

КОНЦЕПЦІЯ ПОБУДОВИ ОБЛАДНАННЯ ЗАХИЩЕНОГО РАДІОТЕЛЕФОННОГО ЗВ'ЯЗКУ ДЛЯ АВІАЦІЙНИХ ЗАСТОСУВАНЬ

Георгій Конахович, Веніамін Антонов, Віталій Курушкін

Національний авіаційний університет, Україна



КОНАХОВИЧ Георгій Філімонович, д.т.н.

Рік та місце народження: 1944 рік, м. Васильків, Київська область, Україна.

Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1968 рік.

Посада: завідувач кафедри телекомунікаційних систем Інституту аеронавігації Національного авіаційного університету.

Наукові інтереси: системи захисту інформації, інформаційно-комунікаційні системи.

Публікації: більше 200 наукових та навчально-методичних праць, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи.

E-mail: tko@nau.edu.ua



АНТОНОВ Веніамін Валерійович

Рік та місце народження: 1968 рік, м. Вільнюс, Литва.

Освіта: Орловське вище військове командне училище зв'язку ім. М.І. Калініна, 1992 рік.

Посада: старший викладач кафедри телекомунікаційних систем Інституту аеронавігації Національного авіаційного університету.

Наукові інтереси: системи захисту інформації, інформаційно-комунікаційні системи.

Публікації: більше 20 наукових публікацій.

E-mail: tko@nau.edu.ua



КУРУШКІН Віталій Євгенович, к.т.н.

Рік та місце народження: 1978 рік, м. Київ, Україна.

Освіта: Національний авіаційний університет, 2001 рік.

Посада: доцент кафедри телекомунікаційних систем Інституту аеронавігації Національного авіаційного університету.

Наукові інтереси: системи захисту інформації, інформаційно-комунікаційні системи.

Публікації: більше 10 наукових публікацій.

E-mail: tko@nau.edu.ua

Анотація. Запропонована та обґрунтована технологічна схема обробки мовного трафіку технічними засобами систем авіаційного аналогового радіозв'язку в діапазоні 118-137МГц для умов, коли є потреба забезпечити високий рівень захищеності обміну мовними повідомленнями. Технічна реалізація запропонованої схеми дозволяє виконати модифікацію існуючих засобів аналогового радіозв'язку, не руйнуючи конструкцію авіаційної радіостанції УКХ діапазону та не порушуючи регламенту радіообміну. Взагалі низку додаткових пристроїв у складі (вокодер + крипто-шифратор + частотно-фазовий маніпулятор) бажано виконати у вигляді окремого пристрою та підключити його в інтерфейсну точку передавального обладнання між мікрофоном та модулятором несучої частоти радіосигналу. А, пристрій, який реалізує ланцюг (частотно-фазовий деманіпулятор + крипто-дешифратор + синтезатор вокодеру), потрібно підключити на приймальній стороні між виходом демодулятора та входом телефону того хто отримує мовні повідомлення. У цьому разі на індикаторну панель штатного обладнання достатньо додати лише один перемикач режиму мовного обміну (захищено \ не захищено).

Ключові слова: вокодер, ЧМ, ФМ, модулятор, демодулятор, маніпулятор, деманіпулятор, мовний трафік.

Вступ

У зв'язку із загостренням світових політичних протиріч документами ІКАО визначена доцільність

створення та подальшого застосування обладнання радіотелефонного зв'язку, зокрема на ділянках «пілот – авіадиспетчер», на яких наразі використовуються стандартні вузько смугові аналогові VHF (Very High

Frequency) радіоканали у діапазоні 118-137 МГц з дискретністю сітки частот 25кГц або 8,33кГц [1-5], але за умов, якщо це обладнання забезпечує високий рівень захищеності мовного обміну. Положеннями концепції ICAO CNS/ATM щодо розвитку мережі авіаційного електрозв'язку (ATN) декларується доцільність використання як VHF-ліній аналогового зв'язку, так і VHF-ліній цифрового зв'язку (тобто, лінії VDL Mode 2,3 та 4). Якщо схеми включення сучасних засобів захисту інформації у склад ліній VDL не складають науково-технічної проблеми (оскільки на базі цих ліній можливо організувати будь-які сервіси пакетних мереж, у т.ч. поряд з каналним шифруванням реалізувати фільтрацію протокольних блоків даних, засоби міжмережних екранів, IPsec, VPN тощо), то архітектура побудови VHF-ліній аналогового зв'язку не підпадає під семирівневу модель інформаційної взаємодії OSI ISO [6], через що при побудові засобів захисту виникають певні труднощі науково-технічного характеру, що пов'язані, головним чином, із вузькою смугою аналогових ліній штатних авіаційних систем радіотелефонного зв'язку. Проте ICAO із загальної кількості стандартних VHF-ліній (усього 760 ліній) для VDL-ліній зарезервувала лише чотири лінії, решта 756 ліній виділена під аналоговий мовний зв'язок [4]. При цьому у концепції ICAO CNS/ATM підкреслюється [4], що навіть у середньостроковій перспективі VHF-лінії аналогового зв'язку будуть активно використовуватися як з частотним розносом у 25кГц, так і у 8,33кГц. Так що актуальність завдань, що пов'язані із забезпеченням надійного захисту саме VHF-ліній аналогового зв'язку не викликає сумніву.

Метою цієї роботи є поліпшення розбірливості мови у вузькосмуговому каналі зв'язку управління повітряним рухом, шляхом оптимізації параметрів модулятора/демодулятора.

Основна частина дослідження

Сутність проблеми. ICAO не висуває вимог щодо вибору показників захищеності радіоканалів і не надає норм щодо конкретних значень цих показників. Проте вочевидь, що будь-яке обладнання радіозв'язку у будь-якій цивілізованій країні має бути сертифіковане за національними та (або) міжнародними критеріями інформаційної безпеки. І ці критерії мають визначати шляхи побудови та оцінювання якості засобів захисту при обміні інформацією через відкрите (незахищене) радіо середовище. В Україні, зокрема, захист інформації, що транспортується через незахищене середовище, згідно діючих норм [7] здійснюється шляхом реалізації системою захисту двох послуг безпеки: «Конфіденційність при обміні» та «Цілісність при обміні». При цьому гарантованість захисту в інформаційній системі має забезпечуватися на рівні ГЗ, не нижче. Подібна функціональність захисту передбачена також у міжнародних та державних стандартах інших країн. Це достатньо високий рівень захисту, що досягається, у більшості випадків, шляхом використання стійких криптографічних засобів. Зрозуміло, що включення стійких засобів захисту інформації у мовні тракти радіоканалів мають не

погіршувати якість мовного обміну, тобто не погіршувати розбірливість мови, завадозахищеність мовного тракту, рівень електромагнітних наводів на сусідні радіоканали та стійкість щодо зривів систем синхронізації сигналів у каналі. Існує думка, яка розділяється практично усіма фахівцями, що єдиним можливим шляхом досягнення названого рівню захищеності радіоканалів мовного обміну є застосування криптографічного шифрування цифрових мовних потоків. Тобто, використання будь-яких засобів захисту безпосередньо в стандартному аналоговому каналі авіаційного зв'язку без відповідних аналогово-цифрових перетворень потоку мовних сигналів не забезпечує необхідний рівень захищеності інформації (зокрема, не забезпечує гарантованість захисту на рівні ГЗ) і тому є неприйнятним. От же, у рамках існуючого розподілу радіочастотного ресурсу для авіаційних застосувань наразі єдиною можливою схемою побудови мовного тракту аналогового радіоканалу на ділянці «пілот – авіадиспетчер», що використовує VHF-лінію аналогового зв'язку, може бути представлена так, як це показано на рис.1, де фактично відображена узагальнена технологічна схема обробки мовного трафіку засобами системи авіаційного радіозв'язку для випадку, коли цей трафік потребує гарантованого захисту на рівні ГЗ та вище. Як бачимо, ця схема передбачає необхідність «оцифровки» потоку аналогових мовних сигналів (що є безальтернативною передумовою застосування криптографічних засобів захисту інформації) та утиснення мовної інформації, оскільки безпосередня «оцифровка» мовних сигналів (наприклад, засобами ІКМ або дельта-модуляції) призводить до неприйнятного розширення спектру потоку цифрових мовних сигналів, що за будь-яких видів модуляції мовного сигналу не може бути розміщений у смузі частот мовного тракту радіоканалу будь-якої існуючої системи аналогового авіаційного радіозв'язку. Так що стиснення та «оцифровка» потоку аналогових мовних повідомлень є необхідними елементами технологічної схеми обробки захищеного мовного трафіку у VHF-лініях аналогового авіаційного радіозв'язку.

Найбільш доцільним шляхом технічної реалізації процедур стиснення та «оцифровки» мовної інформації, як показали результати багатьох досліджень (зокрема, [8]), є застосування вокодерних технологій, оскільки функціональність вокодерів передбачає можливість одночасного здійснення названих вище процедур обробки потоку сигналів. Вокодери класифікуються за багатьма характеристиками [8]. Однак у технологічній схемі, що представлена на рис.1, суттєве значення мають два показники якості функціонування вокодера: показник розбірливості мови W , що забезпечує вокодер, під котрим розуміється відносна кількість (у відсотках) правильно прийнятих елементів артикуляційних таблиць, що були передані через канал транспортування мовної інформації [7]; швидкість цифрового потоку мовних сигналів на виході вокодера R (див. точка A на рис.1), що характеризує його можливості із стиснення мовних повідомлень.

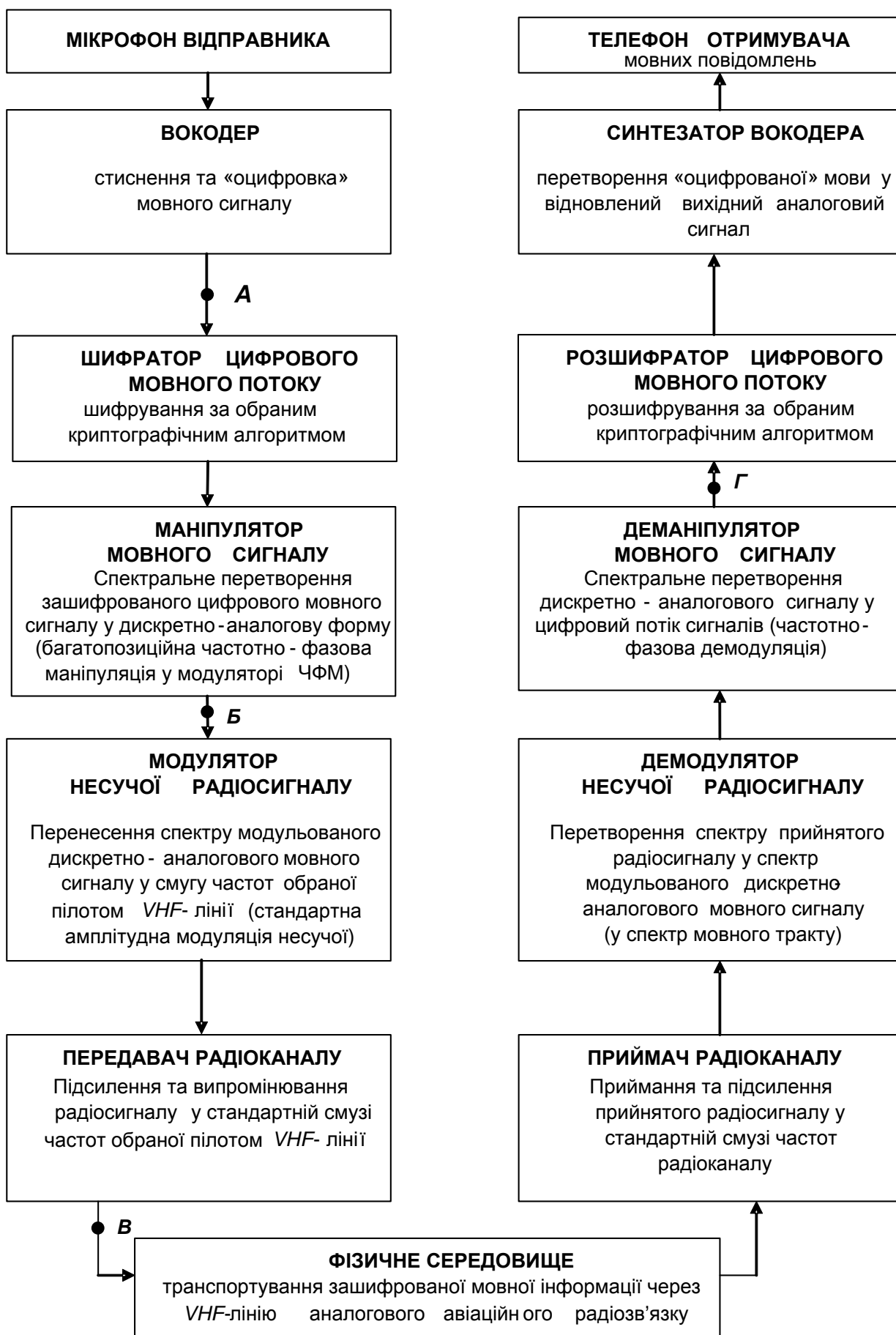


Рис. 1. Технологічна схема обробки захищеного мовного трафіку засобами обладнання авіаційних систем аналогового радіозв'язку

Чим менше значення R , тим вище коефіцієнт стиснення мови, проте тим гірше її розбірливість. З іншого боку, спроби забезпечити прийнятний рівень розбірливості мови змушують включати у мовний тракт радіоканалу вокодер, що характеризується невисокими можливостями щодо стиснення мови і, отже, відносно високими значеннями R . За високих значень параметру R , у свою чергу, ширина смуги спектру маніпульованих сигналів мовного тракту на виході маніпулятора мовного сигналу (див. точка B на рис. 1) може виявитися настільки збільшеною, що після маніпуляції ефективна ширина смуги дискретно-аналогового мовного сигналу (див. точка B на рис. 1) не зможе вкластися у смугу частот мовного тракту радіоканалу. Виникнуть лінійні спотворення сигналів у приймальній частині мовного тракту, що призведе до порушень норм щодо показників завадостійкості, що прийняті для мовних трактів систем телефонного зв'язку. Ще більш складніша ситуація щодо можливостей запобігання лінійних спотворень сигналів в каналі може виникнути, якщо криптографічне шифрування призводить до розширення спектру шифрованої послідовності. Бажано, щоб швидкості потоків сигналів на вході та виході шифратора були однаковими. Але таке не завжди можливо досягнути на практиці. Тому актуальним є завдання вибору обладнання криптографічного захисту: з одного боку, це обладнання має забезпечувати прийнятний у даних конкретних умовах рівень криптостійкості, а з іншого, генерувати шифровані послідовності із невисоким рівнем інформаційної надлишковості. Слід розрізнити ширину смуги мовного тракту радіоканалу, яка дорівнює 3,1кГц, від стандартної ширини смуги VHF-лінії аналогового авіаційного радіозв'язку, яка має дорівнювати 25кГц або 8,33кГц.

У даному випадку інтерес являє негативний вплив завад на розбірливість мови, що оцінюється величиною ймовірності виникнення помилок саме у мовному тракті радіоканалу, яка, у свою чергу, напряму залежить від співвідношення сигнал/завада на виході маніпулятора мовного сигналу (у точці B), а не на виході VHF-лінії (у точці B).

Зрозуміло, що на завадостійкість системи зв'язку суттєвий вплив являє співвідношення сигнал/завада на виході VHF-лінії, величина якого, у першу чергу, позначається на рівні електромагнітних наводів на сусідні радіоканали. Але параметри системи зв'язку у цій точці регламентовані нормами, що не можуть бути модифіковані у рамках структури рис. 1. У той час як параметри внутрішніх інтерфейсних точок структури рис. 1 не регламентуються стандартами і можуть бути відповідним чином обрані проектувальниками обладнання. Отже, раціональний вибір показника швидкості цифрового потоку R у контрольній точці A на виході вокодера (див. рис. 1), у якій вимірюється показник R , а також криптографічного алгоритму, який з мінімально можливим ступенем має розширювати спектр шифрованої послідовності, є найбільш суттєвими елементами проектування обладнання захищеного радіотелефонного зв'язку. По суті, слід знайти область значень параметру R ,

коли обладнання захищеного мовного тракту радіоканалу буде задовольняти вимогам щодо розбірливості мови, інформаційної безпеки, завадозахищеності мовного тракту та стійкості щодо зривів систем синхронізації по тактовій частоті дискретно-аналогового каналу. Звідси витікає актуальність визначення конкретних значень технічних параметрів тих елементів технологічної схеми, що зображена на рис. 1, модифікація яких забезпечує технічну можливість досягнення оптимальних значень параметру R і в той же час не потребує будь-яких модифікацій штатного обладнання існуючих систем аналогового радіозв'язку. Мова йде про визначення оптимальних параметрів вокодерного обладнання, пристроїв шифрування / розшифрування та маніпулятора / деманіпулятора, тобто елементів обладнання зв'язку, які можуть бути інтегровані в існуючу структуру авіаційних VHF-радіостанцій без порушень норм їхнього використання за основним призначенням, зокрема щодо рівню електромагнітних наводів на сусідні радіоканали. Для цього з формальної точки зору слід здійснити параметричну оптимізацію технологічної схеми, що зображена на рис. 1, в умовах обмежень, що накладають на процес захищеного радіообміну мовною інформацією діючі норми та вимоги щодо побудови та ефективності функціонування обладнання систем авіаційного радіотелефонного зв'язку.

Постановка завдань дослідження. Із вищеведеного витікає, що технологічна схема обробки мовного трафіку в авіаційних VHF-радіостанціях систем вузькосмугового аналогового зв'язку, що зображена на рис. 1, в умовах необхідності забезпечення гарантованості захисту на рівні ГЗ та вище є очевидною та єдино можливою. Проте технічна реалізація цієї схеми стикається з рядом труднощів науково-технічного характеру, що потребують вирішення.

По-перше, формальний вибір параметрів цієї схеми є можливим як результат вирішення задачі параметричної оптимізації математичної моделі мовного тракту VHF-лінії аналогового зв'язку. Для цього необхідно мати математичну модель, яка більш/менш адекватно відображає фізичні процеси, що мають місце у реальних мовних трактах цих ліній. Найбільш суттєвим явищем у мовному тракті радіоканалу, що негативно впливає на рівень достовірності оброблених деманіпулятором мовних повідомлень, є лінійні спотворення форми сигналів на виході деманіпулятора мовного сигналу (у точці Γ на рис. 1), величина котрих напряму залежить від амплітудно-частотних (АЧХ) та фазочастотних (ФЧХ) характеристик мовного тракту, що визначаються у точці Γ на виході демодулятора несучої радіосигналу (в авіаційних багатоканальних радіостанціях VHF-діапазону зазвичай використовується амплітудна модуляція несучої радіосигналу). Тому необхідно побудувати математичну модель мовного тракту, що враховує вплив його АЧХ та ФЧХ на показник завадостійкості тракту. По-друге, не менш суттєве значення на рівень достовірності прийнятих мовних повідомлень

мають характеристики маніпулятора / деманіпулятора мовного сигналу, зокрема його належність до класу когерентних або некогерентних систем, вид маніпуляції (модуляції), а також число позицій дискретно-аналогового сигналу, які він у змозі впевнено розпізнавати. Оскільки когерентні системи повинні мати окремо виділений канал фазової синхронізації, що не є можливим здійснити у рамках обмежень VHF-лінії аналогового авіаційного зв'язку, то у математичній моделі мовного тракту мають відобразитися характеристики лише некогерентних систем. При цьому деманіпуляція фазової компоненти дискретного сигналу, якщо таке буде мати місце, має здійснюватися у варіанті диференціальної фазової (фазовідмінної) демодуляції. Так що до розгляду у рамках математичної моделі мовного тракту мають бути включені параметри некогерентних багатопозиційних маніпуляторів / деманіпуляторів, що здатні здійснювати, у т.ч. , і складні види некогерентної модуляції/демодуляції дискретних сигналів, зокрема ЧМ, ФМ, АФМ, АЧМ, ЧФМ та АЧФМ.

Параметричну оптимізацію побудованої моделі мовного тракту доцільно розглядати як класичну задачу оптимального розподілу ресурсів, тобто обрати певну критеріальну (цільову) функцію, екстремальне значення котрої має бути знайдено, задати множину параметрів моделі, оптимальні значення котрих доставляють екстремум критеріальній функції, та визначити обмеження, у рамках котрих модель вважається коректно побудованою. У даному випадку в якості цільової функції бажано обрати параметр R (точніше, параметр r - питому швидкість цифрового мовного потоку на виході вокодера, що приведена до 1Гц ширини смуги мовного тракту), максимально припустиме значення котрого у рамках заданих обмежень слід визначити. До множини параметрів моделі, що мають бути оптимізовані, слід віднести технічні параметри маніпулятора / деманіпулятора, що впливають на швидкість та достовірність передавання мовної інформації і можуть бути об'єктами вибору під час проектування обладнання. Це, перш за все, вид маніпуляції / деманіпуляції дискретно-аналогових сигналів мовного тракту, оптимальне число позицій дискретно-аналогового сигналу по амплітуді, частоті та фазі, бажана кількість паралельних субканалів у смузі частот мовного тракту та оптимальне значення відношення сигнал/завада на вході деманіпулятора мовного сигналу (у точці Γ на рис. 1). Значення параметрів моделі, що визначаються природою фізичних процесів і не можуть бути об'єктами вибору під час проектування обладнання, задаються в якості обмежень на область визначення цільової функції. Це, перш за все, значення ширини смуги мовного тракту та параметри прийнятих апроксимацій АЧХ та ФЧХ цього тракту. У якості обмеження беруться також нормовані значення показників якості передавання інформації. У даному випадку це ймовірність помилок на виході деманіпулятора мовних сигналів. Після визначення математичного виду цільової функції та системи обмежень

з'являється можливість обрати прийнятний метод оптимізації, з використанням котрого визначається екстремум цільової функції та оптимальні значення технічних параметрів маніпулятора / деманіпулятора.

Вибір в якості цільової функції показника швидкості цифрового потоку на виході вокодера пояснюється тим, що саме цей параметр дозволяє узгодити між собою характеристики вокодера, шифратора та маніпулятора мовних сигналів. Припустимо, що в схему на рис.1 включено шифратор, що не розширює спектр вихідної послідовності відносно ширини спектру вхідної послідовності сигналів. Тоді слід обрати значення параметру R , за якому значення індексу артикуляції мови, що забезпечує вокодер, та ймовірності помилок мовного тракту, що забезпечує деманіпулятор, знаходяться в межах припустимих норм. Знайдені оптимальні параметри деманіпулятора у рамках визначених обмежень забезпечують досягнення максимально можливого значення R і, отже, максимально можливого значення індексу артикуляції мови. Якщо це максимально можливе у заданих умовах значення індексу артикуляції мови є більшим або дорівнює припустимій нормі, то звідси витікає висновок про технічну можливість реалізації схеми, що зображена на рис. 1. У цьому випадку параметри вокодера та маніпулятора / деманіпулятора мають відповідати знайденим оптимальним значенням. У протилежному випадку слід зробити висновок про неможливість модифікації обладнання авіаційних VHF-радіостанцій систем аналогового зв'язку відповідно до схеми, що зображена на рис. 1. Якщо припустити, що в схему на рис.1 включено шифратор, що розширює спектр вихідної послідовності відносно ширини спектру вхідної послідовності сигналів, наприклад в N разів, то значення параметру R на виході вокодера має бути в N разів менше за швидкість потоку на вході маніпулятора, тобто знайдене екстремальне значення критеріальної функції має бути у N разів більшим за швидкість потоку на виході вокодера. Інакше будуть порушені норми: або на розбірливість мови, або на достовірність передачі у мовному тракті. Так що вибір криптографічного засобу має бути здійснений з урахуванням результатів параметричної оптимізації мовного тракту радіоканалу. Вищенаведене дозволяє стверджувати, що технічна реалізація технологічної схема обробки захищеного мовного трафіка засобами обладнання авіаційних систем аналогового радіозв'язку можлива лише за умов вирішення наступного кола завдань: 1) побудова математичної моделі мовного тракту VHF-радіоканалу системи авіаційного аналогового зв'язку з урахуванням АЧХ та ФЧХ цього тракту; 2) параметрична оптимізація розробленої моделі мовного тракту; 3) розробка методики знаходження індексів артикуляції мови для вокодерів, що плануються для застосування у мовному тракті радіоканалу; 4) знаходження залежності між індексом артикуляції мови та швидкістю цифрового потоку на виході вокодера; 5) визначення припусти-

мих значень швидкості цифрових потоків на вході та виході шифратора / дешифратора, за яких забезпечується функціонування обладнання у межах норм за показниками розбірливості мови та достовірності передачі у мовному тракті.

Висновки

Вирішення названих вище завдань дозволить теоретично обґрунтувати технічну можливість (або неможливість) модернізації існуючого обладнання VHF-ліній аналогового авіаційного зв'язку в напрямку забезпечення норм щодо інформаційної безпеки у радіоканалі таким чином, щоб не порушити будь-якої із норм або рекомендацій, що існують у сферах електрозв'язку та організації повітряного руху. Результати вирішення цих завдань дозволять визначити технічні параметри вокодера, шифратора / дешифратора та маніпулятора / деманіпулятора, що будуть слугувати в якості вихідних даних для їхнього проектування. Схема на рис. 1 дозволяє здійснити конструювання названих пристроїв у вигляді конструктивних модулів, фізично відокремлених від штатного обладнання системи аналогового радіозв'язку. Ланцюг пристроїв у складі ВОКОДЕР + ШИФРАТОР ЦИФРОВОГО МОВНОГО ПОТОКУ + МАНІПУЛЯТОР МОВНОГО СИГНАЛУ, якщо він буде виготовлений у вигляді окремого конструктиву, можливо включити в інтерфейсну точку штатного передавального обладнання між виходом мікрофона відправника мовних повідомлень та входом модулятора несучої радіосигналу. А ланцюг пристроїв ДЕМАНИПУЛЯТОР МОВНОГО СИГНАЛУ + РОЗШИФРАТОР ЦИФРОВОГО МОВНОГО ПОТОКУ + СИНТЕЗАТОР ВОКОДЕРА можливо включити в інтерфейсну точку штатного приймального обладнання авіаційних радіостанцій між виходом демодулятора несучої радіосигналу та входом телефону отримувача мовних повідомлень. У цьому випадку на індикаторну панель штатного обладнання радіостанції достатньо додати лише один перемикач режиму мовного обміну «ЗАХИЩЕНО / НЕЗАХИЩЕНО».

Наведені висновки розповсюджуються лише на технологічну схему обробки мовного трафіку в авіаційних системах аналогового радіозв'язку. Обробка сигналів в системах цифрового радіозв'язку (лінії VDL Mode 2,3 та 4) здійснюється за іншими технологічними схемами, які у даній роботі не розглядаються.

Конкретна інформація щодо методів та схем вирішення сформульованих вище завдань, а також

аналіз отриманих результатів, міститься у наведеній нижче бібліографії [9-11].

Література

- [1] ИКАО. Doc. 9705-AN/956. Руководство по техническим положениям для сети авиационной электросвязи (ATN) Издание второе – 1999.
- [2] ИКАО. Авиационная электросвязь. Международные стандарты и рекомендуемая практика. Приложение 10 к Конвенции о Международной гражданской авиации. – Том 111. – Системы связи. – Часть 11. – Системы речевой связи. – Изд. первое – Июль 1995 г.
- [3] ИКАО. Поправка №76 к Международным стандартам и рекомендуемой практике. Авиационная электросвязь. Приложение 10 к конвенции о международной гражданской авиации. – Том 111. Системы связи. Часть 11. – Системы речевой связи. – Том 5. – Использование авиационного радиочастотного спектра. – Март 2001 г.
- [4] Андрусак А.І. Мережа авіаційного електрозв'язку / А.І. Андрусак, В.С. Дем'янчук, Ю.М. Юр'єв. – К.: НАУ, 2001. – 448 с.
- [5] Правила авіаційного електрозв'язку в цивільній авіації України (ПЗ ЦА -2003). – К.: Мінтранс України, 2003. – 132 с.
- [6] ISO/IEC 8073:1992. Information Technology – Telecommunications and information exchange between systems – Open System Interconnection.
- [7] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
- [8] Шелухин О.И. Цифровая обработка и передача речи / О.И. Шелухин, Н.Ф. Лукьянцев; под ред. О.И. Шелухина. – М.: «Радио и связь», 2000. – 456 с.
- [9] Антонов В.В. Особливості передавання захищеного мовного трафіка через стандартний радіоканал авіаційних систем зв'язку / В.В. Антонов, Г.Ф. Конахович, І.О. Козлок // Захист інформації. – 2011. – №3. – С. 72-77.
- [10] Антонов В.В. Оптимізація моделі некогерентної передачі даних через мовний тракт авіаційного радіоканалу / В.В. Антонов // Защита информации: Сб. науч. труд. НАУ. – К.: НАУ, 2011. – №18. – С. 3-13.
- [11] Антонов В.В. Визначення параметрів розбірливості мови, що є прийнятними для авіаційних систем захищеного радіозв'язку / В.В. Антонов, О.Г. Голубничий // Захист інформації. – 2012. – №1. – С. 99-103.

УДК 621.396 (045)

Конахович Г.Ф., Антонов В.В., Курушкин В.Е. Концепция построения оборудования защищенной радиотелефонной связи для авиационных применений

Аннотация. Предложена и обоснована технологическая схема обработки речевого трафика техническими средствами авиационной аналоговой радиосвязи в диапазоне 118-137МГц для условий, когда необходимо обеспечить высокий уровень защищенности обмена речевыми сообщениями. Техническая реализация предложенной схемы позволяет выполнить модификацию существующих средств аналоговой радиосвязи, не изменяя конструкцию авиационной радиостанции УКВ диапазона и не нарушая регламента радиообмена. Вообще ряд дополнительных устройств в составе (вокодер + криптошифратор + частотно-фазовый манипулятор) желательно выполнить в виде отдельного устройства и подключить его в

интерфейсную точку передающего оборудования между микрофоном и модулятором несущей частоты радиосигнала. А, устройство, которое реализует цепь (частотно-фазовый деманипулятор + крипто-дешифратор + синтезатор вокодера), нужно подключить на приемной стороне между выходом демодулятора и входом телефона того, кто получает речевые сообщения. В этом случае на индикаторную панель штатного оборудования достаточно добавить лишь один переключатель режима речевого обмена (защищено / нет защиты).

Ключевые слова: вокодер, ЧМ, ФМ, модулятор, демодулятор, манипулятор, деманипулятор, речевой трафик.

Konakhovych G., Antonov V., Kurushkin V. The concept of secure radiotelephone equipment building for aeronautical applications

Abstract. Proposed and substantiated a flow chart of processing voice traffic by technical means air analog radio in the range 118-137MHz for conditions when it is necessary to ensure a high level of protection of voice messaging. Technical implementation of the proposed scheme allows you to modify the existing analog radio resources without changing the design of the aircraft VHF radio and not breaking the rules of the radio traffic. In general, a number of additional devices in the (vocoder + crypto coder + frequency phase manipulator), it is desirable to perform as a single device and connect it to the interface point transmission equipment between the microphone and the modulator carrier frequency of the radio signal. A device, that implements the circuit (frequency-phase demanipulator + decoder + crypto synthesizer vocoder), need to be connected to the receiving side between the output of the demodulator and the input of the phone by person who receives voice messages. In this case, a display panel of standard equipment is sufficient to add only a voice communications mode switch (protected \ no protection)

Key words: vocoder, FM, PM, modulator, demodulator, manipulator, demanipulator, voice traffic.

Отримано 2 жовтня 2014 року, затверджено редколегією 24 жовтня 2014 року
