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 М.С. Мурзін

ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ СИСТЕМ ЗВЯЗКУ, РТЗ, АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПОВІТРЯНИХ СИЛ

О.І. Кушнір
Командування Повітряних Сил Збройних Сил України

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

- застосування цифрових систем передачі інформації, що визначає перехід від аналогових до цифрових методів обробки, комутації та 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 обороти ACCS НАТО;
- застосування інформаційних технологій, які базуються на нових досягненнях у галузі інформатики та обчислювальної техніки;
- 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, зв'язку та засобами захисту можна очікувати значного зростання оперативності і стійкості управління, рівня бойової готовності.

АНАЛІЗ ПІДХОДІВ ЩОДО ОРГАНІЗАЦІЇ ВІДНОВЛЕННЯ ТЕХНІКИ ЗВ'ЯЗКУ ТА РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ПОВІТРЯНИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

О.П. Кулик, к.військ.н., с.н.с.; Ю.М. Добришкін, к.т.н.; С.М. Рот
Харківський університет Повітряних Сил імені Івана Кожедуба

В сучасних умовах кардинально змінюються традиційні зміст і характер військових конфліктів та локальних війн. Вже в перші часи бойових дій зусилля ата-

куючої сторони головним чином з застосуванням високоточної зброї направляються на ураження системи протиповітряної оборони, органів державного управління, системи управління збройними силами, а саме системи зв'язку та бойового управління. В залежності від мети, з якою починаються бойові дії також слід очікувати нанесення ударів й по аеродромах базування авіації. Необхідність розгортання військової техніки (ВТ) зв'язку і радіотехнічного забезпечення (РТЗ) безпосередньо на пунктах управління (ПУ) різних рівнів або у складі вузлів зв'язку, що розгортаються на незначних відстанях від цих ПУ з великою ймовірністю дозволяють вважати, що ВТ зв'язку та РТЗ в ході бойових дій може стати або об'єктом безпосереднього ураження або буде уражатись при нанесенні ударів по інших об'єктах. В результаті цього ВТ зв'язку та РТЗ буде отримувати певні бойові пошкодження та буде вимагати відновлення її справності або працездатності. В роботі проаналізовані підходи щодо організації заходів по відновленню ВТ зв'язку та РТЗ в умовах бойової діяльності військ. Здійснена класифікація ступенів пошкодження ВТ зв'язку та РТЗ, а також перелічені сили і засоби, що залучаються до її відновлення.

МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ В РАДИОТЕХНИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ, ОСНОВАННЫЕ НА ПРИМЕНЕНИИ СЛОЖНЫХ ХАОТИЧЕСКИХ СИГНАЛОВ

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

Одним из способов повышения скрытности радиотехнических систем передачи информации является применение хаотических сигналов. Среди множества существующих подходов к созданию способов скрытой передачи информации с использованием динамического хаоса можно выделить два класса систем передачи информации: системы передачи информации с хаотической синхронизацией и прямохаотические системы связи. Основными типами хаотической синхронизации, лежащими в основе современных систем связи, являются режимы полной, фазовой и обобщѐнной синхронизации. Принципиальным недостатком систем передачи информации с хаотической синхронизацией являются низкая помехоустойчивость. В прямохаотической системе радиосвязи, в отличие от систем с хаотической синхронизацией, используется корреляционная обработка принятого сигнала, что в свою очередь повышает помехоустойчивость системы. Поэтому, для повышения помехоустойчивости систем передачи и приема информации целесообразно применять сигналы с прямохаотической несущей.

ПРИМЕНЕНИЕ РЕКУРРЕНТНОГО АНАЛИЗА ДЛЯ ОБНАРУЖЕНИЯ И ОБРАБОТКИ БИНАРНОЙ ИНФОРМАЦИИ В СЛОЖНОЙ ПОМЕХОВОЙ ОБСТАНОВКЕ

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

В последние годы активно применяются в радиотехнических системах сложные сигналы не традиционной (не гармонической) формы. К таким сигналам можно отнести как хаотические, так и фрактальные сигналы, которые имеют ряд преимуществ над простыми гармоническими сигналами. Наиболее важными из которых являться шумоподобность: визуальная, спектральная и корреляционная; самосинхронизация; повышенная скрытность факта передачи информации. Однако, использование большого количества сигналов сложной формы и высокие требования к каналам инфокоммуникаций формируют ряд проблем перед разработчиками новых сис-

тем передачи информации. Основной из них является сложная помеховая обстановки, а тем самым сложность правильного обнаружения и обработки информации. Для более качественного обнаружения и обработки сигналов в сложной сигнально-помеховой обстановке в работе предлагается применение рекуррентного и кросс-рекуррентного анализа (рекуррентных и кросс-рекуррентных диаграмм). Предложено использование характеристического вектора подобия для статистического оценивания опорного колебания и принятого сообщения. Данный метод подобен корреляционному анализу гармонического колебания, но в отличие от него основан не на анализе сигнала, а его образа в фазовом пространстве спроецированного на плоскость. Решение о приеме бита информации принимается на основании подобности характеристического вектора принимаемого сигнала и опорного.

АНАЛІЗ ВПЛИВУ ЕФЕКТУ РОЗТІКАННЯ СПЕКТРУ, ЩО СУПРОВОДЖУЄ ДПФ, НА ЕФЕКТИВНІСТЬ КОРЕКЦІЇ СПЕКТРАЛЬНОГО АНАЛІЗУ

В.І. Василишин, к.т.н., доц.
Харківський університет Повітряних Сил імені Івана Кожедуба

Сучасні методи спектрального аналізу, основані на аналізі власних значень та власних векторів коваріаційної матриці спостережень (так звані власноструктурні (ВС) методи), забезпечують кращі характеристики розділення та оцінювання частоти в порівнянні з традиційними методами, що базуються на використанні дискретного перетворення Фур'є (ДПФ). Потреба високого розділення за частотою виникає в радіолокації (при розпізнаванні класу цілей і т.д.), безпровідному зв'язку. Проте при низькому відношенні сигнал/шум (ВСШ) або малій кількості відліків вхідних даних точність оцінювання та роздільна здатність цих методів погіршується. Здійснити корекцію спектрального аналізу ВС (і не тільки) методами можливо за рахунок використанням технології сурогатних даних, отриманих наприклад рандомізацією фаз Фур'є спектра спостереження. Використання ДПФ зумовлює наявність ефекту розтікання (leakage) у випадку, коли частоти гармонічних коливань не кратні частотам аналізу ДПФ (на інтервалі аналізу розміщується не ціле число періодів сигналу). В результаті імітаційного моделювання корекції спектрального аналізу з використанням сурогатних даних встановлено, що по мірі збільшення ВСШ середньоквадратичні похибки оцінювання частот ВС методів Root-MUSIC та MUSIC насичуються і не залежать від ВСШ (коррекція стає не ефективною). Така поведінка зумовлена ефектами розтікання та рандомізації спектральних компонент спостереження. Зменшення впливу ефекту розтікання є напрямком подальших досліджень.

ОЦІНЮВАННЯ ЧАСТОТ ГАРМОНІЧНИХ КОЛИВАНЬ МЕТОДОМ MUSIC З ВИКОРИСТАННЯМ ДПФ

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

Метод MUSIC є одним з методів спектрального аналізу, які ґрунтуються на аналізі власних значень та власних векторів коваріаційної матриці спостережень. З метою визначення частот сукупності гармонічних коливань цим методом потрібно здійснювати математичне сканування за частотою. Крок математичного сканування має бути меншим величини рознесення за частою між частотами гармонічних коливань. Оцінки частот визначаються як максимуми отриманої спектральної функції. Для прискорення підрахунку можна занести значення векторів математичного сканування для потріб-

ного діапазону частот в запам'ятовуючий пристрій обчислювального пристрою радіотехнічної системи. Спростити реалізацію методу MUSIC можливо шляхом використання дискретного перетворення Фур'є (ДПФ). При цьому виконується ДПФ кожного з власних векторів (ВВ) підпростору шуму та додавання отриманих по кожному з ВВ результатів (виконується ДПФ матриці ВВ підпростору шуму). Зазвичай довжина вектору «комплексних синусоїд», за допомогою якого реалізується ДПФ, рівна довжині ВВ. Використання так званого доповнення нулями (zero padding) дозволяє отримати більш часту сітку частот для виконання ДПФ та, відповідно, підвищити точність оцінювання частот спектральних піків (максимумів) псевдоспектру методу MUSIC. Результати імітаційного моделювання вказують на підвищення точністних характеристик методу MUSIC у випадку використання ДПФ та доповнення нулями власних векторів коваріаційної матриці спостережень.

СПОСІБ РОЗШИРЕННЯ ЗОН АВТОСУПРОВОДЖЕННЯ І ВВОДУ В АВТОСУПРОВОДЖЕННЯ ЛІТАКА МОНОІМПУЛЬСНОЮ РЛС ПОСАДКИ

М.Д. Рисаков, к.т.н., доц.; І.В. Тітов, к.т.н., с.н.с.; В.В. Куценко; І.Л. Костенко, к.військ.н., с.н.с.
Харківський університет Повітряних Сил імені Івана Кожедуба

Істотним недоліком моноімпульсної РЛС (МРЛС) автосупроводження (АС) літака на етапі посадки з реалізацією амплітудної обробки і допплерівської фільтрації віддзеркалень є малі розміри зони АС в порівнянні із зоною виявлення локатора. Малі кутові розміри зони АС ускладнюють роботу оператора по введенню літака в цю зону. У доповіді обгрунтовується можливість розширення в два рази кутової зони АС і перетворення зони виявлення в зону введення в АС літака такою МРЛС АС шляхом симетричного розташування чотирьох основних пелюсток діаграми спрямованості в двох площинах стеження і складання радіоімпульсів відповідних пар пелюсток на прийом в кожній площині. Уточнений алгоритм роботи вимірювачів кутових координат по значеннях амплітуд накопичених в допплерівських фільтрах відповідної пари сумарних пелюсток. Показано, що для відновлення потужності відбитих імпульсів в розширеній зоні АС необхідно потужність передавача збільшувати в п'ять разів.

ПРОБЛЕМИ ВПРОВАДЖЕННЯ АЛГОРИТМІВ ДОПЛЕРІВСЬКОЇ ФІЛЬТРАЦІЇ ВІДДЗЕРКАЛЕНЬ У РЛС АВТОСУПРОВОДЖЕННЯ ЛІТАКІВ В ЗОНІ ПОСАДКИ

В.В. Куценко; М.Д. Рисаков, к.т.н., доц.; І.В. Тітов, к.т.н., с.н.с.; В.Г. Карєв
Харківський університет Повітряних Сил імені Івана Кожедуба

Для компенсації впливу, що заважає, на обробку сигналів віддзеркалень від земної поверхні та метеорологічних утворень в моноімпульсних РЛС (МРЛС) автосупроводження (АС) літаків в зоні посадки потрібно реалізовувати ефективні алгоритми допплерівської фільтрації, наприклад, шляхом когерентного накопичення в допплерівських фільтрах відбитих імпульсів під час декількох періодів. В зоні посадки пропонується реалізовувати адаптивний алгоритм фільтрації шляхом дискретної зміни періоду повторення для виключення накопичення імпульсів літака у нульовому фільтрі. Такий алгоритм дозволяє практично виключити вплив віддзеркалень, що заважає, від пасивних об'єктів. Проте в МРЛС АС з сумарно-різницевою обробкою така фільтрація призводить до неоднозначності вимірюван-

ня кутових координат. У доповіді наводяться алгоритми адаптивної допплерівської фільтрації відбитих імпульсів і двох способів (фазового та амплітудного) ліквідації неоднозначності вимірювання кутових координат.

ПРО МОЖЛИВІСТЬ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІМПУЛЬСНО-ФАЗОВОЇ РІЗНИЦЕВО-ДАЛЬНОМІРНОЇ РАДІОТЕХНІЧНОЇ СИСТЕМИ ДАЛЬНЬОЇ НАВІГАЦІЇ РСДН-10

С.А. Макаров, к.т.н., доц.; І.М. Токайський; О.А. Павліченко
Харківський університет Повітряних Сил імені Івана Кожедуба

На даний час, існуючий пристрій управління службового зв'язку обслуговуючого персоналу радіотехнічної системи дальньої навігації РСДН-10 має невисоку ефективність, яка обумовлена конструктивними особливостями та недосконалими ергономічними характеристиками. Зокрема, службова інформація надається у вигляді формалізованих команд на спеціалізоване табло. Обслуговуючому персоналу для розпізнання формалізованих команд необхідний додатковий час. Удосконалення пристрою службового зв'язку можливо за рахунок втілення апаратури з процесорною обробкою сигналів із застосуванням завадозахищених кодів та використання пристрою відображення службової інформації із застосуванням рідино-кристалічного екрану. При вбудуванні в апаратуру управління і синхронізації (АУС) інтерфейсних та мультиплексорних пристроїв можливо здійснювати дистанційну корекцію часової затримки випромінювання імпульсів станції РСДН. Застосування цих технічних засобів буде сприяти підвищенню показників скритності, достовірності, своєчасності, оперативності роботи обслуговуючого персоналу радіотехнічної системи дальньої навігації РСДН-10.

ИССЛЕДОВАНИЕ МЕТОДОВ РАДИОУПРАВЛЕНИЯ ОБЪЕКТАМИ, ДВИЖУЩИМИСЯ ПО ПРОГРАММНЫМ ТРАЕКТОРИЯМ

А.В. Мазуренко[1], к.т.н., доц.; О.В. Высоцкий[2], к.т.н., доц.;
О.Г. Лебедев[2], к.т.н., доц.
[1]Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ»;
[2]Харьковский университет Воздушных Сил имени Ивана Кожедуба

Одной из составляющих безопасности судовождения и самолетовождения является обеспечение необходимой точности проводки судов. Рост интенсивности движения, увеличение скоростей судов, их тоннажа и размеров усложняет обеспечение надлежащего уровня безопасности судовождения. Поэтому разработка новых и совершенствование существующих систем и способов управления движением судов является важной и актуальной задачей. В докладе представлены результаты исследования методов управления для проводки объектов по фиксированным траекториям. Объектами, движущимися по таким траекториям могут быть суда, движущиеся по фарватерам, беспилотные летательные аппараты, движущиеся на постоянной высоте по заданной траектории. В качестве объекта управления рассматривался надводный подвижный объект. При этом исследовались классический метод радиоуправления – прямой метод и метод нелинейного сближения. Рассмотрены уравнения динамики судна в пространстве состояний. Проведен анализ замкнутого контура системы управления. Определены управляющие функции для прямого метода управления объектом и метода нелинейного сближения. Определены характерные особенности, достоинства и недостатки исследованных методов радиоуправления.

ОБГРУНТУВАННЯ НАПРЯМКІВ МОДЕРНІЗАЦІЇ КОМАНДНОЇ РАДІОЛІНІЇ УПРАВЛІННЯ ВИНИЩУВАЛЬНОЮ АВІАЦІЄЮ

О.В. Сісков, к.т.н., с.н.с.; М.І. Володін, к.т.н., с.н.с.; В.О. Шевченко
Харківський університет Повітряних Сил імені Івана Кожедуба

Обґрунтована доцільність та актуальність вдосконалення командної радіолінії управління (КРУ) винищувальною авіацію. Визначені причини модернізації КРУ: моральне старіння обладнання КРУ; фізичне старіння обладнання КРУ; знаходження виробничої бази обладнання КРУ за межами України; низька живучість і завадозахищеність КРУ із-за повної інформованості країн, що використовують такі самі системи або мали їх на озброєнні, про порядок і способи їх використання.

Обґрунтовані основні напрямки модернізації КРУ: переведення апаратної частини шифраторів і дешифраторів команд КРУ на сучасну елементну базу; застосування технічних засобів захисту інформації в КРУ; зміна структури кодограм наборів команд і відповідного програмного забезпечення; заміна радіостанцій і приймачів на сучасні зразки з високою завадозахищеністю і дальністю дії.

Визначено ряд організаційних та технічних питань, які необхідно вирішити для застосування модернізованої КРУ для виконання завдань автоматизованого наведення в АСУ авіацією та ППО, зокрема: підготовка та внесення змін до ТТЗ на виконання ДКР «Ореанда-ПС» щодо застосування модернізованої КРУ; розробка протоколів інформаційно-технічного спряження та схем технічного спряження комплексів засобів автоматизації (КЗА) з модернізованою КРУ; виготовлення та встановлення програмно-апаратних засобів спряження КЗА з КРУ; випробування модернізованих зразків КРУ.

ПРИМЕНЕНИЕ ФРАКТАЛЬНОЙ МОДУЛЯЦИИ ДЛЯ ПЕРЕДАЧИ ДАННЫХ В СИСТЕМЕ РАДИОСВЯЗИ

К.С. Васюта, д.т.н., доц.; С.В. Озеров; А.Н. Королюк
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Известно, что фрактальные сигналы в системах передачи данных применяются достаточно давно, однако еще не достаточно изучено применение систем связи, основанных на свойствах фрактальных сигналов в сложной электромагнитной обстановке. Поэтому, актуальной является задача передачи непрерывной или дискретной последовательности данных на фрактальной несущей по зашумленному и ненадежному, непрерывному по амплитуде и времени каналу радиосвязи, когда полоса пропускания или параметры длительности канала известны априорно или совсем не известны. Например, каналы с замираниями или преднамеренными помехами. Понятие “фрактальная модуляция” основано на свойствах и характеристиках гомогенных (однородных) сигналов. Авторы Wornell и Oppenheim первыми отметили, что процессы с самоподобными свойствами наблюдаются в случайных физических явлениях. Более того самоподобные процессы сохраняют свои характеристики, изменяясь во времени. Соответственно автокорреляционная функция таких процессов, обладает свойством масштабной инвариантности в пределах амплитудного множителя. Кроме того, свойством самоподобия (масштабной инвариантности характеристик) обладают и детерминированные процессы, которые являются инвариантными в пределах амплитудного множителя при произвольном масштабировании во времени.

ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ И СКРЫТНОСТИ СИСТЕМЫ РАДИОСВЯЗИ ПУТЕМ ПРИМЕНЕНИЯ MIMO-ТЕХНОЛОГИИ НА ХАОТИЧЕСКИХ НЕСУЩИХ

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

Непрерывное повышение требований, предъявляемых к системам военной радиосвязи, вынуждает искать пути улучшения их характеристик, в частности скрытности и пропускной способности. Для повышения скрытности в настоящее время широко используются хаотические сигналы, которые обладают высокой чувствительностью к начальным условиям и, как следствие, позволяют реализовать многоканальность в заданном диапазоне частот. Кроме того, хаотические сигналы обладают специфическими свойствами, присущими случайным процессам. Главным способом достижения высокой скорости передачи данных (пропускной способности) в MIMO-радиосистемах (Multiple Input Multiple Output – множественный вход множественный выход), является передача данных от источника к получателю через несколько радио соединений, откуда данная технология и получила свое название. Для организации MIMO-технологии необходима установка нескольких антенн на передающей и на приемной стороне. Предлагается MIMO-система радиосвязи, где в качестве несущего сигнала используется хаотический процесс (полином Чебышева) с разными начальными условиями для каждого подканала h, состоящая из M передающих и N приемных антенн.

МОДЕЛЬ ПЛАНИРОВАНИЯ ЧАСТОТНО-ВРЕМЕННОГО РЕСУРСА НИСХОДЯЩЕГО КАНАЛА СВЯЗИ ТЕХНОЛОГИИ WIMAX

С.В. Гаркуша, к.т.н., доц.
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 сетей масштаба города, функционирующих на основе технологии WiMAX. Производительность нисходящего канала связи технологии WiMAX во многом определяется способом распределения частотного и временного ресурсов между пользовательскими станциями (ПС) сети. Предложена математическая модель распределения частотного и временного ресурсов в нисходящем канале связи технологии WiMAX. Предложенная модель направлена на формирование одного пакета данных нисходящего канала для каждой ПС, что позволяет минимизировать количество служебных сообщений передаваемых по используемому частотному каналу связи. В качестве примера получены решения сформулированной в работе оптимизационной задачи, для чего была использована система MatLab R2011a, в рамках которой задействована программа minlpAssign пакета оптимизации TOMLAB. В результате анализа полученных решений установлено, что задача совместного распределения частотного и временного ресурсов позволяет от 1,5 до 2-х раз повысить эффективность использования пропускной способности нисходящего канала технологии WiMAX, по сравнению с задачей распределения частотного и задачей распределения временного ресурса. Кроме того формирование одного пакета данных для каждой ПС, позволяет уменьшить количество служебной информации от 5 до 30%, в зависимости от количества ПС и количества пакетов данных, которые формируются для одной ПС.

ПРОГРАМНА СИСТЕМА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ МОБІЛЬНИХ ЗАСОБІВ ЗВ'ЯЗКУ

С.Б. Сариєв; С.Г. Семенов, к.т.н., доц., Т.М. Шипова
Національний технічний університет «ХПІ»

Реалізація принципів контролю доступу до ресурсів мобільних засобів зв'язку є основою захисту інформації від несанкціонованого доступу. Основу реалізації розмежувальної політики доступу до ресурсів складає призначення і реалізація засобами захисту прав доступу користувачів до ресурсів, у тому числі, до інформаційних. Забезпечення коректності реалізації розмежувальної політики доступу до ресурсів неможливе без коректної автентифікації користувачів. У ряді додатків механізми ідентифікації і автентифікації вбудованими в ОС мобільних засобів реалізуються не коректно. Як наслідок, потрібні додаткові засоби. Застосування ж додаткових засобів призводить до некоректності реалізації інших механізмів, зокрема механізму ідентифікації і аутентифікації користувача при вході в систему в захищеному режимі. В доповіді представляється програмна система автентифікації користувачів мобільних засобів зв'язку, яка забезпечує коректну автентифікацію суб'єкта доступу до ресурсів і дозволяє підвищити рівень захисту внутрішніх інформаційних ресурсів від несанкціонованого доступу.

АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПОШИРЕННЯ РАДІОХВИЛЬ У БЕЗДРОТОВИХ СИСТЕМАХ ДОСТУПУ

С.М. Семенов
Харківський університет Повітряних Сил імені Івана Кожедуба

Однією з найважливіших характеристик поширення радіосигналу є його загасання в каналі зв'язку. Більшість моделей, що використовують для розрахунку радіотрас у системах бездротового радіозв'язку, засновані на найпростішій формулі, яка визначає потужність прийнятого сигналу вільному просторі. Подальший огляд двопроменевої моделі поширення радіосигналу, моделі Окамури, COST231-Hata для конкретних умов визначають особливості визначення втрат сигналу при передачі на відкритих ділянках. Якщо розглядати модель розповсюдження радіохвиль всередині будинку, то ослаблення сигналу на радіолініях у вільному просторі залежить від відстані між радіопристроями і носить логарифмічний характер. Після проведення аналізу залежності втрат від відстані при різних значеннях коефіцієнта поглинання з'ясувалося, що найкращим рішенням для поліпшення дальності зв'язку з розглянутих є коефіцієнт підсилення антен 55 дБ, який дозволяє збільшити дальність зв'язку до 4 км.

МОДЕЛЬ ШВИДКОДІЮЧОЇ СИСТЕМИ ФАЗОВОГО АВТОПІДСТРОЮВАННЯ ЧАСТОТИ

С.А. Макаров[1], к.т.н., доц.; О.М. Чекунова[1], к.т.н.; С.А. Юхновський[2]
[1]Харьківський університет Повітряних Сил імені Івана Кожедуба;
[2]Командування Повітряних Сил Збройних Сил України

Сучасні засоби радіозв'язку тактичної ланки управління потребують введення режиму швидкої псевдовипадкової перебудови робочої частоти, тобто зі швидкістю перебудови вище 1000 стрибків у секунду. Забезпечення зазначеної швидкості перебудови робочої частоти потребує з одного боку підвищення швидкодії синтезатору частот та з іншого – підвищення швидкодії демодулятору фазоманіпульованих (ФМн) послідовностей та дискретно-частотних сигналів. Одним з основних елементів сучасних синтезаторів частот, пристроїв синхронізації та демо-

дуляторів дискретно частотних й ФМн сигналів є система фазового автопідстроювання частоти (ФАПЧ). Зменшення часу перебудови з однієї частоти на іншу синтезатора частот висуває вимогу підвищення швидкодії системи ФАПЧ за умови високої чистоти спектра вихідного сигналу. Це протиріччя доцільно вирішувати із застосуванням систем ФАПЧ зі змінною структурою та параметрами. На основі результатів дослідження різних видів нелінійних законів динамічного регулювання параметру зворотного зв'язку за фазою запропоновано модель швидкодіючої системи ФАПЧ з додатковими фазовими регуляторами. Підвищення швидкодії досягається за рахунок динамічного регулювання параметру (коефіцієнту підсилення) по нелінійному закону зворотних зв'язків з фазовими регуляторами, які у порівнянні з основним колом зворотного зв'язку є мало інерційними.

ПРИСТРІЙ РЕТРАНСЛЯЦІЇ В АВІАЦІЙНИХ СИСТЕМАХ РАДІОЗВ'ЯЗКУ УКХ ДІАПАЗОНУ

О.В. Чечуй, к.т.н., доц.; А.П. Глушко, к.т.н., доц.; Ю.В. Новиков
Харківський університет Повітряних Сил імені Івана Кожедуба

Для підвищення дальності та надійності зв'язку в авіаційних системах радіозв'язку УКХ діапазону пропонується внесення до складу бортової радіостанції УКХ діапазону ретрансляційного (репітерного) пристрою. Такий пристрій в режимі ретрансляції забезпечує приймання, записування мовної інформації та передачі її до передавального пристрою радіостанції. Проведено аналіз існуючих радіостанцій УКХ діапазону, та методів збільшення дальності зв'язку. Оцінка підвищення дальності та надійності зв'язку запропонованого пристрою ретрансляції досліджені імітаційним моделюванням. Пропонується функціональна схема цифрового пристрою ретрансляції з обгрунтуванням його основних елементів. Вказаний пристрій може забезпечувати запис інформації, автоматичне керування всіма режимами радіостанції та побудований на сучасній елементній базі. Розроблений пристрій може бути рекомендований для застосування на всіх типах бортових радіостанцій УКХ діапазону.

ОПТИМАЛЬНІ МЕТОДИ ОБРОБКИ ШУМОПОДІБНИХ СИГНАЛІВ В КУТОМІРНОЇ РАДІОНАВІГАЦІЙНІЙ СИСТЕМІ «ПАР-АРК»

В.А. Дорощук, к.т.н., доц.; В.О. Корнеев, к.т.н.;
Харківський університет Повітряних Сил імені Івана Кожедуба

Одним із засобів, яки забезпечують льотчика інформацією про кутове положення літака відносно наземного радіомаяка (РМ) є кутомірна радіонавігаційна система (КРНС) "привідна аеродромна радіостанція – автоматичний радіокомпас (ПАР-АРК). Така система призначена для автоматичного вимірювання на борту літального апарату (ЛА) курсового кута радіостанції (ККР) з метою рішення ряду навігаційних задач. Однак КРНС "ПАР-АРК" має суттєвий недолік – низьку завадостійкість та недостатню прихованість роботи. Одним з варіантів покращення завадостійкості та прихованість роботи КРНС "ПАР-АРК" є застосування ШПС з використанням кореляційних методів обробки сигналів. Вважається 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. Пропонується структурна схеми приймача АРК кореляційного типу, у якому реалізовані оптимальні методи обробки ШПС сигналу. Використання ШПС сигналів в каналі КРНС "ПАР – АРК", та оптимальних

методів обробки на борту літака дозволяє здійснювати передачу на борт літака сигналів управління в складі високоточного РЛПК для оперативного усунення екіпажем помилок пілотування, підвищити скритність та завадостійкість каналу.

ФОРМИРОВАНИЕ СИНДРОМНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ АЛГЕБРАИЧЕСКИХ СВЕРТОЧНЫХ КОДОВ ПЕРЕМЕЖЕНИЯ

А.В. Боцул[1]; С.И. Приходько[2]; А.С. Волков[2]
[1]Национальный технический университет «ХПИ»;
[2]Украинская государственная академия железнодорожного транспорта

Алгебраическая процедура декодирования сверточных кодов перемежения предусматривает вычисление по известным корням порождающего многочлена синдромную последовательность полубесконечной длины. При этом алгебраическая процедура декодирования сверточных кодов перемежения имеет фиксированное число операций для декодирования блока кодовых слов. Показано, что введение оператора задержки в кодовое слово сверточного кода перемежения позволяет устранить эффект распространения ошибок при вычислении компонент синдрома. Метод декодирования алгебраических сверточных кодов перемежения предполагает вычисление полубесконечной серии не перекрывающихся синдромных последовательностей, что позволяет исправлять группирующиеся ошибки на длине блока кодового слова.

АНАЛІЗ МОЖЛИВОСТІ ПОБУДОВІ КАНАЛУ ПЕРЕДАЧІ НА БОРТ СИГНАЛІВ УПРАВЛІННЯ ЛІТАКОМ ШЛЯХОМ УДОСКОНАЛЕННЯ АВАРІЙНОГО ПРИЙМАЧА РАДІОСТАНЦІЇ ЗВ'ЯЗКУ

Д.М. Воронов, к.т.н.; І.Л. Костенко, к.військ.н., с.н.с.;
М.Д. Рисаков, к.т.н., доц.; І.М. Токайський
Харківський університет Повітряних Сил імені Івана Кожедуба

Важливе місце у складі радіолокаційного комплексу посадки займає канал передачі на борт літака сигналів управління. Проаналізована можливість побудови такого каналу шляхом удосконалення наземного та бортового обладнання радіозв'язку. При побудові таких каналів бажано передбачити можливість одночасного їх використання за призначенням – для переговорів керівника зони посадки з екіпажем. Однак у склад радіостанцій входять аварійні приймачі, які можуть використовувати на борту другим каналом прийому − приймачем сигналів управління. Тому у якості бортового обладнання пропонується використовувати аварійний приймач радіостанції Р-863, а в якості наземного − станцію радіозв'язку Р-809М2, яка настроєна на частоту бортового аварійного приймача.

СПОСІБ РЕАЛІЗАЦІЇ ДЕКОДЕРА ЦИКЛІЧНИХ КОДІВ З ВИПРАВЛЕННЯМ БАГАТОКРАТНИХ ПОМИЛОК

М.Д. Рисаков, к.т.н., доц.; С.А. Макаров, к.т.н., доц.;
О.П. Кулик, к.військ.н., с.н.с.; В.Г. Карєв
Харківський університет Повітряних Сил імені Івана Кожедуба

Основна проблема реалізації коду, що коректує, з виправленням багатократних помилок є необхідність запам'ятовування декодером безлічі значень синдрому помилок у всіляких розрядах і здійснення порівняння цієї множини із значенням синдрому прийнятої комбінації. Так для коду (15,4) з 4-мя інформаційними і 11-тьма перевірочними розрядами, здатного виправляти до трьох помилок, необхідно в звичайному випадку в пам'яті декодера зберігати 575 11-ти розрядних значень синдромів помилок

і при декодуванні для визначення спотворених розрядів необхідно їх порівнювати з синдромом прийнятої комбінації. Такий принцип декодування свідчить про складність схемної реалізації декодера. У доповіді пропонується два варіанти циклічних кодів (ЦК), здатних виправляти два, три і чотирикратні помилки. При цьому в кожній парі ЦК виділяється код з відмінною ознакою синдромів помилок − синдромів одноразових помилок в перевірочних розрядах, що мають по одній одиниці. Обґрунтовується можливість для таких кодів скоротити до двох порядків число значень синдромів, що зберігаються в пам'яті декодера, і на один порядок скоротити число операцій алгебри для визначення і виправлення спотворених розрядів прийнятої комбінації.

ТЕХНІЧНІ ВИМОГИ ДО ЗАВАДОЗАХИЩЕНОСТІ ПЕРСПЕКТИВНИХ ЗАСОБІВ РАДІОЗВ'ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

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

Сучасні засоби радіозв'язку, що призначені для забезпечення радіозв'язком підрозділів при веденні ними бойових дій та під час антитерористичних і миротворчих операцій (заходів), повинні забезпечувати можливість скритної та завадозахищеної передачі інформації (мови й даних) по радіоканалам в умовах впливу комплексу негаусовських та нестаціонарних перешкод, а також багатопроменевого поширення радіохвиль. При роботі у повнозв'язній мережі застосування спрямованої передачі практично неможливе, а необхідність передачі мови не дозволяє суттєво зменшити час випромінювання радіосигналів. Тому використання сигналів з розширеним спектром, а саме широкосмугових шумоподібних сигналів та сигналів з псевдовипадковою перебудовою робочої частоти, є ефективним способом підвищення скритності. Для підвищення завадостійкості приймання цифрової інформації доцільно максимально розширювати частотний діапазон роботи систем радіозв'язку, що забезпечує можливість адаптації до завадової обстановки. Вибір частки робочого діапазону найменш ураженого завадами може бути виконаний шляхом послідовного панорамного аналізу з подальшим вибором за заданим критерієм оптимальної робочої частоти, яка може назначатися адміністратором мережі системи радіозв'язку. У доповіді наведені технічні вимоги до завадозахищеності засобів радіозв'язку військового призначення.

МЕТОДИ РОЗРАХУНКУ ЗОН ДІЇ ЗАСОБІВ РАДІОЗВ'ЯЗКУ В КХ/УКХ ДІАПАЗОНАХ

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

Дослідження проводяться на підставі наказу Командувача Повітряних Сил Збройних Сил України від 12.03.12 № 76 «Про розроблення спеціального програмного математичного забезпечення Повітряних Сил Збройних Сил України». В основу методик, що розробляються, покладено рівняння радіопередачі. Показано, що оскільки при радіозв'язку у діапазоні УКХ потужності передавачів мали та складають десятки Вт, а антени є ненаправлені та мають малий коефіцієнт підсилення, то механізми дифракції радіохвиль і тропосферного розсіяння не дозволяють отримати необхідний рівень поля у точці приймання. Тому основним механізмом розповсюдження радіохвиль при радіозв'язку з повітряними об'єктами в УКХ діапазоні є просторова хвиля в умовах прямого бачення, а множник послаблення розраховується за допомогою інтерференційних формул з урахуванням рельєфу місцевості. Доведено, що аномальні механізми поширення хвиль в УКХ діапазоні враховувати недоцільно, оскільки вони не забезпе-

чують надійного зв'язку. Найбільш складною задачею є розрахунок умов надійного радіозв'язку з повітряними об'єктами іоносферною хвилею у діапазоні КХ. Показано, що при розрахунках необхідно враховувати таки фактори: зміна стану іоносфери на протязі доби вимагає зміну робочих частот; зміна рівня сонячної активності та її вплив на стан іоносфери; довжина траси та її вплив на вибір оптимальної робочої частоти; зміна параметрів антен при зміни робочих частот; наявність загасань сигналу. Розглянуто вплив зовнішніх завад та методика оцінки їх рівня.

ПРОБЛЕМА СУМІСНОГО ВИКОРИСТАННЯ СМУГИ ЧАСТОТ 694-790 МГЦ ЗАСОБАМИ ЗАГАЛЬНИХ ТА СПЕЦІАЛЬНИХ КОРИСТУВАЧІВ УКРАЇНИ

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

Діапазон частот дециметрових хвиль є основним частотним ресурсом для розвитку та втілення цифрового телебачення. Це обумовлено великим завантаженням метрового діапазону аналоговим телебаченням, а також привабливими умовами поширення радіохвиль, які дозволяють економно та ефективно будувати мережі телебачення на великих територіях та використовувати для приймання антени невеликих розмірів. На Всесвітній конференції радіозв'язку 2012 року (ВКР-12) прийнято рішення (Резолюція 232 ВКР-12) про відкладання розподілу смуги частот 694-790 МГц рухомій службі за умови, що цей розподіл ідентифікований для ІМТ та буде введений у дію після ВКР-15. Крім того, необхідно провести дослідження МСЕ-R до ВКР-15, які спрямовані на уточнення нижньої межі розподілу, а також технічні та регуляторні умови використання рухомої служби, тобто систем цифрового стільникового радіозв'язку, у зазначеній смузі. На даний час, в Україні користувачами цього діапазону є радіоелектронні засоби радіозв'язку, аналогового та цифрового телебачення, та засоби спеціальних користувачів Повітряних Сил Збройних Сил України, які працюють на первинній основі. Основні дослідження МСЕ-R спрямовуються на питання сумісності рухомої служби у смузі 694-790 МГц з іншими службами радіозв'язку у цій та сусідніх смугах та визначення балансу між потребами радіомовної служби та потребами широкосмугових мереж рухомого зв'язку, а також спеціальних користувачів.

ПРОПОЗИЦІЇ ПО ПІДВИЩЕННЮ ДОСТОВІРНОСТІ ПЕРЕДАЧІ ДАНИХ В СДУ БАЗОВОЇ СТАНЦІЇ РАДІОЗВ'ЯЗКУ УКХ ДІАПАЗОНУ

С.А. Макаров, к.т.н., доц.; М.Д. Рисаков, к.т.н., доц.;
О.П. Кулик, к.військ.н., с.н.с.; І.Л. Костенко, к.військ.н., с.н.с.
Харківській університет Повітряних Сил імені Івана Кожедуба

Для передачі повідомлень і команд дистанційного управління по дротовим або радіолініям зв'язку в радіостанції Р-845М застосовується частотно-часовий код. Такі коди і лінії зв'язку не забезпечують високу достовірність передачі даних. Для підвищення достовірності потрібно використовувати завадостійкі лінії зв'язку і коди. У якості таких кодів пропонується використовувати циклічні 15-ти розрядні коди, що дозволяють виправляти до трьох помилок в прийнятій комбінації. Для послаблення впливу наведених завад в дротових лініях зв'язку можна використовувати лінію у вигляді витої пари або трьохдротову лінію, в якій третій дріт служить джерелом наведеної завади. Такі лінії доцільно використовувати на позиціях тимчасового базування. На позиціях стаціонарного базування радіостанцій пропонується використовувати волоконно-оптичну 4-х волоконну лінію зв'язку, що працює в другому вікні прозорості.

СПОСІБ ВІДНОВЛЕННЯ МАТРИЦІ ПОРОДЖЕННЯ ДЛЯ ЦИКЛІЧНИХ КОДІВ

І.В. Тітов[1], к.т.н., с.н.с.; М.Д. Рисаков[1], к.т.н., доц.;
В.В. Куценко[1]; В.Ю. Добришкін[2]
[1]Харківській університет Повітряних Сил імені Івана Кожедуба;
[2]Харківський національний університет радіоелектроніки

Широке застосування в апаратурі передачі даних для забезпечення їх достовірності знаходять циклічні коди (ЦК), що є систематичними кодами (СК) з відмінною ознакою їх побудови. Основна перевага ЦК полягає в тому, що вони дозволяють отримати кодові комбінації з максимально можливою кодовою відстанню. Тобто ЦК з певною надмірністю серед СК володіють найкращою здатністю виявляти і виправляти помилки в прийнятій комбінації. Відмінною ознакою ЦК по відношенню до СК є спосіб їх формування. А саме, ЦК задаються не матрицею породження, а утворюючим поліномом для отримання утворюючої матриці. Дана матриця безпосередньо не дозволяє перейти до перевірочної матриці, що визначає правила кодування і декодування даних. У теорії завадостійкого кодування даних описуються правила розрахунку таких матриць на основі утворюючого або перевірочного поліномів. Пропонується і ілюструється спосіб переходу від утворюючої до перевірочної матриці без виконання яких-небудь розрахунків.

ЗАЛЕЖНІСТЬ ЧАСОВИХ ПАРАМЕТРІВ AD-HOC МЕРЕЖ ВІД ШВИДКОСТІ ПЕРЕСУВАННЯ ВУЗЛІВ

Ю.О. Кулаков[1], д.т.н., проф.; В.В. Воротніков[2], к.т.н., доц.; О.С. Бойченко[2]
[1]Національний технічний університет України «КПІ»;
[2]Житомирський військовий інститут імені С.П. Корольова
Національного авіаційного університету

Швидкий розвиток безпровідних мереж висуває нові вимоги до оцінки часових параметрів та вивчення залежностей параметрів Ad-hoc мереж від її структури. Існує проблема оцінки залежності часових параметрів від швидкості зміни структури Ad-hoc мереж з метою оптимального розподілення каналів та потоків інформації в бездротових інформаційно-комунікаційних мережах з урахуванням довжини обраного маршруту та часу, затраченого на передачу відповідного пакету за цим маршрутом. Для оцінки довжини маршруту використовуються різні критерії: число транзитних вузлів маршруту, довжина маршруту, якість трафіку та час передачі пакету з одного вузла мережі до іншого, а також швидкість зміни положення вузлів. Аналіз останніх публікацій свідчить про те, що в теперішній час в бездротових ІКМ використовуються різні методи маршрутизації, які забезпечують динамічне управління потоками інформації та урахування зміни положення вузлів. Головним недоліком є неефективне використання пропускних здатностей каналів зв'язку бездротової ІКМ. В доповіді для оцінки залежності часових параметрів Ad-hoc мереж від швидкості переміщення вузлів запропоновано визначати найкоротший маршрут та його довжину за допомогою метода Дейкстри з урахуванням швидкості зміни місцеположення вузлів. Аналіз результатів свідчить про те, що при швидкій зміні топології бездротових ІКМ, розрахунок основних характеристик зводиться до визначення структури мережі у певний момент часу та безпосереднього розрахунку вищенаведених характеристик. Проведена оцінка залежності часових параметрів Ad-hoc мереж від швидкості переміщення вузлів дозволяє знайти оптимальні параметри для роботи мережі при різних вхідних потоках, які обумовлюють завантаженість як окремих ліній мережі, так і мережі в цілому.

ПОЛИНОМИАЛЬНЫЕ МЕТОДЫ РАЗЛИЧЕНИЯ СИГНАЛОВ НА ФОНЕ НЕГАУССОВСКИХ ПОМЕХ

В.В. Палагин, к.т.н., доц.
Черкасский государственный технологический университет

В теории проверки статистических гипотез разработаны широко известные методы синтеза решающих правил (РП), основанные на использовании классических вероятностных критериев качества, в основе которых лежит использование плотностей распределения случайных величин. Несмотря на то, что при таком подходе теоретически не ограничивается класс исследуемых случайных величин и процессов, на практике в основном широкое использование получили гауссовские модели сигналов и помех, которые не всегда адекватно отображают реальные природные процессы. Одним из важных и актуальных примеров решения подобных задач является синтез эффективных систем различения сигналов (радиосигналов, шумовых сигналов и.т.д.) на фоне негауссовских помех, что характерно для радиолокационных и навигационных систем, систем пассивной локации, систем технической диагностики и т.д., где использование классических подходов вызывает ряд трудностей как алгоритмического, так и практического характера. В работе предложен другой подход, основанный на более простом описании случайных процессов в виде конечной последовательности моментов и кумулянтов, а также использовании полиномиальных РП, оптимальные коэффициенты которых находятся согласно новым адаптированным моментным критериям качества. Синтезированы нелинейные алгоритмы различения сигналов с лучшими показателями качества. Показано, что нелинейная обработка выборочных значений и учет негауссовского распределения случайных величин позволяет увеличивать эффективность обработки в виде уменьшения вероятностей ошибок РП и увеличения количества извлекаемой информации о различии гипотез.

МЕТОД ПРОЕКТУВАННЯ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ІЗ ЗАСТОСУВАННЯМ НОТАЦІЇ ПАРОНДЖАНОВА

О.В. Потій[1], д.т.н., проф.; А.В. Лєншин[2], к.т.н., доц.
[1]Харківський університет Повітряних Сил імені Івана Кожедуба;
[2]Харківський національний університет радіоелектроніки

Невід'ємною складовою комплексних систем захисту інформації є комплекс засобів захисту (КЗЗ) інформації від несанкціонованого доступу. З метою уніфікації та порівнюваності продуктів (у контексті послуг безпеки) в України застосовуються критерії з НД ТЗІ 2.5-004-99. Документ, зокрема, містить неформальний опис 22 послуг безпеки, що розбиті на ієрархічні підкомпоненти, кожний з яких забезпечує різний ступень стійкості від загроз безпеки. Практичне застосування НД ТЗІ 2.5-004-99 при розробці та експертизі КЗЗ свідчить, що форма подання специфікацій послуг є ускладненою і нечіткою. Це призводить до неоднозначності у розумінні вимог розробниками КЗЗ та не лише впливає на рівень захисту, але і зумовлює додаткові фінансові витрати на усунення недоліків, викритих експертами з ТЗІ. Пропонується метод, який за рахунок подання в нотації Пароджанова алгоритмів функціонування КЗЗ, при реалізації послуг безпеки, дозволяє розробити шаблони алгоритмів функціонування КЗЗ, генерувати код програмних продуктів, задовольняти вимогам гарантій рівня Г-3 та вище, проводити випробування КЗЗ із наперед визначеним ступенем покриття. Особливо корисним метод є для розробників захищених від НСД компонентів обчислювальної системи, в яких функції захисту є додатком до основних – "бізнес" функцій продукту.

ПРИМЕНЕНИЕ ПОЛОСОВОЙ ФИЛЬТРАЦИИ В ПРЯМОХАОТИЧЕСКОЙ СИСТЕМЕ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ПОВЫШЕНИЯ ЕЕ СКРЫТНОСТИ

А.А. Малышев, к.т.н., доц.; С.В. Озеров; А.А. Мацулевич, к.т.н., доц.
Харьковский университет Воздушных Сил имени Ивана Кожедуба

С целью повышения скрытности в системах передачи данных используются хаотические сигналы (процессы), которые обладают свойствами, присущими случайным процессам. Однако применение хаотических сигналов в полной мере не удовлетворяет требованиям скрытности системы радиосвязи, так как их аттракторы (фазовые портреты) структурированы и легко отличимые от аттракторов случайных процессов. Таким образом, для повышения скрытности системы передачи данных необходимо усложнять аттракторы хаотических сигналов. Среди различных путей усложнения аттрактора хаотического процесса можно выделить частотную фильтрацию хаотической несущей. Для представления временной реализации сигнала в частотной области используется преобразование Фурье. После этого осуществляется частотная фильтрация хаотической последовательности с применением полосового фильтра. При помощи обратного преобразования Фурье отфильтрованный хаотический сигнал переносится из частотной области во временную, кодируется бинарным сообщением и передается в канал связи.

ВИЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ ЗАГРОЗИ ПРОЦЕСУ ФУНКЦІОНУВАННЯ ВІРТУАЛЬНИХ СПІЛЬНОТ

А.М. Пелещишин[1], д.т.н., проф.; Р.В. Гумінський[2]
[1]Національний університет "Львівська Політехніка";
[2]Академія сухопутних військ імені гетьмана П. Сагайдачного

Оцінка ризику визначається як комплексна оцінка двох показників: можливість втрат, які відбуваються при реалізації загрози; ймовірність виникнення такої загрози. Розглядаючи інформаційні загрози інформаційної безпеки Держави в процесі функціонування віртуальних спільнот (ВС) другий показник залежить від процесу функціонування ВС – показника інформаційної загрози процесу функціонування ВС. Таким чином, враховуючи особливості реалізації функціонування ВС як сукупність вебфорумів, що об'єднюються за метою існування, можна визначити показник інформаційної загрози процесу функціонування, основними складовими якого є: популярність, інформаційність та доступність. Для кожної із запропонованих складових введемо відповідні лінгвістичні змінні та сформулюємо правила для визначення показника інформаційної загрози процесу функціонування ВС. Таким чином, використання даного підходу основаного на теорії нечітких множин надає можливість оцінити показник інформаційної загрози процесу функціонування ВС.

ВИЗУАЛИЗАЦИЯ ПРОЦЕССОВ ОЦЕНКИ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВАМИ ЯЗЫКА "ДРАКОН"

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

Многолетний опыт применения нормативных документов в сфере технологий проектирования защищенных систем информационных технологий (ИТ-систем) и комплексных систем защиты информации (КСЗИ) сделали особенно актуальными задачи обеспечения и оценки гарантий безопасности (уровня доверия). В качестве методологической основы оценивания гарантий было предложено использовать функционально-лингвистический подход, позволяющий обеспечить выполнение тре-

бований, выдвигаемых к процессу и результатам оценивания гарантий. В качестве языка моделирования была выбраны нотации IDEF0, IDEF3. Однако дальнейшие исследования показали, что разрабатываемые диаграммы потоков работ для сложных свойств гарантий, не позволяет наглядно и доступно описать шаги действий оценщика в ходе экспертизы. Обзор доступных языков, нотация которых позволяет накапливать и формализовать знания предметной области, описывать процессы и действия, позволил выявить формальный техноязык «ДРАКОН». Благодаря использованию специальных когнитивных приемов дракон-схемы дают возможность изобразить решение любого, сколь угодно сложного описания процесса оценки свойств гарантий в предельно ясной, наглядной и доходчивой форме, которая позволяет значительно сократить интеллектуальные усилия эксперта, необходимые для зрительного восприятия, понимания, верификации и безошибочного принятия решения относительно степени соответствия характеристик объекта заданных требованиях гарантий.

ОПРАЦЮВАННЯ ЦИФРОВИХ ПІДПИСІВ ЗА ДСТУ 4145-2002 З АВТОМАТИЧНИМ ВИПРАВЛЕННЯМ ПОМИЛОК

В.С. Глухов, д.т.н., доц.; А.Р. Добуш
Національний університет "Львівська політехніка"

У доповіді визначено набір елементів, які складають нормальний базис. Оптимальний нормальний базис поля Галуа другого типу (ОНБ, t=2), можна перетворити на надлишковий поліноміальний базис і в паліндроміальний базис.. Якщо при виконанні множення операнди представляти у цих базисах (А – паліндроміальному, В – у поліноміальному), то результат можна отримати декількома способами при яких будуть задіяні різні вузли помножувача. Це дає можливість порівнювати результати і формувати ознаку помилки при їх незбіганні. Знаходження ще одного добутку дає змогу виправляти помилки за допомогою мажоритарних елементів. Час виконання обчислення зростає при цьому, відповідно, у 2 при виявленні помилки і у 3 рази – при виправленні. Апаратні витрати зростають за рахунок додаткового вузла прийняття рішення. Для множення чисел у вказаних базисах будується систолічний помножувач, який зручно реалізовувати на ПЛІС. Розглянутий метод пропонується використати при створенні пристроїв опрацювання цифрових підписів на основі еліптичних кривих за національним стандартом ДСТУ 4145-2002, де використовується ОНБ.

ОСОБЛИВОСТІ РОБОТИ ГЕНЕРАТОРА ЯДЕР ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА

В.С. Глухов, д.т.н., доц.
Національний університет "Львівська політехніка"

При опрацюванні цифрових підписів на основі еліптичних кривих використовуються поля Галуа GF(2q) і обчислення над їхніми елементами здійснюються в оптимальному нормальному базисі (ОНБ). Знаходження молодшого розряду добутку c0 елементів A та B визначається як c0=AMB-T, де M – мультиплікативна матриця розміром q x q біт (наступні розряди добутку знаходяться аналогічно після циклічного зсуву операндів на 1 біт). В ОНБ кількість ненулевих (рівних 1) елементів матриці M дорівнює 2q-1. При реалізації помножувача на ПЛІС генератор ядер з параметром q перетворює математичний вираз c0=AMB-T у VHDL-опис. VHDL-опис можна створити з використанням двійкового представлення матриці M і множення на усі її елементи (0 та 1) за допомогою двох виразів loop мови VHDL. Але при цьому збільшується час моделювання

створених помножувачів і час проектування топології кристалу, особливо при великих значеннях q (за міжнародними стандартами q може сягати значення 998). У запропонованому генераторі ядер помножувачів використовується більш продуктивний спосіб створення явних VHDL-виразів, у яких використовуються тільки одиничні елементи матриці M. Кількість явних виразів (з логічних функції I та XOR) в описі не менше за q. Вирази враховують особливості ПЛІС: кількість двійкових змінних в них не перевищує кількості входів елементів LUT конкретної ПЛІС. Проміжні результати обчислення зводяться до кінцевого результату c0 з використанням пірамідальних структур.

ВИКОРИСТАННЯ СУЧАСНИХ ПЛІС ДЛЯ ОПРАЦЮВАННЯ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА GF(PQ)

В.С. Глухов, д.т.н., доц.; А.Т. Костик
Національний університет "Львівська політехніка"

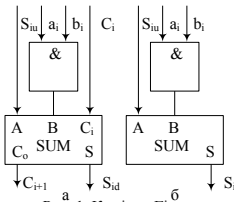

Рис. 1. Комірки Гілда

Національний стандарт опрацювання цифрових підписів визначає використання полів Галуа GF(pq), p=2. Міжнародні стандарти не виключають використання полів з p=3. Кожний розряд поля GF(2m) кодується одним бітом, поля GF(3n) – двома. Порядок n поля GF(3n) обирається з умови nlog3>m; n>0,6m (m – порядок поля GF(2m)). Однією з найскладніших операцій над елементами полів Галуа GF(pq) є множення. Паралельний помножувач будується на основі модифікованих комірок Гілда (рис. 1, б, без вхідних та вихідних переносів). Реалізуються комірки Гілда на комбінаційних елементах ПЛІС (LUT). LUT сучасних ПЛІС Spartan6 мають 6 входів та 1 вихід. Кількість комірок Гілда для побудови паралельного помножувача дорівнює kq2, для поля GF(2m) кожна комірка Гілда має 3-бітний вхід і 1-бітний вихід. Відповідно, кількість LUT N2 = km2. Для поля GF(3n) кожна комірка Гілда має 6-бітний вхід і 2-бітний вихід. Відповідно, кількість LUT N3 = 2kп2. Коефіцієнт співвідношення апаратних витрат s = N2/N3 = km2/2kп2 = m2/2*(0,6m)2= 1,4 > 1. Тобто, на сучасній елементній базі апаратні витрати на реалізацію паралельного помножувача для елементів трійкового поля Галуа менші, ніж для реалізації двійкового поля.

ОСОБЛИВОСТІ ОЦІНЮВАННЯ ПОСЛУГ БЕЗПЕКИ ДЛЯ ОДНОКОРИСТУВАЧЕВИХ ПРИСТРОЇВ

А.С. Бойко[1],к.т.н.; А.В. Лєншин[2], к.т.н., доц.
[1]ЗАТ «Інститут інформаційних технологій»;
[2]Харківський національний університет радіоелектроніки

У складі інформаційно-телекомунікаційних систем, в яких має бути створена комплексна система захисту інформації, часто використовуються пристрої, які в силу власної конструкції підтримують наявність лише одного облікового запису користувача. Прикладами таких пристроїв є планшетні персональні ЕОМ, мобільні телефони, спеціалізовані термінали, електронні ключі та смарт-карти, вимірювальні прилади з цифровими виходами тощо. Аналіз профілів захисту, опублікованих у складі експертних висновків на засоби технічного захисту інформації на сайті Держспецзв'язку, показує, що для пристроїв вказаного типу у загальному випадку відсутні послуги, пов'язані з розмежуванням доступу (адміністративна та довірча цілісність та конфіденційність). У доповіді обґрунтовується підхід до оцінювання цих можливостей з точки зору реалізації зазначених послуг безпеки згідно НД ТЗІ 2.5-004-99.

МОДЕЛЬ ИНСТИТУЦИОНАЛЬНОГО УПРАВЛЕНИЯ И МЕТОД ОЦЕНКИ УРОВНЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Теория и практика защиты информации (ЗИ) показывает, что инциденты безопасности не всегда связаны с нехваткой или неадекватностью политик, практик и процедур безопасности. Зачастую, причина инцидентов заключается в их несоблюдении (человеческий фактор). Недостаточное понимание целей и задач ЗИ приводит к тому, что рядовые сотрудники организаций воспринимают политику безопасности как ограничение и неудобство, что приводит к формированию низкого уровня культуры информационной безопасности (КИБ). Подобная проблема свидетельствует о том, что в рамках управления процессами ЗИ, следует использовать новые подходы и методы, которые позволяют эффективно решать задачи управления и контроля организационных аспектов деятельности по ЗИ. Перспективным подходом к управлению организационными аспектами ЗИ является институциональное управление, сущность которого заключается в управлении нормами и ограничениями. Ключевыми механизмами институционального управления являются: политика безопасности (как инструмент принуждения) и КИБ (как механизм побуждения). Данные механизмы формируют институт информационной безопасности (ИИБ) как двухкомпонентную структуру. В рамках модели институционального управления субъект управления стремится сформировать ИИБ, что позволит снизить риски безопасности организационного характера. Для оценки текущего уровня КИБ предлагается использовать разработанный метод оценки уровня КИБ, который содержит следующие компоненты: методику формирования множества показателей оценки КИБ, шаблон показателя нижнего уровня, подмножество показателей нижнего уровня, описанное согласно шаблону, шкалу оценки КИБ, способ построения дерева комплексной оценки, алгоритм формирования матриц свертки, описание процедуры свертки.

КОМБИНИРОВАННАЯ ТЕХНОЛОГИЯ БЕЗОПАСНОСТИ ВИДЕОИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

В.В. Баранник, д.т.н., проф.; С.А. Сидченко, к.т.н., с.н.с.; В.В. Ларин, к.т.н.
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Разрабатывается комбинированная защита видеоинформационных ресурсов, базирующаяся на скрытии смысловой информации изображений, описываемой в пространственно-временной области на основе яркостных и структурных характеристик. Предложенный подход по созданию комбинированной защиты можно классифицировать: 1) с позиции криптографии как создание симметричных криптографических систем; 2) с позиции компрессии изображений как разработка апостериорных систем сжатия на основе свертки со служебными данными. Построение информационной части кодовой конструкции должно осуществляться по интегральному принципу в два этапа: а) на первом этапе в результате свертки значений элементов исходного фрагмента и системы служебных данных на основе выбранного правила обеспечивалось формирование значения, содержащего информацию сразу о нескольких элементах исходного сообщения; б) на втором этапе для этого значения и служебных данных обеспечивалось построение кодового представления информационной части. Последовательности элементов кодовой конструкции не должны соответствовать последовательностям элементов исходного сообщения.

СПОСОБ КРИПТОКОМПРЕССИОННОГО ПРЕДСТАВЛЕНИЯ ВИДЕОИНФОРМАЦИИ В АСУ

В.В. Баранник, д.т.н., проф.; А.П. Давикоза;
С.А. Сидченко, к.т.н., с.н.с.; В.В. Ларин, к.т.н.
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Рассмотрим потенциальную возможность защиты оперативной видеоинформации в направлении построения стойких к несанкционированной дешифровки (распознавания) изображений на базе систем компактного представления, т.е. обеспечение скрытности видеоинформации на уровне кодирования ее источников. Криптокомпрессионным представлением видеоданных называется такое криптосемантическое представление, для которого семантически маскирующие преобразования строятся на базе технологий и методов сжатия изображений. Криптокомпрессионным преобразованием (кодированием, шифрованием) являются такие сжимающие преобразования (кодирование, шифрование), которые обеспечивают гарантированную стойкость относительно несанкционированного доступа к скрытым изображениям. Методами криптосемантического преобразования являются методы, одновременно обеспечивающие маскировку семантического содержания изображений и их компактное представление для повышения уровня конфиденциальности видеоинформации и оперативности ее доставки в инфокоммуникационных системах. Основными требованиями относительно построения систем стойких к несанкционированному дешифрованию изображений в инфокоммуникациях являются следующие: требуемая оперативность передачи информации и заданный уровень задержек на этапе ее обработки, высокая надежность сохранения информационного содержания, состоящая в исключении потерь информации и снижении временных задержек в процессе обработки и передачи данных, вследствие перегрузки инфокоммуникационных систем; необходимая степень достоверности в процессе ее обработки и передачи по каналам связи, устойчивость к ошибкам и потерям пакетов в процессе передачи кодограмм СНД по каналам связи, возможность автоматической обработки.

АНАЛИЗ ПЕРИОДИЧЕСКИХ СВОЙСТВ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ RC4

Р.В. Королев, к.т.н.; О.В. Петров
Харьковский университет Воздушных Сил имени Ивана Кожедуба

Алгоритм поточного шифрования RC4 разработан в 1987 г. Рональдом Линном Риверстом, американским специалистом в области криптографии для компании RSA Data Security Начиная с 1994 г., он нашел широкое применение в ряде криптографических приложений, включая такие, как SSL и TLS – для шифрования данных, передаваемых по сетям ЭВМ, не предусматривающим защиты пользовательских данных, WPA и WEP-для защиты беспроводных соединений. Таким широким распространением алгоритм обязан ряду свойств, не утратившим актуальности за двадцать лет с его существования. Одно из них – высокое быстродействие. В докладе представлены исследования зависимостей между S-боксами и индексными элементами, использование который приводит к формирование псевдослучайных последовательностей с малым периодом., что в свою очередь может привести к успешным криптоатакам. Методика исследования периодических свойств генератора псевдослучайных чисел RC4 проводилась над его мини-версией, которая получается, посредством масштабирования с сохранением всех базовых операций алгоритма. Миниверсия подвергалась тестированию и эмпирической оценки длин периодов на различных входных ключевых данных.

АНАЛИЗ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ

В.В. Ларин, к.т.н.; Р.В. Тарнополов
Харьковский университет Воздушных Сил имени Ивана Кожедуба

В настоящее время все более актуальной становится проблема защиты видеоинформации. Поскольку основным стандартом, используемым для кодирования и сжатия видеоинформации, является формат MPEG, то большинство способов защиты разработаны именно для этого формата. В них используются особенности кодирования и структуры потока MPEG для сокращения вычислительных ресурсов на защиту видеоданных. Одним из первых способов защиты данных в формате MPEG был алгоритм, предложенный Тангом − так называемый алгоритм перестановки «зигзаг». Суть его заключается в считывании квантованных коэффициентов ДКП не способом «зигзаг» для последующего кодирования, как это определено в формате, а случайным образом. Последовательность считывания коэффициентов создается генератором случайных чисел.

Ченгом и Ли был предложен метод выборочного шифрования, в котором шифруются только низкочастотные составляющие дискретного косинусного преобразования, т.е. коэффициенты, расположенные в верхнем левом углу каждой матрицы коэффициентов ДКП. Этот подход был предложен для защиты изображений формата JPEG, однако затем Канкелманн использовал эту идею для защиты данных видео в формате MPEG. Ценг и Лей предложили следующий способ. Кадр разбивается на сегменты, каждый из которых состоит из нескольких блоков или макроблоков (блок − это матрица значений яркости размером 8×8, макроблок − совокупность квадрата блоков 2×2 яркости и соответствующих матриц цветности). В каждом сегменте значения коэффициентов ДКП, занимающих одну и ту же позицию в матрице, переставляются с использованием некоторой таблицы правил перестановки. Еще один способ выборочного шифрования был предложен Ву и Куо. Суть его заключается в использовании множества таблиц Хаффмана для сжатия без потерь полученной матрицы коэффициентов дискретного косинусного преобразования.

АНАЛІЗ СУЧАСНИХ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ

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

Розвиток сучасних інформаційних технологій та використання комп'ютерних мереж ставить на перший план питання інформаційної безпеки інформації. При цьому однією з найважливіших функцій системи захисту інформації є забезпечення конфіденційності даних, що передаються. В даний час ці питання забезпечуються за рахунок використання блокових симетричних шифрів. На світовому та європейському рівнях є великий досвід організації та виконання проектів зі створення перспективних алгоритмів блокового симетричногошифрування. Проведений аналіз симетричних методів шифрування, використовуваних в сучасних криптографічних системах, дозволяє вибрати найперспективніші шифри, здатні задовольнити зростаючі вимоги до стійкості і швидкості обробки даних. Проведений аналіз показав, що більш перспективним для використання є криптоалгоритмRijndael. Тому при створенні національного стандарту блокового симетричногошифруваннянеобхідно використати великий досвід технологічно розвинених держав, а також досвід накопичений при виконанні проектів AES та Nessie.