СЕКЦІЯ 8

РОЗВИТОК ТА ЗАСТОСУВАННЯ ЗАСОБІВ РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ТА ЗВ'ЯЗКУ ПОВІТРЯНИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Керівники секції: генерал-майор О.І. Кушнір;
д.т.н. професор полковник О.В. Потій
Секретар секції: ст. лейтенант О.В. Ревін

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ЗВ'ЯЗКУ, РТЗ, АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПОВІТРЯНИХ СИЛ

О.І. Кушнір

Викладаються основні положення Концепції створення системи зв'язку, радіотехнічного забезпечення (РТЗ) та інформаційних систем (ІС) Повітряних сил Збройних сил України. Піднімаються питання побудови сучасної системи управління Повітряними Силами. Визначені основні умови ефективного управління та характерні особливості управління в ПС. Визначені головні напрямки розвитку військо зв'язку та інформаційних систем ПС, а саме:

– побудова цифрової інтегральної мережі зв'язку на основі застосування сучасних цифрових технологій, яка дозволить створити єдине інформаційне поле в інтересах усіх ланок управління від стратегічної до тактичної включно;

– створення системи аеронавігаційного обслуговування авіації Збройних Сил України з використанням існуючих та сучасних радіоелектронних засобів повітряної навігації, підсистем зв'язку (телекомунікацій) та спостереження на основі застосування цифрової технології, приведення радіотехнічного забезпечення на аеродромах ПС ЗС України у відповідність до вимог стандартів Міжнародної організації цивільної авіації (ІКАО) та НАТО, чим забезпечити підвищення рівня безпеки повітряного руху;

– створення єдиної системи контролю повітряного простору, управління повітряним рухом та бойовими діями авіації і сил ППО, яка забезпечить оптимальне використання усіх радіолокаційних засобів в інтересах користувачів, підвищить надійність управління авіацією та рівень взаємодії між відомствами та видами Збройних Сил.

Визначаються перспективні напрямки розвитку зв'язку, РТЗ та А та ІС Повітряних Сил, а саме:

– застосування інформаційних технологій, які базуються на нових досягненнях у галузі інформатики та обчислювальної техніки;

– застосування цифрових систем передачі, що визначає перехід від аналогових до цифрових методів обробки, комутації і передачі сигналів різних видів електрозв'язку в єдиному цифровому вигляді;

– застосування способів та засобів високошвидкісного передавання інформації через телекомунікаційні мережі в реальному масштабі часу з мінімальними часовими затримками, які забезпечують гарантовану пропускну спроможність;

– забезпечення сумісності стандартів і систем радіотехнічного забезпечення польотів аеродромів Збройних Сил України та держав-членів НАТО;

– інтеграція до перспективної європейської системи управління польотами авіації та протиповітряної оборони ACCS НАТО;

– удосконалення існуючого парку техніки радіотехнічного забезпечення;

– створення автоматизованої системи управління військами та зброєю Повітряних Сил Збройних Сил України.

За умови реалізації визначених організаційних рішень, оснащення Повітряних Сил Збройних Сил України перспективними системами, засобами автоматизації та зв'язку, та засобами захисту можна очікувати значного зростання оперативності і стійкості управління, рівня бойової готовності.

ПРОБЛЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ ВІЙСЬК ЗВ'ЯЗКУ ПОВІТРЯНИХ СИЛ

О.І. Бабенко, к.військ.н., доц.; О.В. Потій, д.т.н. проф.
Харківський університет Повітряних Сил імені Івана Кожедуба

Сьогодні ми маємо виробити Концепцію організації оперативно-тактичної та військово-технічної підготовки фахівців зі зв'язку, РТЗ, АУ авіації, яка є системою поглядів на послідовність, зміст та загальну методику навчання, метою якого є підготовка висококваліфікованих фахівців, які спроможні ефективно та технічно грамотно ставити та вирішувати завдання: експлуатації широкої номенклатури видів техніки зв'язку, РТЗ систем та комплексів автоматизації бойового управління у ході організації зв'язку та РТЗ польотів авіації, управління бойовими діями авіації; організації та забезпечення взаємодії та спряження елементів систем військового зв'язку між собою, з мережами міністерства зв'язку з іншими операторами; засвоєння нових телекомунікаційних технологій та впровадження їх у системи зв'язку, РТЗ, АУ авіації; розгортання систем зв'язку, РТЗ, АУ на базі нових інформаційно-телекомунікаційних технологій та здійснювати управління такими системами. Така підготовка має здійснювати у двох напрямах:

1. Фундаментальна теоретична підготовка з питань теорії зв'язку, РТЗ, автоматизованих систем управління, теорії розвитку сучасних систем зв'язку та АСУ з урахуванням їх переходу на цифрові способи передачі та комутації на базі реалізації нових інформаційно-телекомунікаційних технологій.

2. Засвоєння конкретних зразків техніки, що стоять на озброєнні та використовуються у процесі організації зв'язку, РТЗ та автоматизації управління авіацією.

Головними принципами, що лежать в основі підготовки наших випускників у нових умовах мають бути:

1. Системність підготовки, тобто забезпечення системної цілісності знань.

2. Орієнтація на перспективні сучасні цифрові та інформаційно-телекомунікаційні технології світового рівня, які вже є реальністю для загально державних та відомчих систем та мереж зв'язку та АСУ, а також охоплення всіх аспектів їх впровадження.

3. Фундаментальність підготовки, суворий відбір та оптимізація навчальної інформації, реалізація принципу необхідної достатності обов'язкових знань.

4. Практична спрямованість підготовки, безперервність зв'язки "знання-практична діяльність"

ПРИМЕНЕНИЕ ШИРОКОПОЛОСНОГО ПРИНЦИПА В ТЕОРИИ ИНФОРМАЦИИ

В.В. Ковальчук, д.физ.-мат.н., доц.; В.В. Клименко, к.т.н., с.н.с.;
А.А. Панченко; В.А. Громов
Одесская военная академия

Широкополосные принципы передачи применяются в технике связи для обеспечения высокой помехоустойчивости и затруднения процесса перехвата. Расшире-

ние диапазона выполняется, в основном, посредством кода, который не зависит от передаваемых данных. В работе предложена математическая модель на основе широкополосного принципа в теории информации. Суть основана на стегосистемности: «растворить» необходимую информацию в контейнере и сделать возможным обнаружение ее лишь тому, кто ее закодировал. Для решения поставленной задачи учитывалось то, что для защиты информации применяют, главным образом, два способа расширения спектра. Такая процедура реализуется с помощью: а) псевдослучайной последовательности, т.е. когда защищаемый сигнал, отличается от основного на константу, модулируемую стохастически; б) прыгающих частот, т.е. когда частота несущего сигнала изменяется по некоторому псевдослучайному закону. Предложенная нами модель основана на одном из этих вариантов реализации широкополосного метода. Для защиты сообщения т предлагается генерировать стегосообщение E(x,y) в виде изображения, формируя взвешенную сумму. Показано, что операция декодирования заключается в восстановлении защищенного сообщения путем проектирования стегоизображения S на все функции. Если $m_i = 0$, то защищаемая информация будет утеряна. Основное преимущество, предлагаемой модели состоит в сравнительно высокой устойчивости к искажениям изображения и разного вида атакам, так как защищаемая информация распределена в широкой полосе частот, и ее трудно удалить без полного разрушения контейнера.

ОЦІНКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗВ'ЯЗКУ ВОЄННОГО ПРИЗНАЧЕННЯ

В.П. Ясинецький, к.військ.н., доц.; М.В. Кас'яненко
Національний університет оборони України

Практика проведення командно-штабних навчань показує, що існуючи системи зв'язку окремих ланок управління не в повній мірі задовольняють потреби органів управління щодо забезпечення своєчасного проходження необхідного обсягу оперативно – тактичної інформації. Це вимагає проведення всебічного аналізу та оцінки існуючих систем зв'язку воєнного призначення, з метою обґрунтування рекомендацій щодо її удосконалення. На теперішній час розроблено та науково обґрунтовано низка моделей та методик оцінки ефективності систем зв'язку воєнного призначення. Але, проведений всебічний аналіз цих моделей та методик показав, що вони, з одного боку є достатньо простими, а з іншого не забезпечують необхідної точності розрахунків внаслідок суттєвих припущень та обмежень. Тому виникає нагальна потреба у вирішенні актуального наукового завдання, суть якого полягає в розробленні моделі та методики оцінки ефективності функціонування системи зв'язку воєнного призначення які б враховували як переваг так і недоліків попередніх моделей та методик. Авторами пропонується варіант такої математичної модель системи зв'язку воєнного призначення. Дана модель основана на теорії випадкових процесів, теорії масового обслуговування та теорії телетрафіка. В ній, на відміну від відомих моделей, враховуються три самостійних, незалежних та випадкових процеси: процес старіння інформації, процес передачі повідомлень та процес відновлення каналів зв'язку внаслідок їх відмов з різних причин. Такий підхід дозволив усунути низку недоліків відомих моделей та забезпечив визначення необхідних параметрів з достатньою, для проведення аналізу, точністю, що дало можливість більш обґрунтовано оцінити ефективність функціонування систем зв'язку воєнного призначення.

ПІДВИЩЕННЯ МОБІЛЬНОСТІ СИСТЕМИ ЗВ'ЯЗКУ, РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ТА АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПОВІТРЯНОГО КОМАНДУВАННЯ

В.Г. Кубрак
Національний університет оборони України

З розвитком і удосконаленням форм та способів збройної боротьби, все більш чітко проявляються такі характерні риси сучасної війни, як різкі та швидкі зміни обстановки, висока маневреність військ та високі темпи їх переміщення. Крім того, зростаючі можливості систем розвідки, радіоелектронної боротьби і вогневого ураження противника приводять до скорочення часу, необхідного йому для виявлення та нанесення ураження вузлам зв'язку. Для успішного функціонування в таких умовах система зв`язку, радіотехнічного забезпечення та автоматизації управління повітряного командування повинна мати високу мобільність. У виступі висвітлена удосконалена методика оцінки мобільності системи зв`язку, радіотехнічного забезпечення та автоматизації управління повітряного командування, проаналізовані зовнішні та внутрішні фактори, які впливають на показник мобільності. Показана залежність часових показників мобільності вузлів зв'язку від можливостей систем розвідки і ураження противника та періоду часу, необхідного для функціонування органів управління. За допомогою вказаної методики обгрунтовані рекомендації щодо підвищення мобільності системи зв`язку, радіотехнічного забезпечення та автоматизації управління повітряного командування. Також обгрунтований вплив показника мобільності системи зв`язку, радіотехнічного забезпечення та автоматизації управління на її пропускну спроможність.

РОЗРОБКА ДИНАМІЧНОГО МЕТОДУ УПРАВЛІННЯ ПОТОКАМИ ІНФОРМАЦІЇ У ФРАГМЕНТІ МОБІЛЬНОГО КОМПОНЕНТУ СИСТЕМИ ЗВ'ЯЗКУ ЗС УКРАЇНИ

О.О. Лаврут, к.т.н., доц.
Військовий інститут телекомунікацій та інформатизації НТУ України "КПІ"

Забезпечення всебічної інтеграції, підвищення рівня взаємодії, а також досягнення синергетичного ефекту за рахунок реалізації принципів нових мережоцентричних концепцій та інтеграції систем управління, зв'язку, розвідки та поразки стає все більш актуальним та пріоритетним напрямком реформування збройних сил більшості країн світу. При всіх існуючих перевагах "мережоцентричних принципів", ефективного математичного апарата кількісної оцінки впливу нової концепції на підвищення ефективності дії військ до цих пір не існує. У зв'язку з цим одним із можливих способів вивчення мережних архітектур перспективних мережоцентричних концепцій є тензорні моделі і методи аналізу. В роботі запропоновано динамічний метод управління потоками інформації у фрагменті мобільного компоненту системи зв'язку ЗС України на основі тензорних моделей. А також наведено приклад розв'язання задачі багатошляхової маршрутизації команди управління на основі даного фрагменту з використанням запропонованого методу. В ході розв'язання задачі забезпечена мінімально однакова затримка передачі частин повідомлення уздовж кожного з розрахованих маршрутів. Показано, що використання запропонованого методу можливе як при нарощуванні структури (її реорганізації), так і в критичних умовах. Результати розрахунку та імітаційного моделювання підтвердили адекватність запропонованого методу та доцільність його реалізації.

ПРОПОЗИЦІЇ ЩОДО АДАПТАЦІЇ НАЗЕМНИХ ЗАСОБІВ УЛЬТРАКОРОТКОХВИЛЬОВОГО РАДІОЗВ'ЯЗКУ ПОВІТРЯНИХ СИЛ ДО СТАНДАРТІВ ТА НОРМ МІЖНАРОДНОЇ ОРГАНІЗАЦІЇ ЦИВІЛЬНОЇ АВІАЦІЇ

Ю.М. Добришкін, к.т.н; І.Л. Костенко, к.військ.н., с.н.с.; З.З. Закіров, к.т.н., с.н.с.
Харківський університет Повітряних Сил імені Івана Кожедуба

Сучасні Повітряні Сили (ПС) Збройних Сил (ЗС) України озброєні літальними апаратами і складними технічними наземними (аеродромними) комплексами, які забезпечують виконання авіацією різноманітних завдань і задач у складних метеорологічних умовах вдень і вночі. Важливу роль у виконанні задач, що вирішуються авіацією, відіграють наземні засоби ультракороткохвильового (УКХ) радіозв'язку. Одним з основних напрямків розвитку наземних засобів УКХ радіозв'язку ПС ЗС України є забезпечення сумісності в роботі радіотехнічних засобів забезпечення польотів зі стандартами та нормами Міжнародної організації цивільної авіації (ІКАО). В роботі запропоновані шляхи щодо адаптації наземних засобів ультракороткохвильового радіозв'язку Повітряних Сил до стандартів та норм Міжнародної організації цивільної авіації на прикладі наземної УКХ радіостанції Р-845М. Показано, що для переходу радіостанції Р-845М до стандартів та норм ІСАО на крок сітки частот 8,33 кГц необхідно провести зміни в приладах 11М, 1-ОС та кабелях керування між ними. Та показано напрям адаптації командно-стартової радіостанції Р-845М до стандартів Міжнародної організації цивільної авіації шляхом проведення організаційних заходів.

ПЕРСПЕКТИВИ РОЗВІТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ВІСЬК ПІД ЧАС СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ

О.Ю. Іохов, к.т.н., с.н.с.; О.М. Горбов; І.В. Кузьминич
Академія внутрішніх військ МВС України

Дослідження сучасних автоматизованих та інформаційних систем, виявило низку проблемних питань, які мають системний характер і суттєво впливають на розробку підсистем управління військ. Серед них головне місце займає створення систем зв'язку з урахуванням сьогодення та перспектив розвитку телекомунікаційної технологій, спроможної охопити все коло завдань управління військ. Тому особливу увагу треба приділити визначенню вимог до системи зв'язку та автоматизації управління військ. Порівняльний аналіз сучасного стану системи зв'язку військ, військових систем зв'язку провідних країн світу та комерційних систем зв'язку дозволяє зробити висновок про необхідність визначення нових вимог до засобів зв'язку та визначення шляхів їх виконання. Визначені та обгрунтовані вимоги до перспективних засобів радіозв'язку, комутації та імітозахисту, в яких чітко зазначені перспективи розвитку вищевказаних засобів, загальною вимогою котрих є перехід виключно на цифрові системи та стандарти, які за своїми можливостями відповідають вимогам сучасності, керівних документів та ДСТУ. Запропонована архітектура перспективної системи зв'язку. Дослідження, створення та впровадження кожного її рівня дозволить значно покращити скритність та достовірність системи зв'язку, характеристики інформаційного обміну. Однак, це вимагає вирішення низки проблем наукового (побудова узгоджених сигнально-кодових конструкцій, розробка систем криптографічного захисту інформації тощо) та технологічного плану (побудова багатофункціональних багатодіапазонних радіозасобів, що перепрограмовуються).

ПІДСЕКЦІЯ 8.1

РОЗВИТОК ЗАСОБІВ РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ТА ЗВ'ЯЗКУ

Керівники підсекції: генерал-майор О.І. Кушнір;
д.т.н. професор полковник О.В. Потій
Секретар підсекції: ст. лейтенант О.В. Ревін

МЕТОД ОЦЕНИВАНИЯ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КСЗИ

А.В. Потий, д.т.н. проф.; Д.С. Комин
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Одним из этапов проведения экспертизы комплексных систем защиты информации (КСЗИ) является оценивание уровня гарантий информационной безопасности (ИБ). Гарантии являются залогом корректности реализации функциональных услуг безопасности и выполнения политики безопасности оцениваемого объекта. Анализ нормативных документов, закрепляющих требования гарантий и регламентирующих процедуру проведения экспертизы, позволили сделать вывод, что к процессу оценивания гарантий предъявляются требования ширины, глубины и строгости, а к результатам такого оценивания – требования объективности, повторяемости, воспроизводимости, сопоставимости, беспристрастности. Обзор нормативной и научной литературы показал, что пути (способы, методы) достижения и обеспечения указанных характеристик не определены. Для обеспечения выполнения вышеуказанных требований к оцениванию гарантий предлагается подходить с позиций функционально-лингвистического подхода. В рамках данного подхода разработан метод оценивания гарантий ИБ. В составе метода предложены следующие научные положения: разработан способ построения объектно-ориентированной онтологической модели области оценивания гарантий ИБ; разработан способ построения процессно-ориентированной онтологической модели области оценивания гарантий ИБ; предложены рекомендации по использованию в рамках метода методологии функционального моделирования в нотации IDEF0, математического аппарата лингвистических переменных и нечеткого логического вывода, метода моделирования потоков работ в нотации IDEF3. Таким образом, применение разработанного метода оценивания гарантий ИБ позволит обеспечить выполнение требований к процессу и результатам оценивания гарантий за счет применения методов моделирования и формализации деятельности эксперта, что, в свою очередь, снижает неопределенность во время проведения экспертизы и создает условия для проведения объективного оценивания.

ОСОБЕННОСТИ ИНСТИТУЦИОНАЛЬНОЙ МОДЕЛИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

А.В. Потий[1], д.т.н. проф.; Д.Ю. Пилипенко[2]
[1]Харьковский университет Воздушных Сил имени Ивана Кожедуба;
[2]Харьковский национальный университет радиоэлектроники

Сегодня происходит стремительное развитие нормативной базы в области обеспечения информационной безопасности (ИБ). Множество рекомендаций, лучших практик, подходов и концепций, которые содержатся в стандартах и различно-

го рода документах с одной стороны, и отсутствие научно-методического аппарата с другой, приводит к системному противоречию. Проблемы в обеспечении информации, которые возникают сегодня, крайне затруднительно решить в рамках экстенсивного подхода к защите информации – увеличивая количество ресурсов, которые используются для защиты информации. Несмотря на высокий уровень эффективности отдельных средств защиты информации, их комплексное применение не отражается на росте эффективности всей системы в целом. Таким образом, сегодня остро чувствуется необходимость введения в практику новых моделей и подходов, которые помогут координировать и организовывать деятельность по обеспечению ИБ. В качестве решения данных проблем предлагается использовать институциональную модель управления ИБ. Суть данного типа управления заключается в формировании норм и ограничений, как явной (политика безопасности, стандарт, должностная инструкция, соглашение о конфиденциальности), так и неявной форме (культура информационной безопасности). Следует отметить, что разработка и обоснование политики безопасности, норм, правил и процедур осуществляется в основном на основе эвристического метода или метода экспертной оценки. Проблемы обоснования правил безопасности и согласования политик безопасности на всех уровнях управления организацией сегодня не решены полностью. Таким образом, институциональная модель управления информационной безопасностью организации представляется перспективным подходом для решения данных проблем.

ПРИМЕНЕНИЕ ДОСТИЖЕНИЙ НЕЛИНЕЙНОЙ ДИНАМИКИ ДЛЯ ПОВЫШЕНИЯ СКРЫТНОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

П.Ю. Костенко, д.т.н., проф.; С.Н. Симоненко

В докладе проводится анализ традиционного подхода к решению задачи повышения скрытности систем передачи информации, основанного на использовании сложных широкополосных сигналов, освещены его недостатки и ограничения. Рассматривается альтернативный подход к ее решению, который использует методы и алгоритмы теории нелинейных динамических систем. Выясняются причины недостаточной скрытности сложных широкополосных сигналов и показывается за счет чего сигналы с хаотической несущей обладают значительно большей структурной скрытностью.

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СЛУЧАЙНЫХ ФРАКТАЛЬНЫХ ПРОЦЕССОВ ДЛЯ ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ БИНАРНОЙ ИНФОРМАЦИИ

К.С. Васюта, д.т.н., доц.; С.А. Щербинин; А.В. Ревин
Харьковский университет Воздушных Сил имени Ивана Кожедуба

В настоящее время военные системы для скрытной передачи информации используют широкополосные сигналы. Обеспечение разведзащищенности военных радиотехнических систем передачи информации с применением широкополосных сигналов позволяет ослабить воздействие многих видов помех и принимать сообщения при соотношении сигнал/шум много меньше единицы. Скрытность, которую называют энергетической, обеспечивается за счет передачи в эфир непрерывных во времени сложных широкополосных радиосигналов с очень низкой спектральной плотностью, при которой сигналы «прячутся» под шумом. При этом без шума такие сигналы

визуально не похожи на случайный процесс. Поэтому их скрытность обеспечивается лишь при наличии шума, уровень которого больше уровня сигнала. Анализ показал, что сложные широкополосные сигналы не являются сигналами, работающими «под шум» и, следовательно, в полной мере не обеспечивают скрытность систем передачи информации, в которых они применяются. Альтернативное решение проблемы обеспечения скрытности дает применение случайных процессов, обладающими фрактальными свойствами. Такие сигналы для несанкционированного наблюдателя неотличимы от шума при визуальном, корреляционном, спектральном анализе и обладают набором специфических свойств, делающих их привлекательными с точки зрения построения схем скрытой передачи информации.

ПРИМЕНЕНИЕ МЕТОДОВ АДАПТИВНОЙ ОБРАБОТКИ СИГНАЛОВ ДЛЯ ВОССТАНОВЛЕНИЯ ИЗОБРАЖЕНИЙ В УСЛОВИЯХ ВНЕШНЕГО АКТИВНОГО ШУМА

В.В. Скачков, д.т.н., доц.; А.Н. Ефимчиков, к.т.н., доц.; В.В. Чепкий, к.т.н., доц.
Одесская военная академия

Искажения сигналов изображений, передаваемых по цифровому каналу связи с неизвестной передаточной характеристикой в условиях внутренних и внешних шумов, актуализирует проблему восстановления исходного изображения и опознавания его репродукции на выходе информационной системы. Применение технологии «слепой» обработки цифровых сигналов позволяет извлекать явным или неявным методом информацию об искажениях изображения непосредственно из выборок реализаций наблюдаемого процесса. Практика приложения методов «слепой» обработки дискретных сигналов ограничивается задачей восстановления дефокусированных изображений только в условии внутреннего шума канала приѐма. При этом, не учитываются внешние аддитивные шумы, которые вызывают появление флюктуаций яркости на изображении, а при высоком уровне шумов делают изображение неразличимым. Предлагается, применительно к беспроводным телекоммуникационным системам решение данной проблемы осуществлять путѐм использования адаптивных антенных решеток (smart-антенн). Это позволяет в условиях априорной неопределѐнности относительно статистических законов распределения наблюдаемых выборок сформировать оптимальную в заданном смысле пространственную передаточную характеристику информационной системы. Приводятся теоретические и экспериментальные результаты, иллюстрирующие эффективность предлагаемого подхода для восстановления зашумлѐнных изображений.

ТЕСТ ОБНАРУЖЕНИЯ СИГНАЛА В НЕОПРЕДЕЛЁННОЙ ПОМЕХОВОЙ ОБСТАНОВКЕ ДЛЯ МНОГОКАНАЛЬНЫХ РАДИОСИСТЕМ

А.Д. Абрамов, к.т.н., с.н.с.; А.М. Ветошко; А.В. Фатеев
Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ»

Разработка структурно устойчивых и эффективных тестов обнаружения сигнала многоканальными радиосистемами в неопределѐнной помеховой обстановке (в частности дисперсия адаптивных помех неизвестна, на интервале наблюдения возможны непредсказуемые искажения сигнала) является актуальной задачей радиотехнической практики. Оптимальные тесты обнаружения, вытекающие из критерия Неймана-Пирсона, в указанных условиях теряют свою значимость. В докладе решение задачи обнаружения сигналы в неопределѐнной помеховой обстановке многоканальной радиосистемой (антенная системы вы-

полнена в виде эквидистантной линейной решѐтки) проведено при использовании критерия отношения правдоподобия. Синтезирована удобная в вычислительном отношении технология обработки наблюдений, которая обеспечивает оперативность получения результата, возможность использования табулированной статистики и управление величиной ошибки первого рода. Эффективность синтезированного правила с учѐтом упомянутых «искажениях» формы сигнала подтверждено результатами цифрового статистического моделирования: приводятся рабочие характеристики синтезированного теста при различных видах «искажений» в форме зависимости вероятности правильного обнаружения от соотношения сигнал/шум для заданной вероятности ошибки первого рода.

ДО ПИТАННЯ УДОСКОНАЛЕННЯ РАДІОТЕХНІЧНИХ СИСТЕМ ТРАЄКТОРНОГО УПРАВЛІННЯ ЛІТАКАМИ

О.А. Коршець, к.т.н.
Командування Повітряних Сил Збройних Сил України

Використання досягнень нестаціонарної аеродинаміки, динаміки польоту в невстановленому русі і застосування сучасних алгоритмів і радіотехнічних систем автоматичного управління, що мають більш високу адаптацію до умов польоту, призвели до появлення нових типів літаків, які відрізняються своїми надманевреними і надшвидкістними якостями. Істотний вплив на тактику застосування таких літаків має надманевреність. Вона впливає як, так і на вигляд бортових оглядово-прицільних систем, включаючи радіолокаційні системи. У зв'язку з цим розширення номенклатури і кількості надманеврених літаків (НМЛ) змушує значною мірою не тільки модернізувати існуючі алгоритми обробки сигналів у радіолокаційних станціях (РЛС), але і шукати нові шляхи вирішення задач пошуку, виявлення, розпізнавання і супроводу цілей. Для ефективного перехоплення НМЛ літаками перехоплювачами, необхідно використовувати більш складні закони наведення, що вимагають для своєї реалізації більшого обсягу інформації. Особливо це відноситься до ситуації, коли в якості перехоплювача також використовується НМЛ. У доповіді проведено аналіз алгоритмів траєкторного управління НМЛ. Визначено, що одним із факторів досягнення успіху при веденні бойових дій у сучасних умовах є комплексне застосування бойових засобів і можливостей, які існують. Це дозволяє прийти до висновку, що основною формою використання бойового потенціалу авіації слід вважати групові дії. Велике завантаження екіпажа, різноманітність тактичних задач, вимоги, які пред’являються до техніки пілотування, поява нових маневрів, викликають необхідність автоматизації координованого управління рухом літаків в групі і розробки алгоритмів групової взаємодії. Таким чином, в сучасній авіації провідну роль займає розробка і застосування автономних багатоконтурних багатопозиційних систем траєкторного управління.

ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ WIMAX В СИСТЕМАХ ЦИФРОВОГО РАДІОЗВ’ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

О.В. Александров, к.т.н.; М.І. Володін, к.т.н., с.н.с.;
М.В. Науменко, к.т.н.; Е.Ю. Першина
Харківський університет Повітряних Сил імені Івана Кожедуба

В теперішній час армії провідних країн світу переходять на застосування новітніх технологій для організації безпроводового зв'язку. Досягнення переваги в цьому питанні розглядається як суттєве збільшення бойового потенціалу військ.

При цьому для забезпечення віддаленого доступу мобільних компонент до стаціонарних провідними виробниками систем зв'язку військового призначення (Ericsson, General Dynamics) розглядаються можливості використовувати засоби безпроводового зв'язку стандарту 802.16 (WiMax), що працюють в діапазонах 2 – 11 ГГц та 10 – 66 ГГц із швидкістю передачі даних порядку 100 Мбіт/с, та дальністю дії порядку 50 км. В доповіді подане обґрунтування використання технології WiMax для забезпечення високої пропускної спроможності, надійності і мобільності засобів зв'язку. Вказано на доцільність використання широкосмугових сигналів з псевдовипадковою перебудовою робочої частоти (FHSS) для забезпечення перешкодостійкості засобів короткохвильового зв'язку, а також застосування ортогонального частотного ущільнення з мультиплексуванням (OFDM) для підвищення швидкості передачі даних. Визначені переваги застосування технології OFDM під час побудови широкосмугових систем цифрового радіозв'язку.

МОДЕЛЬ МЕТАЛОДІЕЛЕКТРИЧНОГО ФІЛЬТРУ ДЛЯ ЗАСТОСУВАННЯ КЛАСИЧНОГО СИНТЕЗУ

Г.О. Мірських, к.т.н., доц.; Є.М. Андрусенко
Національний технічний університет "КПІ"

Монолітні металодіелектричні фільтри (МФ), завдяки своїм високим електричним показникам широко використовуються в різноманітних НВЧ пристроях. Проте, через складність і тривалість процесу їх проектування, використання таких фільтрів в дослідницьких цілях та дрібносерійній апаратурі стикається з певними труднощами. На сьогодні, проектування фільтрів цього класу має більш експериментальний характер, що призводить до значного об'єму робіт, а відоме програмне забезпечення з розрахунку електродинамічних структур орієнтоване скоріше на дослідження готових зразків ніж їх проектування. Відомо, що процес проектування фільтрів доцільно виконувати на базі класичного синтезу, але ефективність використання відповідних методів суттєво залежить від адекватності еквівалентної схеми що використовується. Звичайно на фінішному етапі проектування методи електродинаміки або відповідні експериментальні дані використовуються для розрахунку конструктивних елементів згідно значень отриманих класичним синтезом узагальнених елементів. В результаті запропонована модель металодіелектричного фільтру являє собою еквівалентну схему, яка пов'язана з електричними структурними елементами, де визначення окремих наближених співвідношень, відповідає складності електромагнітної взаємодії контактних площадок між собою та з металізацією інших сторін фільтру. Досвід використання пропонованої еквівалентної схеми показав її ефективність при використанні класичних методів синтезу під час проектування монолітних металодіелектричні фільтрів.

ЗВОРОТНІЙ ЕФЕКТ ДОПЛЕРА В БЛИЖНІЙ ЗОНІ АНТЕН

В.І. Блєднов, к.т.н., доц.; В.І. Василишин, к.т.н., доц.;
М.М. Дігтярь; С.В. Наумович
Харківський університет Повітряних Сил імені Івана Кожедуба

Відомо, що в дальній зоні антени доплерівський зсув частот проявляється звичайним чином і дозволяє визначити швидкість зближення (віддалення) приймальної антени і розсіючого об`єкта. Проте в ближній зоні антени у зв'язку з особливостями структури електромагнітного поля і векторів його складових доплерівські зсуви частот проявляються незвичайно. При прольоті розсіючого об'єкта

(літального апарату) не відбувається миттєвої (скачкоподібної) зміни зсуву частот з додатнього на від'ємний. Проведений аналіз прояву ефекту Доплера в ближній зоні антени або розсіючих електромагнітні хвилі об'єктів показує, що при русі приймальної антени на випромінювачі спочатку спостерігається звичайний додатний зсув, який поблизу випромінювача переходить нульове значення і перетворюється у від`ємний. В безпосередній близькості до об'єкта доплерівський зсув зменшується, а потім переходить в додатний. Після переходу нульового значення поблизу випромінювача зсув стає від`ємним, тобто звичайним для дальньої зони. Явище зворотнього ефекту Доплера у ближній зоні, особливо переходи зсувів частот через нульове або екстремальне значення, можна використати для виміру відстані до випромінюючих або розсіюючих об`єктів. Найбільше практичне значення це може мати для об`єктів і антен з протяжною ближньою зоною, яка визначається їх розмірами та довжиною хвилі.

ОЦІНЮВАННЯ НАПРЯМКІВ НАДХОДЖЕННЯ РАДІОХВИЛЬ УНІТАРНИМ МЕТОДОМ ROOT-MUSIC З ВИКОРИСТАННЯМ ПСЕВДОШУМОВОГО РОЗМНОЖЕННЯ ВИБІРКИ

В.І. Василишин, к.т.н., доц.; О.В. Висоцький, к.т.н., доц.; О.Г. Лебедєв, к.т.н., доц.
Харківський університет Повітряних Сил імені Івана Кожедуба

Оцінювання кутових координат джерел випромінювання з надрозділенням є однією з важливих задач радіолокації (наприклад, пеленгація джерел активних шумових завад). Власноструктурні методи, запропоновані для вирішення цієї задачі, вимагають значно меншого обсягу обчислень у порівнянні з методом максимальної правдоподібності (МП) і при високому відношенні сигнал-шум (ВСШ) мають близькі до методу МП точністні характеристики. Проте при низькому ВСШ або малому числі вибірок даних, отриманих на виході антенної решітки радіолокаційної станції, їх характеристики погіршуються. Серед ряду підходів, запропонованих для покращення точністних характеристик власноструктурних методів викликає інтерес метод псевдошумового розмноження вибірки, запропонований О. Гершманом. По аналогії з бутстрепом даний метод дозволяє отримувати синтетично згенеровані вибірки (псевдовибірки) на основі отриманих вибірок даних. В роботі метод псевдошумового розмноження вибірки використано для унітарного методу Root-MUSIC, в якому враховується персиметрія просторової кореляційної матриці. Результати проведеного імітаційного моделювання вказують на покращення точністних характеристик унітарного методу Root-MUSIC за рахунок використання методу псевдошумового розмноження вибірки в умовах низького ВСШ.

МОДИФІКОВАНИЙ МЕТОД ROOT-MIN-NORM

В.І. Василишин, к.т.н., доц.; О.В. Нікітін, к.т.н., доц.;
Ф.Ф. Мисик, к.т.н., доц.; М.О. Глущенко
Харківський університет Повітряних Сил імені Івана Кожедуба

Фазовані та цифрові антенні решітки (ФАР та ЦАР) знаходять застосування в сучасних радіолокаційних станціях, системах мобільного зв'язку. Серед різноманіття розв'язуваних за допомогою ФАР (ЦАР) задач важливе місце займає оцінювання напрямків надходження сигналів. Серед запропонованих для визначення кутових координат джерел випромінювання методів особливий інтерес викликають власноструктурні методи MUSIC, Root-MUSIC, Min-Norm, Root-Min-Norm,

ESPRIT, які потребують розкладення кореляційної матриці сигналів, що приймаються антенною решіткою, за власними значеннями та власними векторами. Разом з тим точністні характеристики даних методів погіршуються при низьких (порогових) відношеннях сигнал-шум, коли мають місце так звані аномальні помилки оцінювання. Такі помилки пов'язані з можливістю прийняття одного з завадових викидів вихідного ефекту системи обробки за сигнальний. В роботі запропоновано модифікований метод Root-Min-Norm, який є комбінацією методів Root-Min-Norm та Бартлетта. Таке комбінування дозволяє зменшити вплив аномальних помилок оцінювання на точністні характеристики методу Root-Min-Norm. Результати імітаційного моделювання вказують на те, що точністні характеристики модифікованого методу Root-Min-Norm в області граничних відношень сигнал-шум є кращими у порівнянні з початковим методом Root-Min-Norm.

РАЗРАБОТКА И АНАЛИЗ ДВОХИНДЕКСНОЙ МОДЕЛИ ЧАСТОТНОГО ПЛАНИРОВАНИЯ В МНОГОКАНАЛЬНЫХ MESH-СЕТЯХ СТАНДАРТА IEEE 802.11

С.В. Гаркуша, к.т.н.; М.О. Евдокименко
Харьковский национальный университет радиоэлектроники

Беспроводные сети традиционно занимают ключевое место в системах связи военного назначения различных звеньев управления. При этом с точки зрения повышения уровня саморганизации и производительности сетей в целом заслуживает внимания подход, основанный на использовании многоканальных mesh-сетей, производительность которых во многом определяется способом распределения частотных каналов (ЧК) между радиоинтерфейса (РИ) mesh-станций. В связи с этим предложена двухиндексная математическая модель распределения ЧК в многоканальных mesh-сетях. На выходе модели сформулирована оптимизационная задача, связанная с минимизацией количества mesh-станций по доменам коллизий, взвешенных по активности и территориальной удаленности. Проведен анализ результатов аналитического моделирования (система MatLab с использованием пакета TOMLAB) и имитационного (пакет NS-3) моделирования разработанной модели распределения частотных каналов. Анализ результатов аналитического моделирования показал, что увеличение числа станций одновременно находящихся в нескольких зонах устойчивого приема, приводит к увеличению размера доменов коллизий и соответственно уменьшению производительности mesh-сети. Как показали результаты имитационного моделирования задачи распределения ЧК, использование предложенной модели позволило повысить производительность беспроводной сети на 30 – 55% по сравнению с известными методами (CoMTaC, C-Hyacinth) и в среднем в 3 – 4 раза по сравнению с одноканальными решениями.

МЕТОД ЗАБЕЗПЕЧЕННЯ ГАРАНТОВАНОЇ ЯКОСТІ ОБСЛУГОВУВАННЯ В МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

О.А. Дробот, к.т.н.; О.М. Усачов, к.т.н.; Д.Г. Еферов
Харківський університет Повітряних Сил імені Івана Кожедуба

На сьогоднішній день якість обслуговування в мультисервісних телекомунікаційних мережах (ТКМ) багато в чому визначається переліком підтримуваних засобів управління трафіком маршрутизації, резервування ресурсів, профілюванням трафіку та ін. З введенням нових послуг і підвищенням вимог до якості обслугову-

вання відповідні модифікації повинні торкнутися в тому числі протоколів і механізмів управління трафіком в ТКМ. Для вирішення зазначених проблемних питань пропонується застосування методу забезпечення гарантованої якості обслуговування (Quality of Service, QoS) для ТКМ, з метою підвищення масштабованості рішень, що сприятиме зниженню обсягів створюваного службового трафіку, розмірності і обчислювальної складності реалізації завдань забезпечення QoS обслуговування для подальшого підвищення продуктивності роботи ТКМ. Запропонований підхід повністю відповідає вимогам сучасних і перспективних технологій MultiPath Routing, QoS-Based Routing. Розвиток запропонованого підходу передбачає перехід до динамічних та стохастичних математичних моделей управління мережними ресурсами, які більш повно враховують зміну стану ТКМ, обумовлену випадковим характером структури ТКМ та характеристик абонентського трафіку.

ОЦІНЮВАННЯ ЧАСТОТ СУКУПНОСТІ ГАРМОНІЧНИХ СИГНАЛІВ МЕТОДОМ MUSIC З ВИКОРИСТАННЯМ СУРРОГАТНИХ ДАНИХ

П.Ю. Костенко, д.т.н., проф.; В.І. Василишин, к.т.н., доц.
Харківський університет Повітряних Сил імені Івана Кожедуба

Задача надрозділення за частотою є актуальною радіолокаційною задачею (наприклад, надрозділення за частотою Доплера відбитих від групової цілі сигналів в імпульсно-доплерівських радіолокаторах, при розпізнаванні цілей і т.д.), яка може вирішуватися методами спектрального аналізу. Серед методів спектрального аналізу з надрозділенням особливе місце займають власноструктурні методи (MUSIC, Root-MUSIC, ESPRIT, Min-Norm та інші). Проте при низькому відношенні сигнал/шум (ВСШ) або малій кількості даних ефективність спектрального аналізу (точність оцінювання, розділювальна здатність) погіршується. Для збереження ефективності спектрального аналізу в указаних умовах запропоновано методи, отримані модифікацією методу бутстрепу (формування псевдовибірок на основі отриманих даних). Дані методи зберігають кореляційні та *енергетичні властивості сигналів.* Однак вони є недостатньо ефективними в умовах когерентної обробки сигналів. Тому в роботі для формування псевдовибірок запропоновано використовувати технологію формування *сурогатних даних за допомогою методу* ATS (attractor trajectory surrogates)*, що дозволяє зберегти не тільки статистичні але і топологічні властивості сигналів*. Проведене математичне моделювання демонструє збереження ефективності методу MUSIC за рахунок використання сурогатних даних в умовах малої кількості даних або низького ВСШ.

ПЕРСПЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ СЛОЖНЫХ СИГНАЛОВ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Ю.С. Литвинов, к.т.н., с.н.с.; Н.Ф. Линник, к.т.н.
Национального технического университета «ХПИ»

Для повышения частотно-энергетической эффективности каналов связи предложено использовать в качестве переносчиков информации сложные сигналы – параллельные фазово-частотно-модулированные. В результате проведенного сравнительного анализа установлено, что параллельные ФЧМ сигналы превосходят одночастотные ФМ и последовательные ФЧМ сигналы в несколько раз по показателям удельных частотных и энергетических затрат на передачу единицы информации. Данные сигналы являются одним из наиболее перспективных классов сигналов для использования в каналах связи систем передачи информации и

обладают потенциальными характеристиками, обеспечивающими достижение высокого уровня частотно-энергетической эффективности.

МАТЕМАТИЧНА МОДЕЛЬ ОПТИМАЛЬНОГО УПРАВЛІННЯ ЧЕРГАМИ НА МАРШРУТИЗАТОРАХ ТЕЛЕКОММУНІКАЦІЙНОЇ МЕРЕЖІ

М.В. Семеняка
Харківський національний університет радіоелектроніки

Однією з найважливіших задач, що вирішуються в телекомунікаційних мережах є завдання забезпечення якості обслуговування трафіків користувачів. Забезпечення якості обслуговування в свою чергу базується на узгодженій роботі різноманітних рішень з управління трафіком, це і механізми QoS маршрутизації, механізми профілювання, маркування пакетів, механізми підвищення ефективності передачі та ін. Важливе місце серед задач забезпечення якості обслуговування займають задачі управління чергами, що дозволяють покращити показники якості обслуговування шляхом ефективного управління доступними мережними ресурсами, такими як пропускна здатність каналу зв'язку. В свою чергу ефективність отриманих результатів управління чергами базується на тих математичних моделях та методах, що в них покладені. В роботі представлена потокова модель управління чергами, в якій задача балансування навантаження на буферний ресурс маршрутизатора була зведена до вирішення оптимізаційної задачі. Балансування здійснювалось за двома показниками: доступною пропускною здатністю каналу зв'язку та середньою довжиною черги з урахуванням пріоритету вхідного потоку. В результаті математичного моделювання спостерігалося оптимальне балансування черг зважене відповідно до пріоритету, вдалось забезпечити краще обслуговування трафіку з вищим пріоритетом. При цьому коефіцієнт навантаження на інтерфейс маршрутизатора зростав лінійно з ростом інтенсивності вхідних потоків.

ПЕРЕДАЧА КООРДИНАТНОЇ ІНФОРМАЦІЇ НА БОРТ ЛІТАКА ПО КАНАЛУ "ПАР-АРК"

Д.М. Воронов, к.т.н.; О.А. Павліченко; В.О. Корнєєв
Харківський університет Повітряних Сил імені Івана Кожедуба

Як відомо, до складу радіотехнічних засобів, що розміщуються на аеродромі, входять приводна аеродромна радіостанція (ПАР) та автоматичний радіокомпас (АРК), які у сукупності утворюють кутомірну радіонавігаційну систему (КРНС) "ПАР-АРК". Така система призначена для автоматичного вимірювання на борту літального апарату (ЛА) курсового кута радіостанції (ККР) з метою рішення ряду навігаційних задач. Вбачається можливим побудова каналу передачі на борт літака сигналів управління для включення в состав високоточного радіолокаційного посадочного комплексу (РЛПК) шляхом модернізації наземного і бортового обладнання КРНС "ПАР-АРК" з використанням в каналі складних сигналів. Приведено склад РЛПК, пропонується принцип побудови наземного та бортового обладнання каналу передачі сигналів управління (КПСУ), а також формувача М-послідовності. Таким чином, використання шумоподібних сигналів в каналі КРНС "ПАР – АРК", та оптимальних методів обробки на борту літака дозволяє здійснювати передачу на борт літака сигналів управління в складі високоточного радіолокаційного посадочного комплексу для оперативного усунення екіпажем помилок пілотування, підвищити скритність та завадостійкість каналу.

ЗАСТОСУВАННЯ СИГНАЛІВ СИСТЕМИ ЄДИНОГО ЧАСУ ТА ЧАСТОТИ (СЄЧЧ) ДЛЯ СИНХРОНІЗАЦІЇ ВИПРОМІНЮВАННЯ РАДІОІМПУЛЬСІВ РСДН-10

В.А. Дорощук, к.т.н., доц.; І.М. Токайський
Харківський університет Повітряних Сил імені Івана Кожедуба

Заходження до синхронізації системи РСДН-10 у сучасний час потребує великих витрат часу, сил, високої кваліфікації обслуговуючого персоналу. Виконання цієї задачі складається з зведення по частоті та по фазі високо стабільних кварцових генераторів апаратури управління та синхронізації системи. З метою підвищення оперативності в роботі обслуговуючого персоналу РСДН-10 розглянута можливість застосування сигналів системи єдиного часу та частоти (СЄЧЧ) для синхронізації випромінювання радіоімпульсів РСДН-10, які мають більш високу відносну стабільність ($1{,}5 \cdot 10 - 12$) по відношенню до відносної стабільності кварцового генераторів ($1 \cdot 10 - 9$) за рахунок попередньої атестації частот кварцових генераторів станцій РСДН. Крім цього, це дозволить здійснювати повірку кварцових генераторів та їх ремонт.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ СИСТЕМ ФАЗОВОГО АВТОПІДСТРОЮВАННЯ ЧАСТОТИ З РОЗШИРЕНОЮ СМУГОЮ ЗАХОПЛЕННЯ

Ю.І. Лосєв, д.т.н. проф.; С.А. Макаров, к.т.н., доц.;
С.М. Рот; О.М. Чекунова, к.т.н.
Харківський університет Повітряних Сил імені Івана Кожедуба

Еволюція системи фазового автопідстроювання частоти (ФАП) з розширеною смугою захоплення описується нелінійним диференційним рівнянням 4-го порядку. Отримати рішення такого рівняння у аналітичному вигляді неможливо, тому найбільш ефективним способом дослідження основних властивостей запропонованого класу систем ФАП є імітаційне моделювання на основі пакету візуального та ситуаційного моделювання Simulink програмної системи MATLAB. Імітаційне моделювання складних динамічних систем (систем ФАП з динамічно регульованими параметрами по нелінійним законам) в пакеті Simulink дозволяє: побудувати модель системи; настроїти загальні параметри системи та кожного функціонального блоку структурної схеми; проконтролювати встановлені параметри опорного генератора (ОГ) та генератора керованої напруги (ГКН), порівнюючи осцилограми їх вихідних сигналів; зняти імпульсну і передаточну характеристики фільтру, використовуючи спектроаналізатор; шляхом зміни початкової розстройки частоти ОГ та ГКН визначити смуги захоплення та утримання системи; визначити характер перехідних процесів та їх залежність від постійної часу фільтру нижніх частот.

ВИБІР ВИДУ СИГНАЛУ СИСТЕМ РАДІОДОСТУПУ НА ОСНОВІ ЧАСТОТНОЇ ЕФЕКТИВНОСТІ МЕТОДІВ МОДУЛЯЦІЇ

С.А. Макаров, к.т.н., доц.; О.А. Павліченко; В.П. Поздняк
Харківський університет Повітряних Сил імені Івана Кожедуба

Сучасні системи стільникового зв'язку та радіодоступу надають широкий спектр послуг зв'язку між абонентським та базовим (комутаційним обладнанням). Важливою проблемою цих систем є підвищення ефективності використання доступних ресурсів мережі. Основним показником якості функціонування систем радіодоступу вважають стійкість до зовнішніх завад (завмирання, міжсимвольна інтер-

ференція, багатопроміневість), яка забезпечується способом обробки сигналів, вибором параметрів модуляції, кодування, синхронізації, протоколів доступу до каналу. Однак, ці параметри суттєво впливають на частотну ефективність системи радіозв'язку. Кількісна оцінка ефективності систем зв'язку характеризується коефіцієнтом частотної ефективності, який залежить від швидкості передачі інформації та ширини смуги частот сигналу обраного стандарту. Важливим етапом проектування систем радіозв'язку є оптимальний вибір методу та числа позицій модуляції, який забезпечить найбільшу ефективність системи, тобто максимальну швидкість передачі даних. При проектуванні сучасних систем зв'язку необхідно враховувати заданий рівень імовірності помилок на біт (для передачі мови приймається рівним 10-3, а для міжкомп'ютерного зв'язку – 10-19…10-20). Наприклад, у персональних мережах бездротового доступу найбільш висока частотна ефективність досягається у стандарті IEEE 802.15.3 за рахунок використання багатопозиційної амплітудно-фазової модуляції (64-QAM), при цьому забезпечується максимальна швидкість передачі даних. При застосуванні модуляції 32-QAM або квадратурної фазової модуляції (QPSK) максимальна швидкість передачі даних знижується.

ЗВ'ЯЗОК ДОЦІЛЬНОГО ТЕМПУ ПЕРЕДАННЯ НА БОРТ ЛІТАКА СИГНАЛІВ УПРАВЛІННЯ З ПАРАМЕТРАМИ РАДІОКАНАЛУ ТА ПІЛОТАЖНИХ ПРИЛАДІВ

С.А. Макаров, к.т.н.,доц.; М.Д. Рисаков, к.т.н.,доц.; Р.В. Воробйов; С.А. Кочура
Харківській університет Повітряних Сил імені Івана Кожедуба

Важливими характеристиками каналу передання на борт сигналів управління (КПСУ) посадкою літака є темп (періодичність) їх передання та форма представлення екіпажу. Потреба в КПСУ виникає при рішенні завдань виводу літака в розрахункову точку посадки в складних метеорологічних умовах. При побудові таких КПСУ для літаків ТА доцільно передбачити використання існуючих пілотажних приладів та можливість мінімальних доробок бортового обладнання. Таким приладом є командно-пілотажній прилад (КПП), що є для екіпажу індикатором кутових відхилень літака від заданої траєкторії посадки (ЗТП). Використання КПП у якості індикатору лінійних відхилень, що передані по КПСУ, визначає можливій темп $F_м$ передання по КПСУ координатної інформації, якій випливає з інерційності F_i приладу за принципом $F_м \geq F_i$. З іншого боку, максимально значення F_{max} темпу $F_м$ обмежується смугою перепускання радіоканалу та обсягом координатної інформації, що перелається. У доповіді пропонується методика вибору доцільного темпу передання по КПСУ координатної інформації по значенням інерційності F_i КПП, смузі перепускання приймача радіоканалу та обсягу координатної інформації, що передається. Методика дозволяє оптимально вибрати частотні характеристики КПСУ для його розробки або засоби радіотехнічного забезпечення для побудові КПСУ шляхом їх незначної доробки.

ОСОБЛИВОСТІ РОБОТИ АДАПТИВНОГО КОГЕРЕНТНОГО НАКОПИЧУВАЧА ВІДБИТТІВ У ЗОНІ ПОСАДКИ АЕРОДРОМУ

М.Д. Рисаков, к.т.н., доц.; В.В. Куценко; В.Г. Карєв; В.А. Дорощук, к.т.н., доц.
Харківській університет Повітряних Сил імені Івана Кожедуба

Для підвищення відношення сигнал/завада на виході радіолокаційного приймача та суттєвого послаблення впливу, що заважає пасивних завад (ПЗ) у окремих сучасних РЛС виконується когерентне сумування по Nн імпульсів пачки відбиття в

доплерівських фільтрах накопичувача. При цьому для суттєвого зменшення рівня накопичення ПЗ у фільтрах виконується згладжування бокових пелюстків амплітудно-фазових характеристик фільтрів. До недоліків такої фільтрації відбиттів слід віднести накопичення у нульовому та сусідніх з ним фільтрах не тільки ПЗ але й також окремих імпульсів літаків, швидкість котрих близька до "сліпої". Для РЛС, що здійснює радіолокаційній контроль зони посадки аеродрому, в апаратурі цифрової обробки сигналів (ЦОС) є можливість реалізувати адаптивній алгоритм накопичення імпульсів літака у фільтрах без незначного накопичення ПЗ. У доповіді обґрунтовується можливість реалізації та особливості адаптивного алгоритму роботи когерентного накопичувача в складі апаратурі ЦОС посадкового радіолокатора та апаратурі ЦОС моноімпульсної РЛС автосупроводження. В обох випадках сутність адаптивного алгоритму роботи полягає в підборі значення періоду зондування, при якому забезпечується накопичення імпульсів літаків у фільтрах без ПЗ. Для цього в складі апаратури ЦОС використається вимірювач швидкості літака.

СПОСІБ ЗАБЕЗПЕЧЕННЯ ІДЕНТИЧНОСТІ АМПЛІТУДНИХ ХАРАКТЕРИСТИК КАНАЛІВ ПРИЙМАЧА МОНОІМПУЛЬСНОЇ РЛС АВТОСУПРОВОДЖЕННЯ ЛІТАКА

М.Д. Рисаков, к.т.н.,доц.; І.В. Тітов, к.т.н.;
О.П. Кулик, к.військ.н.; О.А. Павліченко
Харківській університет Повітряних Сил імені Івана Кожедуба

При керуванні польотами літаків у зоні посадки керівник користується радіолокаційною інформацією, що відображається на виносних індикаторах посадкового радіолокатору (ПРЛ). На жаль, недостатні точність та частота вимірювання координат у існуючих ПРЛ не дозволяють їх використати для побудови автоматизованих систем управління посадкою літака (АСУ ПЛ) у складних метеоумовах. Доцільним напрямком у створенні АСУ ПЛ може стати використання в складі радіолокаційного комплексу посадки літаків моноімпульсної РЛС (МРЛС) автосупроводження з реалізацією амплітудних способів пеленгації літака та доплерівської фільтрації його відбиттів. Для отримання високої точності вимірювання координат літака за допомогою названої МРЛС необхідно забезпечити високу ідентичність амплітудних характеристик двох приймальних трактів координатної площині. Для забезпечення ідентичність амплітудних характеристик каналів приймача в доповіді пропонуються схемні рішення способу вирівнювання коефіцієнтів підсилення в кожної пари каналів. Сутність способу полягає в забезпеченні проходження малої частині енергії зондувального сигналу каналів приймача кожної площині, вимірювання різності амплітуд цих імпульсів на виходах і формуванні відповідних напруг управління коефіцієнтами підсилення двох приймальних трактів у напрямку їх вирівнювання.

ОСОБЛИВОСТІ РОЗРОБКИ ПРОГРАМНИХ МОДЕЛЕЙ ЗРАЗКІВ ОЗБРОЄННЯ ДЛЯ ПРОВЕДЕННЯ КОНТРОЛЮ ФУНКЦІОНУВАННЯ

Антонов Д.В.
Харківський університет Повітряних Сил імені Івана Кожедуба

Вибір середовища розробки програмного забезпечення може частково уніфікувати процес розробки та створення програмних моделей на вимоги замовника, стандартизувати інтерфейс, елементи керування, контролю та сигналізації. Кожне з найбільш поширених середовищ розробки має свої позитивні та негатив-

ні риси. Borland Delphi, Borland C++ Builder дозволяють швидко та зручно описати алгоритми програмних моделей, але для побудови тотожних елементів керування (тумблери, перемикачі) треба застосовувати сторонні графічні пакети, наприклад Corel Draw. Macromedia Flash дозволяє об'єднати процес програмування та створення графічних елементів, але проект будується у вигляді файлу .flv, який потребує запуску із flash-програвача, що не завжди зручно. Для конвертування у формат виконуємого файлу .exe також необхідно застосовувати сторонні програми. У цьому випадку зростає об'єм .exe файлу порівняно із Borland Delphi/C++ Builder. При побудові частини алгоритму, яка відповідає за навчання різним режимам роботи або порядку проведення контролю функціонування елементів зразків озброєння є сенс звернутися не до програмування цього алгоритму, а до запису відео з екрану монітору у файл .avi. Наведені особливості дозволять уніфікувати процес розробки та створення програмних моделей, скоротити час та стандартизувати інтерфейс, елементи керування, контролю та сигналізації.

ИСПОЛЬЗОВАНИЕ СИСТЕМ MIMO ДЛЯ УВЕЛИЧЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ И ПОВЫШЕНИЯ НАДЕЖНОСТИ СИСТЕМ СВЯЗИ

А.П. Зелинский; В.Н. Симоненков; Ж.А. Хижняк
Военная академия, Одесса

В настоящее время в системах связи существует необходимость повышения пропускной способности (ПС), которая может быть увеличена с помощью расширения полосы частот или повышения излучаемой мощности. Но, из-за требований электромагнитной совместимости и биологической защиты, расширение полосы частот и повышение мощности ограничено. Одним из эффективных способов решения этой проблемы является применение антенных решеток с слабонаправленными антенными элементами. Системы связи, которые используют такие антенны, получили название систем MIMO (Multiple-Input-Multiple-Output), "множественный вход – множественный выход", в которых несколько передатчиков и несколько приемников, разнесенных в пространстве, создают уникальные каналы информационного обмена внутри одного участка спектра. Эти каналы образуются разделением информационных потоков во времени и пространстве. Такая технология позволяет повысить ПС за счет разделения исходного потока данных между двумя и более пространственными каналами. В условиях релеевских замираний сигналов технология MIMO позволяет увеличивать ПС пропорционально числу таких каналов, без повышения излучаемой мощности и расширения полосы частот. Рассмотрены возможные варианты реализации технологии MIMO на базе адаптивных антенных решеток. Приведены количественные результаты, которые иллюстрируют эффективность информационных систем подобного класса.

АПАРАТНО-ПРОГРАМНА МОДЕЛЬ ДИСПЕТЧЕРСЬКОГО РАДІОЛОКАТОРУ РАДІОЛОКАЦІЙНОЇ СИСТЕМИ ПОСАДКИ В СКЛАДІ ТРЕНАЖНО-ІМІТАЦІЙНОГО КОМПЛЕКСУ "ВІРАЖ-АВІА"

Д.Ю. Свистунов, к.т.н., с.н.с.; С.П. Лешенко, д.т.н., с.н.с.
Харківський університет Повітряних Сил імені Івана Кожедуба

Велика вартість закупівлі й експлуатації сучасного озброєння не дозволяє проводити на ньому усі види бойової підготовки особового складу. Навіть в економічно розвинутих країнах первинне навчання проводиться, як правило, на тренажерах. Тому

питання розробки тренажерних комплексів є актуальним для збройних сил будь-якої держави, у тому числі й України. При підготовці курсантів спеціалізації "Бойове управління польотами авіації" в Харківському університеті Повітряних Сил формування їх високого рівня професійності в керівництві польотами необхідно здійснювати шляхом систематичних, цілеспрямованих тренувань в умовах, що наближені до реальних. В Харківському університеті Повітряних Сил створено апаратно-програмний комплекс "ВІРАЖ-АВІА" для проведення тренувань офіцерів бойового управління командно-диспетчерських пунктів у масштабі реального часу. Розроблені математичні моделі та відповідне програмне забезпечення імітації роботи диспетчерського та посадкового локаторів радіолокаційної системи посадки (РСП). Імітована сигнально-завадова обстановка видається на робочі місця групи керівництва польотами, що обладнані виносними індикаторами системи посадки. В доповіді викладені задачі, принципи побудови та технічні характеристик пристрою, який моделює роботу диспетчерського локатору у складі радіолокаційної системи посадки з видачею інформації на штатні робочі місця виносних індикаторів системи посадки.

УПРАВЛЕНИЕ ДВИЖЕНИЕМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ЭКСТРЕМАЛЬНЫХ УСЛОВИЯХ: АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ПРИНЯТИЯ РЕШЕНИЙ

А.И. Тимочко, к.т.н., доц.
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Управление движением истребителями в экстремальных условиях автоматизировано слабо. Оперативность принятия решений остается низкой, а эффективность управления летательными аппаратами – недостаточной. Следовательно, необходима разработка подходов к автоматизации процессов принятия решений по управлению движением истребителями в экстремальных условиях. Для этого необходимо последовательно решить следующие взаимосвязанные задачи: проанализировать современное состояние автоматизации процессов принятия решений по управлению летательными аппаратами; разработать методы и средства формализации задач принятия решений по управлению летательными аппаратами при ликвидации ими угроз и вызовов и их последствий; предложить методы формализации знаний и манипулирования ими для поддержки принятия решений при наведении истребительной авиацией на воздушные цели; синтезировать методы нечетких логических выводов на логико-лингвистических продукционных иерархических моделях при управлении истребителями; разработать методы и модели рефлексивного выбора действий при управлении летательными аппаратами; реализовать задачу наведения в специализированной АСУ на основе объектно-ориентированного подхода; оценить эффективность разработанных методов по управлению истребителями.

ПІДСЕКЦІЯ 8.2

КОДУВАННЯ ІНФОРМАЦІЇ В СИСТЕМАХ ЗВ'ЯЗКУ

Керівники підсекції: генерал-майор О.І. Кушнір;
д.т.н. професор О.О. Кузнецов
Секретар підсекції: майор О.В. Першин

МЕТОД ДИНАМИЧЕСКОГО КОДИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОЗАЩИЩЕННОСТИ, ИМИТОСТОЙКОСТИ И СКРЫТНОСТИ РАДИОКАНАЛОВ УПРАВЛЕНИЯ

Ю.В. Стасев, д.т.н., проф.; А.А. Кузнецов, д.т.н., проф., С.Ю. Стасев
Харьковский университет Воздушных Сил имени Ивана Кожедуба

В современных условиях вероятностно-временные требования к автоматизированным системам управления войсками и оружием существенно возросли. Перспективная система управления должна обеспечить доведение сигналов и команд в условиях резко возросших объемов обрабатываемых и передаваемых данных, активных действий частей и подразделений РЭБ противника. Проведенный анализ показал, что повышение защищенности от преднамеренных помех противника, имитостойкости и скрытности радиоканалов управления на сегодняшний день достигается за счет использования сложных дискретных сигналов с нелинейными законами формирования манипулирующих последовательностей, а также реализации динамических режимов их передачи, при которых соответствие бит информации сложным сигналам изменяется с течением времени по закону, предсказание которого возможно с вероятностью, не превышающей заданной величины. Применение динамических режимов функционирования на уровне контура избыточного кодирования позволяет обеспечить повышение помехозащищенности, имитостойкости и скрытности радиоканалов управления. Информационная скрытность, имитозащищенность моноканала на уровне динамического контура кодирования определяется размерами ансамблей разрешенных к использованию параметров кода, а также устойчивостью управляющей последовательности.

МОДЕЛИ И МЕТОДЫ КЛЮЧЕВОГО ХЕШИРОВАНИЯ ИНФОРМАЦИИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

А.А. Кузнецов[1], д.т.н., проф.; О.Г. Король[2]; Л.Т. Пархуць[3], д.т.н., доц.
[1]Харьковский университет Воздушных Сил имени Ивана Кожедуба
[2]Украинская государственная академия железнодорожного транспорта;
[3]Национальный университет «Львівська Політехніка»

Для исследования коллизионных свойств схем хеширования предлагается подход, основанный на использовании уменьшенных моделей (мини-версий) всех слоев преобразования. Предложенный подход реализован при разработке мини-версии алгоритма ключевого хеширования UMAC. Разработанная модель (мини-UMAC), используя уменьшенные модели отдельных слоев преобразований, на основе оценки распределения столкновений формируемых образов позволяет экспериментально исследовать коллизионные свойства кодов аутентификации сообщений. Перспективным в этом смысле является разработка математического

аппарата для исследования коллизионных свойств схем ключевого хеширования с использованием соответствующих мини-версий, а также проведение экспериментальных исследований коллизионных свойств каскадного ключевого хеширования информации на примере мини-UMAC.

СИНТЕЗ НЕЛИНЕЙНЫХ ЭЛАСТИЧНЫХ ФУНКЦИЙ С ИСПОЛЬЗОВАНИЕМ ДВОИЧНЫХ БЛОКОВЫХ КОДОВ

А.А. Кузнецов[1], д.т.н., проф.; Г.С. Цымбал[2]; Ю.Н. Рябуха[1], к.т.н.
[1]Харьковский университет Воздушных Сил имени Ивана Кожедуба;
[2]Украинская государственная академия железнодорожного транспорта

Построение криптографических узлов замен с высокими показателями нелинейности и алгебраической степени является важнейшей задачей в современной теории защиты информации [1]. В работе были исследованы криптографические узлы замен, которые основаны на эластичных криптографических функциях. Для этого на основе метода [2] были получены нелинейные эластичные функции, из различных классов двоичных линейных блоковых кодов. В результате проведенных исследований было показано, что с помощью рассмотренного метода [2] можно синтезировать эластичные булевы функции, обладающие корреляционным иммунитетом заданного порядка, с высокими показателями нелинейности. Следует отметить, что нелинейность полученных функций, не превышает известные ранее результаты [1]. Однако, перспективным направлением, по мнению авторов, является использование недвоичных блоковых кодов для синтеза эластичных функций, разработка вычислительных алгоритмов их построения и анализа.

МЕТОДИКА ПОБУДОВИ ПРОФІЛЮ ЗАХИСТУ ДЛЯ БЕЗДРОТОВОЇ МЕРЕЖІ НА ОСНОВІ ВІДПОВІДНОГО РІВНЯ ДОВІРИ

Д.Ю. Голубничий, к.т.н., доц.; С.М. Грабар
Харківський університет Повітряних Сил імені Івана Кожедуба

Для побудови профілю захисту для бездротової мережі спочатку необхідно провести аналіз самої мережі на предмет реалізованих в ній механізмів захисту, причому варто відзначити, що особливу увагу потрібно приділити розмежуванню основних механізмів захисту, описаних в сімействі стандартів 802.11. Всю процедуру формування профілю захисту можна розділити на декілька етапів: аналіз об’єкту оцінки на відповідність його системи захисту стандартам 802.11 з використанням критеріїв оцінки захищеності; знаходження рівня довіри до об’єкту оцінки; формування профілю захисту з використанням базового функціонального пакету для відповідного рівня. Необхідно врахувати, що через специфіку функціонування бездротової мережі, захист компонентів інформаційної системи від несанкціонованого фізичного доступу утруднений. У зв'язку з цим, тривале зберігання конфіденційної інформації, і інших активів, що захищаються, на даних компонентах неможливо. При описі середовища безпеки об’єкту оцінки необхідно акцентувати увагу на припущеннях безпеки, пов'язаних з фізичним захистом бездротової мережі, і передбачуваних погрозах по відношенню до бездротової мережі через її широкомовну природу. Також варто відзначити, що активи бездротової мережі можуть бути доступні зовнішнім інформаційним системам, які знаходяться поза політикою безпеки об’єкту оцінки. Хоча користувачі зовнішніх інформаційних систем можуть бути якоюсь мірою довіреними, вони знаходяться поза областю управлін-

ня цим конкретним об'єктом оцінки, і так як ніхто не може припускати про їх наміри, то вони не повинні розглядатися як довірені користувачі.

ВИКОРИСТАННЯ АЛГЕБРО-ГЕОМЕТРИЧНИХ КОДІВ ДЛЯ ПОБУДОВИ ШИРОКОСМУГОВИХ СИГНАЛІВ

О.О. Кузнецов, д.т.н., проф.; А.М. Коваленко
Харківський університет Повітряних Сил імені Івана Кожедуба

Використання широкосмугових сигналів в сучасних системах зв'язку є достатньо розповсюдженим явищем. Для цих систем, актуальною є завдання вдосконалення за рахунок оптимізації характеристик ансамблів сигналів, що використовуються. Алгебро-геометричні коди мають добрі якості, тому їх використання є доволі перспективним для побудови ансамблів широкосмугових сигналів з поліпшеними характеристиками.

АНАЛІЗ МЕТОДІВ КРИПТОАНАЛІЗУ АЛГОРИТМІВ СПРЯМОВАНОГО ШИФРУВАННЯ

О.В. Сєвєрінов, к.т.н. доц.; С.Г. Перебийніс
Харківський університет Повітряних Сил імені Івана Кожедуба

Криптографічний алгоритм можна розглядати з двох різних точок зору: з одного боку, це абстрактний математичний об'єкт, що переводить деякий вхідний текст у вихідний текст, з іншого боку, цей алгоритм повинен бути реалізований у програмі, що виконується на певному процесорі, на певному обладнанні, та буде володіти певною специфікою, притаманною саме цій реалізації. Класичний криптоаналіз розглядає криптографічні алгоритми з першої точки зору. Другий підхід використовується в атаках спеціального виду. Криптоаналіз на основі атак спеціального виду використовує особливості реалізації, щоб дізнатися ключові параметри, що використовувані в обчисленнях. Атаки спеціального виду використовують данні, отримані у результаті спостереження за фізичним процесом роботи пристрою, що реалізує криптографічний алгоритм. Найбільш поширені атаки за часом, на основі вимірювання енергоспоживання, по електромагнітному випромінюванню, на основі акустичного аналізу, диференціального аналізу помилок, атаки з зондуванням та з внесенням помилок. Спеціальний криптоаналіз є індивідуальним, так як він працює тільки для заданої реалізації, однак проведений аналіз показав, що цей криптоаналіз часто значно більш потужний, ніж класичний.

АНАЛІЗ ВИМОГ ДО ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

О.В. Сєвєрінов, к.т.н. доц.; О.В. Проніна
Харківський університет Повітряних Сил імені Івана Кожедуба

Основними складовими систем захисту інформації є засоби генерування ключів і параметрів. Існуючі методи генерування можна розділити на два великі класи - випадкові і детерміновані генератори випадкових послідовностей. Вимоги до генераторів представлені в міжнародному стандарті ISO/IEC 18031. Серед основних вимог до генераторів псевдовипадкових послідовностей на сьогодні відносять: невідмітна, безповоротність, непередбачуваність, швидкість. Основні вимоги діляться на вимоги до початкових даних, вимоги до роботи генератора і функціональні вимоги. Крім того однією з вимог до генераторів псевдовипадкових послідовностей є позитивна оцінка

за наслідками графічних і статистичних тестів. Графічні тести є суб'єктивними, так як їх результати інтерпретуються людиною, а тому висновки на їх основі можуть бути неоднозначними. Рішення щодо випадковості послідовності, що пройшла статистичні тести, приймається на основі чітких математичних критеріїв. Вимоги міжнародного стандарту ISO/IEC 18031 можуть застосовуватися до будь-якого генератора випадкових бітів, як детермінованого, так і недетермінованого.

АНАЛІЗ МЕТОДІВ КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

О.В. Сєвєрінов, к.т.н. доц.; О.Ю. Пузирьков
Харківський університет Повітряних Сил імені Івана Кожедуба

Захист комп'ютерних систем від несанкціонованого доступу ґрунтується на спеціальних засобах ідентифікації користувача, основним з яких є використання паролів. Проте слабкий парольний захист не задовольняє сучасному рівню вимог інформаційної безпеки. Надійність цього способу ідентифікації в значній мірі залежить від людського чинника. Крім того застарілий і принцип розділення методів контролю фізичного доступу і контролю доступу до інформації. Рішення цих проблем можливо на основі застосування для ідентифікації особи біометричних характеристик людського організму. Недоліками біометричних систем є їх складність, можливість підробки відмінної риси, відтворення поведінки користувача. Для підвищення безпеки необхідно використовувати декілька чинників ідентифікації, при цьому біометрію поки відносять до додаткових методів, що дозволяють ідентифікувати користувача. Тому необхідно проведення роботи по усуненню недоліків систем біометричної ідентифікації для їх більшого застосування.

СПОСОБ ОТЫСКАНИЯ ПРИМИТИВНЫХ МНОГОЧЛЕНОВ В ДВОИЧНОМ ПОЛЕ

И.Г. Кириллов, к.т.н. с.н.с., доц.; А.Я. Слободянюк
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Широкое использование современных информационных технологий при организации обмена данными в КСА АСУ специального назначения требует повышенного внимания к решению задач криптографической защиты информации и помехоустойчивого кодирования. Вопросам развития теории конечных полей, лежащей в основе решения таких задач, посвящена обширная литература. Однако практические способы решения некоторых частных задач, имеющих и общетеоретическое значение, освещены на взгляд авторов недостаточно. Предлагается способ отыскания примитивных многочленов в двоичном расширенном конечном поле Галуа, основанный на учете свойств проверочной матрицы несистематического кода Хэмминга примитивной длины с конструктивными параметрами (2^m-1, 2^m-1-m, 3). Эти многочлены в частности могут использоваться для генерации таких кодов. Учет того факта, что m-мерные столбцы проверочной матрицы представляют собой различные (2^m-1) кодов, позволяет получить все примитивные многочлены методом простого перебора коэффициентов g_i ($i \in 1, m-1$) полинома g(x) степени m ($g_0 = g_m = 1$), представляющих элементы поля GF(2). Для случая больших m оказывается достаточным отыскание одного примитивного многочлена. Остальные могут быть получены выбором из минимальных многочленов на основе учета отмеченных выше свойств проверочной матрицы.

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ В ДВОИЧНО-ЧЕТВЕРИЧНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

И.В. Миронец, к.т.н.; В.В. Веретельник
Черкасский государственный технологический университет

На практике вводимая информационная избыточность преследует цели повышения надежности, помехозащищенности и отказоустойчивости функционально автономных устройств. Вместе с тем был бы идеальным случай представить всю информацию одним избыточным кодом, обеспечивающим единство процессов обнаружения и исправления ошибок на всех этапах переработки информации. Эффективность любого применяемого кода определяется, прежде всего, соответствием его реальной модели ошибок. Любое целое число X может быть представлено 2r кодом в следующем виде: $X = \pm\sum_{j=0}^{n-1}\sum_{i=0}^{r-1} x_{r\cdot i+j} ir^i,\ x \in [0;1]$. Следовательно, данные коды можно рассматривать как системы счисления. Данная система счисления получила название двоично-четверичной системы счисления с постоянным числом единиц. Синтезированные системы счисления с постоянным числом единиц являются частным случаем кодов с постоянным числом единиц, поэтому они предназначены для обнаружения ошибок в каналах передачи, хранения и обнаружения информации. На основании разработанной двоично-четверичной системы счисления, для 24 исследованных логических функций кодирования-декодирования в двоичной системе были получены соответствующие функции кодирования и декодирования.

ДОСЛІДЖЕННЯ ГРУПИ ТРЬОХРОЗРЯДНИХ КРИПТОГРАФІЧНИХ ОПЕРАЦІЙ

В.Г. Бабенко, к.т.н.; С.В. Рудницький
Черкаський державний технологічний університет

В попередніх роботах доведено, що синтезовані трьохрозрядні криптографічні операції утворюють групу. Основною задачею, яка вирішується, є знаходження функцій перекодування, які формуються з визначеного набору логічних операцій за допомогою операції композиція, для двох заданих функцій кодування, тобто дослідження функціональних залежностей між синтезованими функціями кодування, при чому функція перекодування теж повинна належати множині функцій кодування. Якщо процес перекодування видозмінити так, щоб при застосуванні функції криптографічного перетворення над даними, які закодовані першим користувачем, безпосередньо одержували дані, які закодовані другим користувачем, без необхідності реалізації процесу декодування для повторного кодування. Звідси виходить, що дійсно застосування операції перекодування зменшує кількість перетворень, що потрібно виконати: $x_i^{**} = f_{\text{перекод}}(x_i^*) = f_{\text{код2}}(f_{\text{декод}}(f_{\text{код1}}(x_i)))$, де $x_i^* = f_{\text{код1}}(x_i)$, $x_i = f_{\text{декод}}(x_i^*)$; $x_i^{**} = f_{\text{код2}}(x_i)$. Для спрощення отримання математичної моделі побудови операцій перекодування ми розглядали поєднання логічних операцій без врахування інверсії. В результаті проведення досліджень було одержано модель синтезу групи операцій перекодування на базі групи трьохрозрядних логічних операцій, що забезпечують криптографічне перетворення, без врахування інверсій відповідно до матричного представлення вхідної та вихідної логічних операцій.

СТРУКТУРНАЯ ИДЕНТИФИКАЦИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ПРОЦЕССЕ ИХ МОДЕЛИРОВАНИЯ

С.Г. Семенов, к.т.н.
Национальный технический университет «ХПИ»

В настоящее время состояние информационно-телекоммуникационных систем (ИТС) характеризуется многообразием структурных элементов, сложностью алгоритмов и процедур управления. Украинские операторы связи интенсивно занимаются поиском решений в обеспечении качества телекоммуникационных услуг. Анализ протоколов и рекомендаций международного союза электросвязи показал, что, одной из основных характеристик качества обслуживания при передаче данных является безопасность информации циркулирующей в ИТС. Проведенные исследования показали, что, несмотря на большой выбор средств обеспечения безопасности и широкий спектр вариантов построения защищенных ИТС, остается нерешенной задача оптимального выбора вариантов, обеспечивающих максимальные показатели безопасности. Для решения указанной задачи возникает необходимость в разработке и исследовании математических моделей защищенных ИТС. В докладе проведена постановка задачи математического моделирования защищенной ИТС и представлена динамическая модель защищенной ИТС с учетом апостериорных данных. В ходе математического моделирования проведены исследования метрических и графических методов структурной идентификации. Получены качественные и количественные результаты, позволяющие классифицировать различные структурно-функциональные элементы ИТС. Результаты исследований дали основания предположить целесообразность использования методов структурной идентификации в процессе оптимизации защищенных ИТС.

ВСТРАИВАНИЕ ДАННЫХ В ЧАСТОТНУЮ ОБЛАСТЬ НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

А.А. Смирнов, к.т.н., доц.
Кировоградский национальный технический университет

Методы цифровой стеганографии находят в последнее время все большее применение. Помимо сокрытия смыслового содержания передаваемых сообщений их использование позволяет скрыть сам факт организации скрытного канала связи, что является особенно полезным в ряде инфокоммуникационных систем специального назначения. Стеганографическая защита информации заключается в сокрытии от противника информационных сообщений в контейнерах – цифровых данных с высоким уровнем естественной избыточности. Если встраивание информационных данных не привело к порче данных контейнера (например, не ухудшилось восприятие контейнера органами чувств человека), тогда передача заполненных контейнеров по каналам связи не вызывает попыток у противника уничтожить контейнер или, по крайней мере, нарушить (испортить) информационное содержимое контейнера. Т.е. таким способом скрывается сам факт организации скрытной передачи данных, а не только содержательная часть встроенных информационных сообщений. Современные стеганосистемы используют в качестве контейнеров цифровые изображения и аудио-сигналы, текстовые документы, сигналы телеметрии и пр. Наибольшее распространение в последние годы получили стеганосистемы с неподвижными изображениями в качестве цифровых контейнеров. Проблема встраивания информационных сообщений в этом

случае осложняется возможностью противника применять методы сжатия изображений, что неизбежно отразиться на качестве скрытно встроенных сообщений. Современные алгоритмы сжатия неподвижных изображений основаны на использовании сложных, многоэтапных преобразований, в основе которых лежит обработка данных изображения в частотной области. Например, алгоритм сжатия JPEG использует для этих целей развитый математический аппарат дискретно-косинусного преобразования. Цифровые компоненты изображения в частотной области несут основную визуальную информацию, и их обработка осуществляется с учетом особенностей зрительной системы человека. Предлагается метод встраивания данных в частотную область неподвижных изображений с использованием технологии прямого расширения спектра. Данные информационного сообщения модулируются шумоподобными дискретными сигналами с большой базой, благодаря чему достигается расширение спектра. Полученные модулированные сигналы принимают вид псевдослучайных последовательностей, что позволяет обеспечить скрытность и помехозащищенность передачи данных. Сформированные модулируемые сообщения добавляются к цифровым данным контейнера-изображения в частотной области, в результате чего формируется стеганограма (заполненный контейнер). За счет незначительной амплитуды шумоподобных дискретных сигналов цифровые данные контейнера искажаются незначительно, то есть зрительная система человека не воспринимает внесенные погрешности в заполненном контейнере. В результате чего удается организовать скрытный канал передачи данных путем передачи заполненного контейнера по открытым каналам связи.

СПОСІБ СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ

В.І. Бритик, к.т.н.; Б.І. Борзенков, к.т.н.; Є.В. Струков
Харьківський національний університет радіоелектроніки

Для забезпечення криптографічного захисту інформації, переданої по мережах зв'язку, розглядається спосіб з використанням симетричного ключа, який полягає в тому, що шифрування здійснюється за допомогою блокового шифру з 256-бітовим ключем і 32 циклами перетворення, що оперує 64-бітними блоками і використовує мережу Фейстеля. Формування ключів і підключів виконується за допомогою трьох детермінованих складових, які є випадковими щодо інформації. При цьому ключ формується в три етапи – передача інформації щодо зображення, передача інформації про локальні фрагменти на зображенні, передача інформації про значення фільтра, що дозволяє сформувати значення ключа W шляхом конкатенації координат, отриманих у результаті згортки точок локального фрагмента з маскою, що визначається деякою особливістю цього фрагменту за формулою, яка є випадковою щодо інформації, але X постійна щодо процесу шифрування-розшифрування і яка є складовою ключа. Ключі генеруються випадковим образом за допомогою виконання операції згортки обраних локальних фрагментів L, одного із множини K зображень, розміром M*N, наведеного у вигляді двовимірного масиву дійсних чисел B[xi, yj] – значень інтенсивності (яскравості для напівтонового зображення), а xi, yj – номера рядків і стовпців, відповідно, а локальні фрагменти L визначаються шляхом завдання їхніх геометричних особливостей – координат точок вершин багатокутників S або центрів і радіусів кіл S, необов'язково покриваючи все зображення та однієї або декількох масок – цифрових фільтрів із множини F, що зображають собою матрицю дійсних значень фільтра розміром P×Q. Користувач довільним образом обирає деяке зображення, довільного розміру, наприклад N×M, із множини K, задає множину L довільних S-вугільних фігур,

що покривають зображення, які є початковими даними для формування коду шифрування. Загальна кількість фільтрів залежить від розмірів (P×Q). За допомогою обраного фільтра на заданій множині L виділяємо характерні точки, отримані у результаті згортки точок локального фрагмента з маскою. Цифровий підпис забезпечується передаванням зворотного повідомлення, закодованого зміненим кодом; генерація ключів поєднує у собі простоту запам'ятовування та використання генератора «натурального» випадкового процесу. Накопичення ключів у вигляді їхніх складових виключає можливість зчитування, розподіл ключів (прямий обмін ключами між користувачами інформаційної системи) дозволяє виконати ідентифікацію.

АРХІТЕКТУРА СИСТЕМИ ВИЯВЛЕННЯ АТАК

Д.Ю. Голубничий, к.т.н., доц.; О.Ю. Сироватський
Харківський університет Повітряних Сил імені Івана Кожедуба

Визначається, що до складу системи виявлення атак можуть входити наступні модулі: мережний сенсор; вузловий сенсор; консоль управління; база даних сигнатур атак та агенти реагування. Мережний сенсор призначений для аналізу поведінки мережних об'єктів на основі даних мережного трафіку і повідомлень від вузлових сенсорів. Ядром аналізу є система підтримки виконання програм. Вузловий сенсор призначений для аналізу поведінки мережних об'єктів комп'ютерної мережі на основі даних системних журналів і подій операційної системи. База даних системи виявлення атак є розподіленим сховищем описів нормальної і аномальної поведінки об'єктів комп'ютерної мережі, повідомлень про атаки і журналу компонентів системи виявлення атак. Консоллю управління є графічний додаток управління системи виявлення атак, в завдання якого входить: відображення фізичної і логічної структури системи виявлення атак і захищеної комп'ютерної мережі; управління і настройка компонентів системи виявлення атак; сповіщення оператора про події безпеки в режимі реального часу (візуальні і звукові ефекти); кореляція повідомлень про атаки; централізоване реагування; візуалізація повідомлень про атаки і журналу компонентів. Агенти реагування системи виявлення атак встановлюються на вузли комп'ютерної мережі, де встановлені засоби реагування (міжмережні екрани), або на контрольовані вузли комп'ютерної мережі, і виконують команди від підсистеми реагування мережного сенсора і консолі управління.

ВДОСКОНАЛЕННЯ АПАРАТНИХ ЗАСОБІВ РЕАЛІЗАЦІЇ МЕТОДУ ЗАХИСТУ ТЕХНОЛОГІЧНОЇ ІНФОРМАЦІЇ

Д.А. Жиляєв
Черкаський державний технологічний університет

Одними з найбільш простих в реалізації методів захисту технологічної інформації є методи з використанням перестановок. Хоча «в цілому» методи на основі перестановок не можуть вважатися достатньою мірою стійкими до криптоаналізу, однак для розв'язання конкретної задачі через свою простоту в реалізації можуть бути ефективно використані. У доповіді подано схему реалізації пристрою, в якому використовується перестановка трьохбайтних повідомлень, обчислено схемотехнічну складність цього пристрою. Запропоновано варіанти зміни кодів вхідних команд, побудовані карти Карно для нових команд, в результаті мінімізації яких показано що змінивши вхідні коди команд досягається зменшення складності

пристрою на 28%. Наведено вдосконалену схему пристрою перестановки трьохбайтних повідомлень з використанням вже нового набору вхідних команд. Вказується, що подібний підхід до змін кодів дозволяє зменшити схемотехнічну складність і інших пристроїв. Результат дослідження був використаний для розробки простого в реалізації і ефективного методу захисту технологічної інформації на основі перестановок.

ОБРАБОТКА КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ РАСПРЕДЕЛЁННЫХ ВЫЧИСЛЕНИЙ

В.И. Барсов, к.т.н., доц.; А.С. Фещенко
Украинская инженерно-педагогическая академия

Одной из актуальных задач нашего времени является необходимость обеспечения безопасности, достоверности и аутентификации передаваемой информации, поскольку сегодняшний Интернет и Web-технологии не рассматривают таких возможностей. Поэтому целью доклада является сформулировать концепцию создания быстрой и достоверной обработки криптографический информации на основе использования информационной технологии распределенных вычислений в модулярной системе счисления. Решить данную задачу можно используя криптографические методы защиты позволяющие осуществлять как закрытие данных, хранимых в базах данных или передаваемых по каналам связи, так и контроль целостности и аутентичности данных. Одним из практических направлений повышения пользовательской производительности и надёжности системы обработки криптографической информации (СОКИ) является внедрение нетрадиционных методов представления и параллельной обработки информации в числовых системах с параллельной структурой и таким методом может быть использование модулярной системы счисления МСС, благодаря максимальному уровню ее внутреннего параллелизма в организации процесса переработки информации и способности обнаруживать и исправлять ошибки, возникающие в динамике процесса обработки информации. В докладе рассмотрена концепция создания СОКИ, обладающая повышенными характеристиками по быстродействию обработки модульных операций. Основное преимущество предложенного подхода состоит в возможности достижения высокой производительности обработки криптографической информации, а также в создании уникальной системы контроля и коррекции ошибок данных. Поэтому представляется актуальным рассмотрение и создание системы криптографической обработки информации на основе использования модулярной системы счисления (МСС).