшості, в якості пристроїв захисту інформації теж застосовуються аналогові мовні скремблери.

Перетворення сигналу в аналогових скремблерах здійснюється в спектральній або в часовій області. Для малогабаритних скремблерів, що застосовуються в УКХ радіостанціях, найчастіше використовуються такі види перетворення сигналу [4; 10]:

– частотна інверсія сигналу;

– розбиття смуги частот мовного сигналу на кілька піддіапазонів (зазвичай на два) і частотна перестановка в кожному піддіапазоні відносно середньої частоти піддіапазону;

– сепарація смуги частоти мовного повідомлення на декілька піддіапазонів і їх частотні перестановки;

– розбиття сигналу на мовні сегменти і їх перестановки в часі.

По режиму роботи аналогові пристрої захисту інформації можуть являти собою як статичні системи, параметри перетворення сигналу, в яких залишаються незмінними протягом всієї передачі мовного повідомлення, так і динамічні системи, в яких параметри перетворення змінюються в часі (наприклад, зміна швидкості розбивки смуги мовного сигналу з певною періодичністю) [11].

Частотна інверсія є найпростішим видом аналогового скремблювання [10]. В такому скремблері (частотному інверторі) здійснюється перетворення мовного спектру, що дорівнює повороту частотної смуги мовного сигналу навколо визначеного частотного значення [8], що виступає в якості деякого ключа системи. При цьому досягається ефект перетворення низьких частот у високі (високих у низькі). Вказаний підхід не забезпечує достатнього рівня закриття інформації, тому що при перехопленні легко встановлюється номінал частоти, відповідно середньої точці інверсії в смузі спектра мовного повідомлення [10].

Практично для здійснення несанкціонованого прослуховування радіопереговорів досить мати аналогічну радіостанцію з можливістю підбору частоти інверсії. Крім цього, слід зазначити, досить високу залишкову розбірливість скремблерів з частотною інверсією. Разом з тим, частотні інвертори володіють максимальною якістю відновлення сигналу [11] і практично не погіршують розбірливість мови.

Деяке підвищення рівня закриття інформації забезпечує скремблер з розбивкою смуги мовного сигналу на піддіапазони з частотною інверсією мовного повідомлення в кожному піддіапазоні (смуго-зсувний інвертор) [12]. При цьому в якості ключа системи виступає точка розбиття. Однак, і такий спосіб аналогового скремблювання не забезпечує надійного закриття інформації і має досить високу залишкову розбірливість. Так само, як і у випадку частотної інверсії, для перехоплення переговорів досить мати радіостанцію, оснащену аналогічним скремблером, з можливістю підбору частоти розбивки сигналу.

Процес скремблювання на основі так званих однорідних перестановок мовних вибірок описується виразом [9]:

$$s = (k_1 \times r) \bmod N, \qquad (1)$$

де k_1 – таємний ключ, що є взаємно простим з N; N – число відліків мовного повідомлення у часовому кадрі мовного повідомлення; r – номер всередині початкового кадру; s – номер відліку всередині кадру, що скремблюється.

Процес дескремблювання здійснюється згідно відношення:

$$r = (k_2 \times s) \bmod N, \qquad (2)$$

де k_2 – таємний ключ, який є зворотною величиною k_1;

$$k_2 = k_1^{-1} \bmod N. \qquad (3)$$

Смугові скремблери [6; 8; 11], що використовують спосіб розбиття смуги мовного сигналу на кілька піддіапазонів з частотними перестановками цих піддіапазонів володіють приблизно тими ж характеристиками по рівню закриття інформації та залишкової розбірливості, як і смуго-зсувні інвертори. У даному випадку ключем системи є кодова комбінація перестановки частотних смуг.

Додаткове підвищення рівня закриття інформації забезпечується зміною параметрів перетворення сигналу в часі (динамічні скремблери) [3; 10]. Для способів частотного перетворення сигналу такими ключовими параметрами можуть бути частота інверсії (для частотного інвертора), частота розбиття смуги сигналу (для смуго-зсувного інвертора) та комбінація частотної перестановки піддіапазонів сигналу (для смугового скремблера). При цьому рівень захисту визначається кількістю параметрів мовного повідомлення, що підлягає перетворенню [12], а саме: довжиною ключа, тобто числом можливих комбінацій параметра та швидкістю зміни параметра.

Теоретично для перехоплення повідомлень в реальному масштабі часу в каналах зв'язку, захищених за допомогою скремблерів з параметрами перетворення, що змінюються в часі, необхідно застосу-

вання спеціальних технічних засобів, що дозволяють спочатку визначити ключову послідовність (тобто правила зміни параметрів перетворення мовного повідомлення), а потім підлаштуватися під знайдену ключову послідовність. Разом з тим, практично для всіх типів скремблерів з динамічно змінюваними параметрами перехоплення переговорів може проводитися більш простими методами [10-12].

Динамічні скремблери [12], як правило, істотно дорожчі за скремблери з фіксованими параметрами перетворення сигналу, сильніше впливають на характеристики радіозасобів та вимагають початкової синхронізації, що обмежує їх застосування для багатьох сфер використання.

Поряд з частотними, в аналогових скремблерах можуть бути застосовані часові перетворення сигналу. Найпростішим видом часового перетворення є часова інверсія [11], суть якої полягає в розбитті мовного повідомлення на декілька сегментів кожен з них передається в зворотному порядку.

Ще одним шляхом підвищення рівня захищеності сигналу, що підлягає скремблюванню є перестановка сегментів мовного сигналу в рамках фіксованого кадру в часовій площині [6]. Ключове значення задає алгоритм, за яким відбувається перестановка. Залишкова розбірливість залежить від тривалості відрізків мовного повідомлення і кадру, яка зі збільшенням останнього зменшується.

Зменшення часу затримки може бути отримано шляхом використання скремблера з перестановкою часових сегментів зі змінним вікном [6; 9].

В даному випадку кількість варіантів перестановок сегментів штучно обмежено верхнім граничним максимальним значенням. Тобто кожен сегмент вихідного повідомлення має визначений часовий інтервал, в межах якого відрізок може зміщуватись при скремблюванні. Визначений часовий інтервал змінюється по мірі надходження кожного нового сегмента повідомлення. Слід зазначити, що існують й інші більш складні види аналогового скремблювання такі, як основані на використанні швидкого перетворення Фур'є [10], різні комбінації часового і частотного перетворення і т.д. [7]. Однак, вони поки не знайшли широкого застосування в засобах УКХ радіозв'язку, через складність їх апаратної реалізації в заданих габаритах, великим енергоспоживанням та великою вартістю.

З метою аналізу різноманітних варіантів скремблювання проведено імітаційне моделювання, результати якого наведено на рис. 1.

На рис. 1 наведено графіки, що характеризують якість розбірливості відновленого мовного повідомлення в залежності від рівня сигнал/шум в каналі радіозв'язку та способу обраного аналогового скремблювання [6].

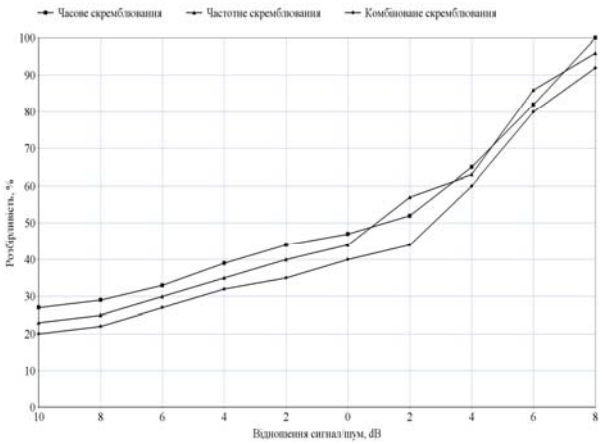

Рис. 1. Якість залишкової розбірливості відновленого мовного повідомлення

З аналізу результатів, наведених на рисунку, видно, що найбільшу залишкову розбірливість має мовне повідомлення, оброблене за допомогою методу часового скремблювання. А найменшу розбірливість має повідомлення оброблене за допомогою методу комбінованого (частотно-часового) скремблювання. Дану залежність необхідно врахувати під час організації системи військового УКХ радіозв'язку.

Висновки

Проведений аналіз аналогових методів скремблювання свідчить про те, що даний підхід широко впроваджується в системах радіозв'язку з метою шифрування (закриття) мовної інформації, що є особливо актуальним у тих засобах радіозв'язку, що застосовуються у військових цілях.

Застосування аналогових методів скремблювання має свої переваги та недоліки. До переваг можна віднести відносну простоту апаратної реалізації та відповідно невелику вартість даного підходу в порівнянні із цифровими методами скремблювання. Суттєвим недоліком слід вважати недостатню ступінь закриття інформації та збільшення часу затримки передачі повідомлення під час радіообміну.

Перевагами з точки зору залишкової розбірливості характеризується комбіноване скремблювання, яке полягає в сумісному використанні часового та частотного скремблювання.

Але у цього методу значно більша вартість та складність реалізації ніж у часового або частотного скремблювання. Таким чином, при здійсненні вибору методів шифрування інформації слід враховувати задачі, які буде виконувати система радіозв'язку та наявність ресурсів.

Список літератури

1. Кушнір О.І. Аналіз впливу "гібридної" війни на розвиток автоматизованої системи управління авіацією та ППО Збройних Сил України / О.І. Кушнір, О.П. Давикоза, Ю.Ф. Кучеренко // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – № 2(27). – С. 116-120. https://doi.org/10.30748/nitps.2017.27.22.

2. Кузнецов М. Російські засоби РЕБ у бойових діях на Донбасі [Електронний ресурс] / М. Кузнецов // Informnapalm. – 2018. – № 1. – С. 1-3. Режим доступу: www.informnapalm.org/ua/rosijski-zasoby-reb-na-donbasi/.

3. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – К.: Вид. МК-Пресс, 2005. – С. 191-205.

4. Jayakurami J. A review of analog speech scrambling for secure communication / J. Jayakurami, G. Dhanya // Progress in science and engineering research journal. – 2016. – Vol. 2. – P. 194-198.

5. Lim Y.C. Quality analog scramblers using frequency-response masking filter banks circuits / Y.C. Lim, J.W. Lee, S.W. Foo // Syst. Signal Process. – 2010. – Vol. 29. – P. 135-154.

6. Jayakurami J. An efficient voice scrambling technique for next generation communication systems / J. Jayakurami, G. Dhanya // International Journal of Engineering and Technology. – 2016. – Vol. 8, No. 1. – P. 293-299.

7. Andrade J.F. Speech privacy for modern mobile communication systems / J.F. Andrade, M. Campos, J.A. Apolinario // Acoustics, Speech and Signal Processing. – 2008. – P. 177-178.

8. Lin K.T. Hybrid encoding method by assembling the magic matrix scrambling method and the binary encoding method in image hiding // Optics Communications. – 2011.Vol. 284, No. 7. – P. 1778-1784.

9. Климович О.К. Визначення перспективних технологій в системах радіозв'язку та транкінгового зв'язку для подальшого використання в Збройних Силах України / О.К. Климович, О.О. Лаврут, С.О. Івко // Збірник наукових праць ОНАЗ. – 2016. – №2(6). – С. 30-35.

10. Sattar B.A. Proposed Speech Scrambling Based on Wavelet Transform and Permutation / B.A. Sattar // 3th International Conference on Systems, signals and Devices, SSD'05, March 21-24, 2005, Sousse, Tunisia.

11. Lee J.W. Efficient fast filter bank with a reduced delay / J.W. Lee, Y.C. Lim // Circuits and Systems. – 2008. – P. 1430-1433.

12. Wu Y. NPCR and UACI randomness tests for image encryption / Y. Wu, J. Noonan, S. Agaian // Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications. – 2011. – № 1(2). – P. 31- 38.

References

1. Kushnir, O.I., Davykoza, O.P. and Kucherenko, Yu.F. (2017), "Analiz vplyvu "hibrydnoi" viiny na rozvytok avtomatyzovanoi systemy upravlinnia aviatsiieiu ta PPO Zbroinykh Syl Ukrainy" [The influence analysis of "hybrid" war on the developmentof automatic system of aviation control and anti-aircraft defenses of the Armed Forces of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 116-120. https://doi.org/10.30748/nitps.2017.27.22.

2. Kuzneczov, M. (2018), "Rosijsjki zasoby REB u bojovykh dijakh na Donbasi" [Russian means of RF in hostilities in the Donbass], *Informnapalm*, No. 1, pp. 1-3, available at: www.informnapalm.org/ua/rosijski-zasoby-reb-na-donbasi/ (accessed 29 October 2018).

3. Konakhovych, Gh.F., Klymchuk, V.P., Pauk, S.M. and Potapov, V.Gh. (2005), "*Zashhyta informaciy v telekommunikaciynyh systemah*" [*Protection of information in the telecommunication system*], publishing house MK-Press, Kyiv, p.p. 191-205.

4. Jayakurami, J.A. and Dhanya, G. (2016), A review of analog speech scrambling for secure communication, *Progress in science and engineering research journal,* Vol. 2, pp. 194-198.

5. Lim, Y.C., Lee, J.W. and Foo, S.W. (2010), Quality analog scramblers using frequency-response masking filter banks circuits, *Syst. Signal Process,* Vol. 29, pp. 135-154.

6. Jayakurami, J. and Dhanya, G. (2016), An efficient voice scrambling technique for next generation communication systems, *International Journal of Engineering and Technology,* Vol. 8, No. 1, pp. 293-299.

7. Andrade, J.F., Campos, M. and Apolinario J.A., (2008), Speech privacy for modern mobile communication systems, *Acoustics, Speech and Signal Processing*, No. 1, pp. 177-178.

8. Lin, K.T. (2011), Hybrid encoding method by assembling the magic matrix scrambling method and the binary encoding method in image hiding, *Optics Communications,* Vol. 284, No. 7, pp. 1778-1784.

9. Klymovych, O.K., Lavrut, O.O. and Ivko, S.O. (2016), "Vyznachennya perspektyvnyh texnologij v systemax radiozvyazku ta trankingovogo zv'yazku dlya podalshogo vykorystannya v Zbrojnyx Sylax Ukrayiny", [Definition of advanced technologies in radio communication and trunk communication systems for further use in the Armed Forces of Ukraine], *Collection of scientific works of Odessa National Academy of Communication*, No. 2(6), pp. 30-35.

10. Sattar, B.A. (2005), Proposed Speech Scrambling Based on Wavelet Transform and Permutation, *3th International Conference on Systems, Signals and Devices*, March 21-24, 2005, Sousse, Tunisia, pp. 42-54.

11. Lee, J.W. and Lim, Y.C. (2008), Efficient fast filter bank with a reduced delay, *Circuits and Systems,* No. 1,pp. 140-143.

12. Wu, Y., Noonan, J.P., and Agaian, S. (2011), NPCR and UACI randomness tests for image encryption, *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, No. 1(2), pp. 31-38.

Надійшла до редколегії 1.10.2018
Схвалена до друку 5.11.2018

Відомості про авторів:

Северілов Андрій Володимирович
викладач
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-6984-6643

Васьковський Віктор Васильович
бакалавр
курсант Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-4738-9151

Волосенко В'ячеслав Миколайович
бакалавр
курсант Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-6704-0929

Шуварін Ігор Анатолійович
бакалавр
курсант Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-2172-6789

Information about the authors:

Andriy Severilov
Instructor
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0001-6984-6643

Viktor Vaskovskyi
Bachelor
Cadet of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4738-9151

Viacheslav Volosenko
Bachelor
Cadet of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0001-6704-0929

Ihor Shuvarin
Bachelor
Cadet of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-2172-6789

АНАЛИЗ АНАЛОГОВЫХ МЕТОДОВ СКРЕМБЛИРОВАНИЯ, КОТОРЫЕ ПРИМЕНЯЮТСЯ В СИСТЕМАХ ВОЕННОЙ РАДИОСВЯЗИ

А.В. Северилов, В.В. Васьковский, В.М. Волосенко, И.А. Шуварин

В работе проведен анализ аналоговых методов скремблирования, используемый в системах военной ультракоротковолновой радиосвязи, а именно инверсия сигнала по частоте, разделение полосы частот речевого сообщения на определенное количество поддиапазонов, разбиение сигнала на языковые сегменты и их перестановки во времени. Рассмотрены принципы функционирования и показаны основные преимущества и недостатки приведенных методов аналогового скремблирования.

Ключевые слова: *радиосвязь, аналоговое скремблирование, инверсия, временной интервал, несанкционированный наблюдатель, трафик, шифрование, полоса частот.*

ANALYSIS OF ANALOG METHODS OF SCRAMBLING USED IN THE MILITARY RADIO COMMUNICATION SYSTEM

A. Severilov, V. Vaskovskyi, V. Volosenko, I. Shuvarin

Research into the experience of the Combined Forces Operation suggests that the main component of the command and control system of troops in the tactical level of control remains the ultra-shortwave radio communication system, especially at depth, the platoon strong point and the company strong point. This is especially true in cases where the combat situation does not allow the deployment of wire lines of communication. In this case, there is often a need to ensure the protection of transmitted information in VHF radio networks. This is primarily due to the fact that the electronic intelligence units of the enemy constantly monitor the radio and have modern Russian-made electronic warfare equipment in their composition, which allows for efficient interception of voice information and neutralization of radio engineering systems, in particular, VHF radio communications. The EBC Borisoglebsk-2 complex, which was recorded in the Lugansk region and in Lugansk itself in the winter of 2015, and the EW complex Thorn, which was recorded at Donetsk airport in 2015, deserve the most attention. An analysis of the literature indicates that the security of communication when transmitting voice messages is based on the use of a large number of different methods of encrypting messages that change the properties of a message in such a way that it becomes unclear and therefore inaccessible to an unauthorized observer who monitors the radio channel. The order of implementation of voice message encryption methods is chosen depending on the specific tasks assigned to the information transmission system and the specifics of building a technical transmission channel. The most common and budget method that provides secure transmission of voice messages in VHF radio communication systems can be considered scrambling - a process carrying or inverting signals or otherwise encoding messages on the transmitting side to make the message incomprehensible on the receiving side not equipped with a properly installed descrambling device. Therefore, an analysis of existing scrambling methods that are used in VHF radio communication systems was carried out.

Keywords: *radio communication, analog scrambling, inversion, time interval, unauthorized observer, traffic, encryption, frequency band.*