СЕКЦІЯ 4

РОЗВИТОК ТА ЗАСТОСУВАННЯ ЗАСОБІВ РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ, ЗВ'ЯЗКУ ТА АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ПОВІТРЯНИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Керівники секції: д.т.н. професор полковник Васюта К.С.
Секретар секції: капітан Багацька Н.В.

ПІДВИЩЕННЯ ТОЧНОСТІ ВИЗНАЧЕННЯ ДАЛЬНОСТІ В РСБН ЗА РАХУНОК ВИКОРИСТАННЯ СКЛАДНИХ СИГНАЛІВ

А.І. Дацун
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Об'єктом дослідження є розробка пропозицій щодо підвищення завадостійкості та скритності далекомірного каналу (ДК)радіотехнічної системи ближньої навігації (РСБН).В ході виконання дослідження були розглянуті принципи дії ДК РСБН, характеристика завадостійкості та скритності в ДК РСБН, методи підвищення завадостійкості та скритності в ДК РСБН, а також розрахунок спектральної щільності імпульсу та широкосмугових сигналів, розрахунок впливу широкосмугової радіозавади на ДК РСБН при імпульсному та ЛЧМ сигналів. Актуальність роботи полягає у підвищенні завадостійкості ДК РСБН для забезпечення безперервної роботи радіотехнічної системи, в умовах радіоелектронної боротьби.

Аналіз характеристик завадостійкості та скритності визначив, що для підвищення даних параметрів можливо використовувати метод збільшення об'єму сигналу, шляхом підвищення смуги частот, а також підвищення завадостійкості досягається застосуванням завадостійких кодів та спеціальних методів приймання слабких сигналів. Підвищення завадостійкості та скритності далекомірного каналу можливо здійснювати шляхом використання лінійно частотно-модульованого сигналу. При визначеній девіації частоти (Δf=20 МГц) потенційна похибка визначення дальності зменшується з 227 м до 75 м.

При дослідження постановника завад із заданими параметрами при відношенні сигнал/завада плюс 3 дБ на Вт дальність дії РСБН знижується від до 650 км до 10 км. При використані широкосмугових сигналів та при тих же значеннях сигнал завада дальність дії практично не змінюється.

АСПЕКТИ УДОСКОНАЛЕННЯ АВТОМАТИЧНИХ СИСТЕМ КОНТРОЛЮ ТА ДІАГНОСТУВАННЯ ДИСПЕТЧЕРСЬКИХ РАДІОЛОКАТОРІВ РАДІОЛОКАЦІЙНИХ СИСТЕМ ПОСАДКИ ЛІТАКІВ

А.А. Залюбівський
Харківський національний університет Повітряних Сил ім. І. Кожедуба

На основі проведеного аналізу порівняння сучасних типів АСКД їх характеристик, розробленого алгоритму контролю функціонування АСКД та на підставі аналізу угруповання засобів радіотехнічного забезпечення польотів

державної авіації, задач і характеристик радіолокаційних систем посадки літаків (РСП) та вимог до них, а також рівня безпеки польотів державної авіації обґрунтовано необхідність удосконалення систем АСКД РСП, яке відбувається за такими основними напрямками:

автоматизація процесів контролю та діагностування роботи обладнання для зменшення витрати часу на пошук відмов на основі впровадження комп'ютерно-інтегрованих технологій;

удосконалення АСКД за критерієм максимуму інформації про стан об'єкту контролю;

удосконалення АСКД за рівнем дальності (повнота);

достовірність контролю.

Впровадження автоматичних систем контролю та діагностування диспетчерських радіолокаторів радіолокаційних систем посадки літаків дозволить відмовитись від старих методів пошуку та діагностування відмов за рахунок результатів прогнозування, створити передумови для роботи з вдосконаленням системи технічного обслуговування і ремонту об'єктів контролю (самоконтроль, надійність, працездатність, контроль та ремонтопридатність, модернізація).

АСПЕКТИ УДОСКОНАЛЕННЯ РАДІОЛОКАЦІЙНИХ СИСТЕМ ПОСАДКИ ЛІТАКІВ

Д.О. Землянський
Харківський національний університет Повітряних Сил ім. І. Кожедуба

На підставі аналізу задач, характеристик, принципів побудови та функціонування радіолокаційних систем посадки літаків (РСП) та вимог до них, закордонних і вітчизняних оглядово-посадочних РЛС, а також рівня безпеки польотів державної авіації обґрунтовується необхідність удосконалювання систем та пристроїв РСП Повітряних Сил Збройних Сил України за такими основними напрямками:

– використання складних видів сигналів (оптимізація формату радіолокаційних сигналів зондування) як у диспетчерських, так і у посадочних радіолокаторах РСП, що дозволяє підвищити завадозахищеність, роздільну здатність та точність вимірювання координат повітряних суден (ПС);

– застосування когерентних методів виявлення сигналів та цифрової обробки радіолокаційної інформації, що дозволяє збільшити дальність спостереження ПС, зменшити енергетичні витрати при збереженні заданої зони спостереження ПС;

– використання моноімпульсних методів вимірювання кутових координат, що підвищує точність їх вимірювання;

– застосування фазованих антенних решіток для реалізації електронного сканування простору променями за курсом і глісадою, що дозволяє підвищити надійність системи та збільшити розміри секторів спостереження.

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ РАДІОЛОКАЦІЙНОЇ ФУНКЦІЇ НЕВИЗНАЧЕНОСТІ СИГНАЛІВ СКЛАДЕНИХ З ПОЛІНОМІВ ЧЕБИШОВА РІЗНИХ ПОРЯДКІВ

Н.І. Килимиста
Харківський національний університет Повітряних Сил ім. І. Кожедуба

На підставі аналізу засобів радіотехнічного забезпечення польотів державної авіації, задач і характеристик радіолокаційних систем посадки літаків та вимог до них, закордонних і вітчизняних оглядово-посадочних РЛС, а також рівня безпеки польотів державної авіації обґрунтовано необхідність удосконалювання систем та пристроїв РЛС Повітряних Сил Збройних Сил України.

Подальший розвиток та удосконалення РЛС відбувається з використанням складних сигналів. В першу чергу це радіолокаційні сигнали з лінійною частотною модуляцією (ЛЧМ) які дуже поширені в теперішній час. Це результат переваги таких сигналів над простими сигналами з точки зору властивостей їх функції невизначеності.

Незважаючи на важливість складних сигналів, необхідно шукати нові типи зондувальних сигналів, даючи шанс покращити роздільну здатність, якість виявлення, оцінки місця положення літаків, їх швидкості та іншої інформації, отриманої з РЛС. Відомо, що досягти такої мети, можливо за рахунок покращення властивостей функції невизначеності радіолокаційних сигналів.

У докладі розглядаються результати моделювання функції невизначеності радіолокаційного сигналу за затримкою та частотою Допплера складеного з поліномів Чебишова різного порядку. Показано, що для таких сигналів можливо наблизитись до функції невизначеності, яка має вузький головний та низький рівень бічних пелюстків. Такі властивості дослідженого сигналу можуть бути використані у перспективних посадочних РЛС з врахуванням досягнень у технології твердотільних ВЧ генераторів.

АНАЛІЗ IID-СКРИТНОСТІ ХАОТИЧНИХ СИГНАЛІВ, ЩО ПРОПОНУЮТЬСЯ ДО ВИКОРИСТАННЯ У РД ПРМГ ТА РСБН

М.Л. Крючка; С.В. Волинець
Харківський національний університет Повітряних Сил ім. І. Кожедуба

У контексті розв’язку завдання забезпечення IID-скритності сигналів РД ПРМГ та РСБН у доповіді розглядається підхід до формування сигнальної конструкції, що використовує просту одномірну модель (парадигму) хаосу зі структурованою безліччю точок у фазовому просторі й концепцію аналітичного сигналу.

Для передачі інформації по радіоканалу використовується фізичний хаос, коли хаотичний сигнал, генерується безпосередньо в радіо- або НВЧ-діапазоні довжин хвиль (прямохаотичні схеми зв’язку). На жаль прямохаотичні системи зв’язку, працюють на відносно невеликих відстанях. У теперішній час у зв’язку з

розвитком цифрових методів формування та обробки сигналів з'явилась можливість створення джерел хаотичних сигналів на основі цифро-аналогових пристроїв, які серійно випускаються з різним ступенем інтеграції, які дозволяють формувати широкосмугові й смугові сигнали з більшим радіусом дії для навігаційних, телекомунікаційних і радіолокаційних систем.

У докладі розглядаються результати моделювання міри IID-скритності хаотичних сигналів РД ПРМГ та РСБН. Показано, що для таких сигналів можливо наблизитись до IID-скритності "білого" смугового шуму. В той же час інтерполяція дискретних хаотичних сигналів призводить до зниження їх скритності. Показано, що смугові хаотичні сигнали мають меншу скритність, ніж широкосмугові.

АСПЕКТИ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ЗБОРУ, ОБРОБКИ ТА ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ ПРО ПОВІТРЯНУ ОБСТАНОВКУ НА КОМАНДНО-ДИСПЕТЧЕРСЬКОМУ ПУНКТІ ПРИ КЕРУВАННІ ПОЛЬОТАМИ ДЕРЖАВНОЇ АВІАЦІЇ

Р.В. Лимар
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Можливість створення нового покоління автоматизованих систем керування польотами державної авіації (АС КПДА) обумовлено розробкою новітніх інформаційних технологій та їх впровадженням на базі сучасних програмних і апаратних комп'ютерних засобів.

У роботі проводиться аналіз автоматизації процесів збору, передавання, перетворення, обробки та відображення інформації про повітряну обстановку на командно-диспетчерському пункті при керуванні польотами державної авіації особами групи керівництва польотами. Обґрунтовується розширення функціональних можливостей обладнання сучасних пунктів керування повітряним рухом у районі аеродрому. Визначається необхідність автоматизації процесів збору, обробки та відображення інформації щодо підтримки прийняття рішень, динамічної метеоінформації, планової та довідкової інформації.

Результати аналізу ступеню автоматизації процесів збору, обробки та відображення інформації про повітряну обстановку автоматизованими система керування польотами державної авіації визначають такі загальні вимоги до їх технічної реалізації як готовність АС КПДА виконувати функції за призначенням, її цілісність як ступінь достовірності результатів, відкритість, безперервність, надійність та відповідність експлуатаційним вимогам, які безпосередньо впливають на безпеку аеродромних польотів державної авіації та ефективність керування польотами в районі аеродрому.

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ЗБОРУ, ОБРОБКИ ТА ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ ПРО ПОВІТРЯНУ ОБСТАНОВКУ НА КОМАНДНО-ДИСПЕТЧЕРСЬКОМУ ПУНКТІ ПРИ КЕРУВАННІ ПОЛЬОТАМИ ДЕРЖАВНОЇ АВІАЦІЇ

А.А. Мартинов
Харківський національний університет Повітряних Сил ім. І. Кожедуба

У роботі проводиться дослідження параметрів спектру зондувального сигналу посадкового радіолокатору, відбитого від повітряного судна, що виконує посадку та рухається у напрямку радіолокаційної системи посадки, тобто посадкового радіолокатору. Обгрунтовується розширення функціональних завдань радіолокаційних систем посадки літаків щодо визначення швидкості повітряного судна на етапі посадки, що безпосередньо впливає на забезпечення належного рівня безпеки польотів. Визначається дискретність вимірювання допплерівського зміщення частоти зондувального сигналу посадкового радіолокатору на основі аналізу параметрів спектру сигналу, відбитого від повітряного судна, що знаходиться на етапі посадки. Розробляються пропозиції щодо реалізації пристрою вимірювання допплерівського зміщення частоти, як наслідок, визначення швидкості повітряного судна на етапі посадки.

Основною метою дослідження є аналіз автоматизації процесів збору, передавання, перетворення, обробки та відображення інформації про повітряну обстановку (ПвО) на командно-диспетчерському пункті (КДП) при керуванні польотами державної авіації особами групи керівництва польотами (ГКрП), що дозволить визначити ступінь автоматизації процесів інформаційно-апаратного забезпечення ГКрП, що безпосередньо впливає на оперативність та якість, безперервність та постійну готовність керування аеродромними польотами державної авіації.

ПІДВИЩЕННЯ ТОЧНОСТНИХ ХАРАКТЕРИСТИК АЗИМУТАЛЬНОГО КАНАЛУ РАДІОТЕХНІЧНОЇ СИСТЕМИ БЛИЖНЬОЇ НАВІГАЦІЇ

І.С. Мороз
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Радіотехнічні системи ближньої навігації призначені для визначення навігаційних параметрів, які характеризують положення ЛА у полярній системі координат. В азимутальному каналі використовується часовий метод вимірювання азимута. При використанні гостроспрямованої азимутальної антени, що обертається, цей метод дозволяє одержати більш високу точність вимірювання азимута у порівнянні з фазовим, внаслідок меншого впливу перевідбитих сигналів від місцевих предметів на точність вимірювання азимута. У кутомірних каналах РСБН-4н використовуються всеспрямовані радіомаяки з гостроспрямованою двопелюстковою ДС, яка обертається у горизонтальній площині з постійною

швидкістю 100 об/хв.

Для підвищення точнісних характеристик у радіомаяках з часовим методом необхідно зменшувати похибку нестабільності частоти обертання азимутальної антени. При використанні синхронних генераторів в системі обертання необхідно забезпечити його живлення стабільною по частоті що забезпечується використанням кварцової стабілізації параметрів живлення. При таких параметрах цю похибку можна не враховувати та потрібно зменшувати похибку установки нуля азимуту за рахунок обробки азимутального сигналу в бортовій апаратурі ЛА і забезпечувати як мінімум $0{,}17^{o}$.

Висока точність визначення азимуту обумовлюється використання цифрових методів виміру часового інтервалу і введенню автоматичних та контролюючих систем до складу наземної та бортової РСБН, які не дозволяють змінюватись робочим параметрам вище встановлених норм.

РОЗШИРЕННЯ ФУНКЦІОНАЛЬНИХ ЗАВДАНЬ РАДІОЛОКАЦІЙНИХ СИСТЕМ ПОСАДКИ ЛІТАКІВ ЩОДО ВИЗНАЧЕННЯ ШВИДКОСТІ НА ЕТАПІ ПОСАДКИ

В.Я. Поворознюк
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Основною метою дослідження є визначення параметрів спектру відбитого сигналу від повітряного судна, що дозволяють вимірювати доплерівське зміщення частоти зондувального сигналу посадкового радіолокатору, відбитого від повітряного судна на етапі посадки, тобто визначати радіальну або посадкову швидкість повітряного судна у посадковому радіолокаторі, що безпосередньо впливає на забезпечення належного рівня безпеки польотів.

Задача із дослідження параметрів спектру зондувального сигналу посадкового радіолокатору, відбитого від повітряного судна на етапі посадки, є актуальною і дозволить вирішити проблему відсутності у керівника зони посадки групи керівництва польотами об'єктивної інформації про посадкову швидкість повітряного судна, особливо після виконання бойових завдань з пошкодженнями та відмовами авіоніки літаків бригад тактичної авіації.

Проведений аналіз методів дослідження спектру сигналів та вимірювання його параметрів показав, що застосовуються два методи вимірювання характеристик спектру сигналів: метод фільтрації та метод обчислення перетворення Фур'є. Спектр відбитого сигналу від повітряного судна на етапі посадки містить спектральні складові на частоті більшій за частоту зондувального сигналу на доплерівське зміщення. Метод цифрового спектрального аналізу, а саме дискрене перетворення Фур'є дозволяє вимірювати доплерівське зміщення частоти зондувального сигналу, відбитого від повітряного судна на етапі посадки, тобто визначати посадкову швидкість повітряного судна, що забезпечить підвищення рівню безпеки польотів.

ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ "ПАР-АРК" ЗА РАХУНОК ВИКОРИСТАННЯ ХАОТИЧНОЇ ДИНАМІКИ

Ю.В. Скарнович
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Одним зі способів підвищення завадостійкості роботи засобів зв'язку і РТЗ є використання завадостійких видів сигналів, до яких відносяться широкосмугові сигнали ШСС. Іноді, ще їх називають шумоподібними.

При розв'язанні завдань підвищення структурної скритності сигналів використання хаотичної динаміки не обмежується випадками маскування сигналу й перенесення корисної інформації.

Для підвищення завадозахищеності важливо також забезпечити інформаційну скритність. Слід зазначити, що структурна й інформаційна скритність можуть бути взаємозалежні, і тоді висока інформаційна скритність може ускладнювати розв'язання завдання розкриття структури сигналу. Тому є важливим розглянути нелінійні дискретні відображення для кодування переданої інформації на етапі, що передує маскуванню або модуляції переданих хаотичних послідовностей. Значно підвищити розвідзахищеність систем передачі інформації можна шляхом використання багатопараметричних відображень, що генерують хаотичні послідовності. Як показало математичне моделювання, гарні результати також були отримані при використанні моделей на основі композиції трикутних відображень.

Результатом є тактико-технічні вимоги до проектованої кутомірної РНС з використанням хаотичної динаміки, структурна схема кутомірної РНС типу "ПАР-АРК", та характеристики її скритності, а також використання завадостійких видів сигналів в кутомірній радіонавігаційній системі "ПАР-АРК", які широко використовується при вирішувані задач навігації і посадки літальних апаратів всіх видів авіації.

МЕТОД ПІДВИЩЕННЯ ТОЧНОСТІ ДОППЛЕРІВСЬКОГО РАДІОПЕЛЕНГАТОРА ЗА РАХУНОК ЗБІЛЬШЕННЯ БАЗИ АНТЕННОЇ СИСТЕМИ

В.Д. Юдін
Харківський національний університет Повітряних Сил ім. І. Кожедуба

У державній авіації України ще достатньо широко застосовуються застарілі методи і засоби радіопеленгування, що не дозволяють отримання кутомірної інформації з достатньої точністю. Це призводить до великих лінійних похибок при виході літака в район злітно-посадкової смуги по пеленгаторної інформації, а так само до оцінки місця проведення пошуково-рятувальних операцій.

В основу побудови авіаційних пеленгаторів покладені такі широко відомі методи пеленгування, як амплітудний, амплітудно-фазовий, допплерівській. Основними факторами, що впливають на точність, є: горизонтальна складова поля

сигналу, що пеленгується, відбиття від місцевих об'єктів і співвідношення сигнал/завада в точці прийому. Найбільшу завадостійкість мають допплерівські пеленгатори, похибка яких в 3 рази менше, ніж у амплітудних.

З метою підвищення точності пеленгування допплерівським пеленгатором запропонований двошкальний метод, при якому по грубому каналу проводиться однозначний, але менш точний вимір пеленга, з подальшим його уточненням в точному каналі, де присутня багатозначність. Грубий канал працює на першій гармоніці частоти модуляції, а точний на одній з наступних. При цьому база антенної системи вибирається з міркувань найкращої роботи грубого (однозначного) каналу. Для точного каналу база антенної системи віртуально збільшується в число, що відповідає номеру гармоніки напруги частоти модуляції. Це збільшення бази антенної системи призводить до підвищення крутості пеленгаційної характеристики (чутливості) пеленгатора, та надає можливість підвищити точність.

ДОСЛІДЖЕННЯ ШЛЯХІВ ПОКРАЩЕННЯ ОСНОВНИХ ХАРАКТЕРИСТИК ЗАСОБІВ РАДІОЗВ'ЯЗКУ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО ЗА РАХУНОК ВИКОРИСТАННЯ МОДИФІКОВАНОЇ ТЕХНОЛОГІЇ MIMO-OFDM

А.І. Шкода; В.І. Василишин
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Досвід проведення антитерористичної операції в Україні вказує на потребу підвищення пропускної спроможності системи радіозв'язку. Така потреба виникає при вирішенні задачі передачі даних між безпілотним літальним апаратом та наземним пунктом управління і в ряді інших випадків.

На сьогоднішній день для підвищення пропускної спроможності систем радіозв'язку можуть бути використані технології MIMO (Multiple Input Multiple Output), згідно з якою антенні решітки розташовані на передавальній та приймальній сторонах лінії, OFDM (Orthogonal Frequency-Division Multiplexing –мультиплексування з ортогональним частотним розділенням сигналів), поєднання цих технологій, адаптивна модуляція і інші підходи.

Особливістю технології OFDM та відповідно технології MIMO-OFDM є те, що вони пов'язані з використанням прямого (зворотнього) швидкого перетворення Фур'є (ШПФ). При цьому виникає потреба блокування позасмугового приймання небажаних сигналів, що діють по бічних пелюстках амплітудно-частотних характеристик (АЧХ) фільтрів, синтезованих за допомогою ШПФ. Для зниження рівня бічних пелюсток АЧХ фільтрів пропонується використовувати віконні (вагові) функції (Хеммінга, Хеннінга (Ханна) та ін.), які можуть бути розглянути основою одного з варіантів модифікованої технології MIMO-OFDM. Результати проведеного імітаційного моделювання підтверджують переваги використання віконних функцій.

МЕТОДИ ПІДВИЩЕННЯ ДАЛЬНОСТІ АВІАЦІЙНОГО РАДІОЗВ'ЯЗКУ УКХ ДІАПАЗОНУ

А.М. Магурін; О.І. Чечуй
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Досвід ведення бойових дій в сучасних військових конфліктах різного рівня переконливо свідчить про те, що стійкий зв'язок, який відповідає вимогам з живучості, надійності та завадостійкості, є однією з найважливіших умов успіху бойових дій авіації та інших родів військ.

Для підвищення дальності зв'язку в авіаційних системах радіозв'язку УКХ діапазону існує велика кількість методів. Найбільш широке та виправдане застосування отримали методи з використанням пристроїв ретрансляції. З метою скорочення витрат та можливостей модернізації існуючих засобів авіаційного радіозв'язку пропонується внесення до складу бортової радіостанції УКХ діапазону ретрансляційного (репітерного) пристрою. Такий пристрій в режимі ретрансляції забезпечить 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 зв'язку запропонованого пристрою ретрансляції досліджені імітаційним моделюванням.

Для автоматичного керування режимами роботи радіостанції пропонується використання методу VAD (Voice Activity Detection), що дозволить оператору не ускладнювати методику роботи з радіостанцією та підвищити оперативність зв'язку.

Запропоноване рішення може бути рекомендовано для застосування на всіх типах бортових радіостанцій УКХ діапазону.

ПРОПОЗИЦІЇ ЩОДО ПОКРАЩЕННЯ ХАРАКТЕРИСТИК ТЕЛЕВІЗІЙНИХ СИСТЕМ ПОВІТРЯНОЇ РОЗВІДКИ

А.В. Лук'яненко; А.П. Глушко
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Досвіду проведення АТО та інших військових (збройних) конфліктів висуває до повітряної розвідки (ПР) певні вимоги й обумовлює нові напрямки її розвитку. Проведення повітряної розвідки вдень та вночі в широкому діапазоні висот і швидкостей на визначену глибину в умовах використання противником різноманітного роду завад та засобів маскування й імітації можливе тільки при комплексному застосуванні інфрачервоної, радіолокаційної, телевізійної, лазерної, радіотехнічної розвідки.

З аналізу характеристик телевізійних систем ПР, які знаходяться на озброєнні, можна зробити висновок, що вони не відповідають в повному обсязі сучасним вимогам. В той же час стан розвитку й застосування інформаційних технологій дозволяє вирішити ряд важливих задач при побудові телевізійних систем, а саме:

– покращити розділювальну здатність системи;

– збільшити тривалість "світлового дня";

– збільшити висоту ведення повітряної розвідки.

Таким чином, пропозиції щодо покращення характеристик телевізійних систем ПР є актуальними для Повітряних Сил.

Поставлену задачу вирішено шляхом синтезу цифрового пристрою (фільтр), який здійснює двомірну рекурсивну обробку відеосигналу та реалізований на основі диференційної імпульсно-кодової модуляції. Вибрана модель телевізійного зображення розглядалась як випадкове поле на фоні шуму та апертурних викривлень, обумовлених первинним перетворювачем. Синтезований цифровий пристрій містить дві складові. Перша частина – кодер телевізійної системи, розташований на літальному апараті, друга частина – декодер телевізійної системи, розташований на пункті управління. Передача інформації від кодеру до декодеру здійснюється по цифровому авіаційному каналу зв'язку. У результаті синтезу запропонована шумостійка телевізійна система (по відношенню до шуму фотоелектричних перетворювачів) з корекцією апертурних викривлень відеосигналу.

Висновки роботи ґрунтуються на результатах імітаційного моделювання. Урахування шуму первинного перетворювача покращує шумостійкість системи в порівнянні з випадком коли шум вважається білим. Компенсація шуму збільшить тривалість "світлового дня" та висоту польоту літального апарату, який здійснює розвідку. Корекція апертурних викривлень суттєво залежить від відношення сигнал-шум, збільшення якого впливає на розділювальну здатність телевізійної системи.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ СКОРОЧЕННЯ ЧАСУ ПЕРЕБУДОВИ ДКМХ РАДІОСТАНЦІЇ СЕРЕДНЬОЇ ПОТУЖНОСТІ НА НОВІ ЧАСТОТИ З УРАХУВАННЯМ ОСОБЛИВОСТЕЙ ЇХ ЗАСТОСУВАННЯ ПРИ ПРОВЕДЕННІ АТО

С.В. Женжера; Л.Г. Левченко
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Досвід організації зв'язку в ході АТО призвів до зміни ряду поглядів на способи організації зв'язку та принципи побудови системи зв'язку у Збройних силах України. Виникла проблема використання короткохвильових (КХ) радіостанцій середньої потужності поблизу лінії бойового зіткнення, які через велику потужність випромінювання легко визначалися засобами радіоелектронної розвідки супротивника і знищувалися ракетно-артилерійським вогнем відразу ж після включення на передачу. Тому актуальним постало завдання модернізації існуючих ДКМХ радіостанцій з метою забезпечення більш високої оперативності, швидкості налаштування та випромінювання з більш високим коефіцієнтом корисної дії для оперативного інформаційного обміну на відстані їх від лінії бойового зіткнення в радіомережах штабу АТО з пунктами управління оперативних командувань і штабами ПС, а також в радіомережах за межами АТО.

Скорочення часу перебудови на нові частоти можливе за рахунок запропонованого датчика модуля та датчика фаз в системі автонастройки антенно-погоджуючого пристрою (АПП), при цьому це можливо реалізувати без серйозних

переробок елементів системи управління обраної за прототип радіостанції. Перевагами запропонованого інженерного рішення є використання малого інтервалу часу (близько 1,5...4 хв. замість 30...60 хв.) на настроювання десяти фіксованих частот та перехід з одного пакету частот в інший, спрощення налаштування АПП, забезпечення максимального рівня сигналу на виході антени, тобто передача сигналу з високим коефіцієнтом корисної дії.

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ШВИДКОДІЇ СИНТЕЗАТОРІВ ЧАСТОТ З МЕТОЮ ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

О.М. Чекунова; Я.Ю. Старусьов
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Події, що відбуваються у зоні АТО, засвідчують про застосування противником нового підходу до ведення бойових дій, що більше підвищило значення живучості військ в зоні АТО для досягнення успіху в бою (операції), та значно ускладнило рішення цієї задачі. Живучість військ в зоні АТО нерозривно пов'язана з живучістю органів управління, ефективність яких забезпечує одна з складових, а саме система зв'язку.

Важливими тенденціями розвитку систем зв'язку являються освоєння високих частот та перехід до використання складних сигналів для створення нових перспективних систем зв'язку з підвищеною швидкодією.

Застосування методів цифрового синтезу частот дозволяє значно покращити технічні характеристики РЕЗ: в радіомовленні та телебаченні – покращити якість звукових та телевізійних сигналів, в радіолокації – підвищити пропускну здатність по дальності та по швидкості, в навігації та радіопеленгації – зменшити помилки визначення координат об'єкту, в радіозв'язку – покращити швидкодію, скритність та надійність сеансу зв'язку.

До недавнього часу для створення малогабаритних та швидких синтезаторів частот (СЧ) найбільш широко застосовувалися цифрові обчислювальні синтезатори, основною перевагою яких є можливість точної зміни вихідної частоти та фази по команді з ЕОМ або цифрового процесора. Однак у даних синтезаторах порівняно невисока частота вихідного сигналу, недостатній рівень бічних спектральних складових, високе енергоспоживання та потреба в додатковому тракті формування сигналу тактової частоти, значення якої як мінімум в три рази перевищує максимально синтезуєму частоту. Перераховані недоліки обумовили актуальність застосування в приймально-передавальних пристроях СЧ, побудованих на основі методів косвенного синтезу, що використовують систему імпульсно-фазової автопідстройки (ІФАП) та мають більш просту реалізацію.

Однією з проблем створення СЧ на основі системи ІФАП є погіршення фазових шумів синтезованого коливання при зменшенні кроку сітки вихідних частот. Однак, використання в синтезаторах з ІФАП цифрових ДДЗКД дозволяє отримати вихідне коливання з достатньо високою спектральною чистотою. Крім того, прискорити час входження в синхронізм.

Запропоноване технічне рішення побудови цифрового СЧ дозволило зменшити час входження системи в синхронізм до 20%, спростило технічну реалізацію блоку

ДОЧ та другого гетеродина за рахунок відсутності потреби використання 12 функціональних елементів, що значно розширило технічні можливості обраної за прототип радіостанції М, а також дало змогу забезпечувати якісний зв'язок, між наземними пунктами управління при виконанні бойових завдань в зоні АТО.

DDOS-АТАКА ТА ЇЇ ЗАГРОЗА І НАСЛІДКИ У СУЧАСНОМУ ЖИТТІ

Л.В. Алексейчик
Харківський національний університет Повітряних Сил ім. І. Кожедуба

На DDoS-атаки почали скаржитися ще в 1996 році. Однак широку увагу до проблеми виникло тільки в кінці 1999 року, коли практично одночасно були виведені з ладу веб-сервіси найбільших світових корпорацій (Amazon, Yahoo, CNN, eBay, E-Trade та інших). Вживати термінових заходів щодо вирішення проблеми стали лише в грудні 2000 року, коли знову були здійснені впливу на сервера ключових корпорацій.

Найпоширеніші проблемні питання:

- Що таке DdoS?
- Хто може постраждати від DDoS-атаки?
- Як відбувається DDoS-атака?
- Як запобігти DDoS-атаку?
- Історія виникнення DDoS-атак

Мета DDoS-атаки – повне припинення роботи атакується сервера за рахунок подачі на нього велику кількість помилкових запитів.

Ddos атака: причини виникнення:

- Конкуренція
- Шахрайство
- Розвага

Як наслідок будь-яка DDoS атака прямо надає впливає на продуктивність корпоративних порталів, додатків, сервісів і послуг. Все частіше зустрічаються випадки проведення атак на конкретну компанію і результатом таких атак зазвичай є зниження продуктивності ресурсів не тільки компанії жертви, а й інших підприємства. Популярними жертвами DDoS-атак стають комерційні та інформаційні сайти. Хакери останнім часом використовують такий вид атак з метою вимагання, вимагаючи грошей за припинення атаки, або ведуть інформаційну війну.

У доповіді подається перелік наслідків DDoS-атак. Боротися з таким видом атак досить складно з огляду на те, що запити надходять з різних сторін. Як правило, захист включає такі заходи: фільтрація, усунення вразливостей сервера, нарощування ресурсів, розосередження (побудова розподілених систем, які продовжать обслуговувати користувачів), ухилення (відведення безпосередньої мети атаки від інших пов'язаних ресурсів, маскування IP- адреси).

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

СНІФФЕР

С.О. Бойко
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Сніффер – аналізатор трафіку, або сниффер (від англ. To sniff – нюхати) – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначене для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів. Під час роботи сніффер мережевий інтерфейс перемикається в "режим прослуховування" (Promiscuous mode), що і дозволяє йому отримувати пакети, адресовані іншим інтерфейсів в мережі.

Перехоплення трафіку може здійснюватися: звичайним "прослуховуванням" мережевого інтерфейсу; підключенням сніффер в розрив каналу; відгалуженням (програмним або апаратним) трафіку і напрямком його копії на сниффер; через аналіз побічних електромагнітних випромінювань і відновлення, таким чином, що прослуховується трафіку; через атаку на канальному або мережевому рівні, що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сниффер з подальшим поверненням трафіку в належний адресу.

Сніффери застосовуються як в благих, так і в деструктивних цілях. Аналіз минулого через сниффер трафіку дозволяє: виявити паразитний, вірусний і закільцований трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв'язку.

- Виявити в мережі шкідливе і несанкціоноване ПО;
- Локалізувати несправність мережі або помилку конфігурації мережевих агентів;
- Перехопити будь-який не зашифрований призначений для користувача трафік з метою отримання паролів і іншої інформації;

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

BITCOIN - ДЕЦЕНТРАЛІЗОВАНА ЕЛЕКТРОНА ВАЛЮТА

О.В. Гейвах
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Bitcoin – електронна валюта в основі якої лежать криптографічні методи, вона була створена у 2009 році Сатосі Накамото, має відкритий код та написана мовою C++. Повна капіталізація ринку біткоїнів зараз становить $8,274,088,241 USD. Ціна одного біткоїна на 5 березня 2014 року – 663.78доларів.

Bitcoin не має централізованого управління (криптографічні ключі до грошей зберігаються на локальному диску користувача) та немає прив'язки до жодної з валют чи до будь-якого дорогоцінного матеріалу. Транзакції із цифровим підписом між двома вузлами передаються до всіх вузлів через peer-to-peer мережу, а самі дані про переміщення коштів зберігаються у розподіленій базі даних. Для запобігання можливості трати чужих грошей або використання своїх коштів двічі –

використовуються криптографічні методи. За допомогою цих методів створюються унікальні маркери валюти. Фізично, кожна монета в системі має свій унікальний ключ. Фактично, номінал однієї монети дорівнює певній кількості процесорного часу. Математично алгоритм спроектований так, що з розвитком системи, генерація нових грошей стає більш складнішим обчислювальним завданням, вимагаючи більше потужностей. Спочатку система активно залучає широкі маси учасників мотивацією досить легко збагатитися, наступна стадії запуск стандартної біржової торгівлі, породжуючи конвертованість і зовнішній попит на BTC.

Максимальна кількість монет 21 млн, після чого емісія буде зупинена та настане третя заключна фаза – стабілізація. Країни які фактично визнали валюту: Німеччина, Хорватію. Наприкінці серпня 2013 Міністерство фінансів ФРН зробило заяву про те, що Bitcoin не може бути класифікований як електронна або іноземна валюта, а більше підходить під визначення приватні гроші, за допомогою яких можуть здійснюватися багатосторонні клірингові операції. Національний банк Хорватії вважає, що Bitcoin є законним в Хорватії, але його не слід розглядати як електронні гроші, хоча він має деякі подібності з ними, може легально використовуватися в країні, але продавці не зобов'язані їх приймати в Хорватії нарівні з місцевою валютою. А от США, Китай та Росія намагаються утримати громадян від транзакцій з Bitcoin. 5 грудня 2013 Народний банк Китаю заборонив китайським фінансовим компаніям проводити операції з Bitcoin. У заяві зазначено, що Bitcoin не є валютою в реальному сенсі цього слова. Фінансовим компаніям заборонені не тільки прямі операції з Bitcoin, а й публікація даних про його курс або страхування фінансових продуктів, пов'язаних з Bitcoin. Водночас фізичні особи можуть вільно брати участь в інтернет-транзакціях на свій страх і ризик. Bitcoin-монети при цьому розглядаються як якийсь товар, але не грошові кошти. На даному етапі є десяток форків валюти Bitcoin і тільки одна з них почала другий етап розвитку, тоді коли Bitcoin розпочинає третій етап.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

М.О. Грошова
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Фальсифікація товарів, документів і продукції останнім часом набула масового характеру. Майнова та моральна шкода наноситься громадянам і підприємствам підробкою товарів, цінних паперів і фальсифікацією документів. Шахраї використовують сучасну копіювальну техніку та інші новітні технічні засоби.

Для захисту інформації від навмисних або випадкових спотворень в електронний документообіг знаходить широке використання електронний цифровий підпис.

Електронний цифровий підпис – реквізит електронного документа, призначений для захисту даного електронного документа від підробки, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису, що дозволяє ідентифікувати власника

сертифіката ключа підпису, а також встановити відсутність спотворення інформації в електронному документі.

Мета роботи: вивчення електронного цифрового підпису як інструменту для надання юридичної сили електронним документам.

Електронний цифровий підпис – послідовність символів, отримана в результаті криптографічного перетворення вихідної інформації, яка дозволяє підтверджувати цілісність і незмінність цієї інформації, а також її авторство.

Електронний цифровий підпис заснований на асиметричних криптографічних алгоритмах. Особливістю таких алгоритмів є те, що для шифрування інформації використовується один ключ, а для її розшифровки – інший, спеціальним чином отриманий з першого.

Використання електронного підпису дозволяє здійснити:

Контроль цілісності переданого документа: при будь-якому випадковому або навмисному зміні документа підпис стане недійсним, тому що обчислений він на підставі вихідного стану документа і відповідає лише йому.

Захист від змін (підроблення) документа: гарантія виявлення підробки при контролі цілісності робить підроблення недоцільним в більшості випадків.

Неможливість відмови від авторства. Так як створити коректний підпис можна лише знаючи закритий ключ, а він відомий тільки власнику, він не може відмовитися від свого підпису під документом.

Доказове підтвердження авторства документа: так як створити коректний підпис можна, лише знаючи закритий ключ, а він відомий тільки власнику, він може довести своє авторство підпису під документом. Залежно від деталей визначення документа можуть бути підписані такі поля, як "автор", "внесені зміни", "мітка часу" тощо.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ СЕРВЕРА БД SQL SERVER

В.С. Данилюк
Харківський національний університет Повітряних Сил ім. І. Кожедуба

У сучасних умовах, коли інформація має величезне значення, вживання заходів для запобігання несанкціонованому доступу, попередження втрати або пошкодження інформації стають невід'ємною частиною роботи будь-якої організації. Система зберігання інформації повинна бути максимально захищена як від випадкового, так і від зловмисного пошкодження або спотворення інформації. Система управління базами даних Microsoft SQL Server 2000 має різноманітні засоби забезпечення захисту даних.

Оскільки SQL Server є досить складним продуктом і постійно удосконалюється стоїть питання підвищення рівня його захисту,яке раціональніше проводити у декілька етапів:

- захист мережевого обміну;
- захист операційної системи;
- захист компонентів бази даних;
- захист програм, що використовують базу даних.

Захист SQL Server повинен бути простий для адміністрування. У нових версіях SQL Server, з'явився цілий набір гнучких і могутніх методів управління доступом користувачів до ресурсів SQL Server і базам даних.

Аутентифікація – це підтвердження наявності права у користувача. Авторизація – це визначення можливості допуску користувача до операцій над об'єктами, до набору яких він пройшов аутентифікацію. В даному випадку, аутентифікація відбувається тоді, коли користувач підключається до SQL Server, а авторизація відбуваються всякий раз, коли користувач намагається звертатися до даних або виконує команди.

Наступний крок у формуванні системи безпеки полягає у виділенні груп, в які будуть поміщені облікові записи користувачів, схожих за типом доступу до даним або об'єднаних використанням однієї програми. Кожна група потребує різних прав доступу до бази даних. Останній крок в налаштуванні системи безпеки сервера баз даних полягає в створенні призначених для користувача ролей баз даних і призначенні ним дозволів. Найпростіший спосіб, це створити ролі з назвами, які відповідають іменам глобальних груп. Використовуючи такий підхід можна обмежити процес надання доступу даним операціями, що виконуються на контролері домена, причому так, що внесені зміни будуть відбиті у всіх серверах.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

МУЛЬТИФУНКЦІОНАЛЬНА ІГРОВА СИСТЕМА

О.А. Кліменко
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Як створюються відеоігри? Яку шкоду вони приносять людині? Чи потрібні відеоігри? Етапи створення гри? За допомогою чого? Малювання, графіка, розмальовка, анімація. Яку позицію відеоігри зайняли в сучасній інфраструктурі?

Відеоігри міцно зайняли свою позицію в сучасній індустрії розваг. Робились спроби виділити комп'ютерні ігри як окрему область мистецтва. Перші примітивні комп'ютерні та відео ігри були розроблені в 1950-х і 1960-х роках. Вони працювали на таких платформах, як осцилографи, університетські мейнфрейми і комп'ютери EDSAC. Найпершою комп'ютерною грою став симулятор ракети, створений в 1942 Томасом Голдсмітом.

Перед тим як почати створювати комп'ютерну гру, потрібно визначити до якого класу вона буде відноситися. Один з найпоширеніших варіантів класифікації має такий вигляд: адвентурні (пригодницькі), стратегії, аркадні, рольові, логічні, симулятори.

Адвентурні (пригодницькі) – візуально ці ігри оформлені як мультиплікаційний фільм, однак з інтерактивними властивостями – можливістю управляти перебігом подій.

Стратегії. Головна мета стратегічних ігор: управління ресурсами, корисними копалинами, військами, енергією чи іншими подібними складовими (юнітами). Стратегічні ігри розвивають наполегливість, здатність планувати свої дії, тренують багатофакторне мислення.

Аркадні. Для такого жанру характерний поділ гри на рівні, коли нагородою і метою є право переходу до наступного епізоду, так званої місії. Аркадні ігри тренують увагу, швидкість реакції.

Рольові. В іграх цього жанру в розпорядженні гравця є невеликий загін персонажів, кожний з яких виконує певну роль чи функцію.

Логічні – їх корисність полягає в тому, що вони розвивають логічне мислення, особливо в дітей дошкільного віку. Здебільшого це гра з одним завданням чи набором головоломок, які повинен розв'язати гравець.

Умовно виділяють шість етапів створення гри: концепція, програмування, дизайн рівнів, графіка, звукове оформлення, тестування.

Система, що розроблюється представляє комп'ютерну рольову гру в жанрі hack and splash/action RPG з багатьма можливостями для користувача.

Проект, містить наступні завдання:

- створення сюжету;
- створення фізичного движка;
- звукового движка;
- обмеження, ризики, критичні фактори, що впливають на успішність проекту;
- термін завершення окремих етапів;
- майбутні вимоги до системи в разі її розвитку, наприклад, можливість грати через Інтернет;
- інтерфейси і розподіл функцій між людиною і системою;
- як комп'ютерні ігри та відео ігри погано впливають на людину.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

КРИПТОГРАФІЯ

Я.К. Козаріз
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Мета – вивчити літературу по криптології, виявити поняття криптографії, її сфери діяльності.

Завдання даної роботи:

- з'ясувати, що включає в себе поняття "криптология";
- дізнатися, які відомі способи шифрування;
- вивчити сфери використання криптографії;

Завдання дослідження – забезпечення конфіденційності, цілісності і автентичності інформації.

Актуальність:

В даний час, коли комп'ютерні технології знайшли масове застосування, проблематика криптографії включає численні завдання, які не пов'язані безпосередньо з засекречуванням інформації. Сучасні проблеми криптографії включають розробку систем електронного цифрового підпису та таємного електронного голосування, протоколів електронного жеребкування і ідентифікації

віддалених користувачів, методів захисту від нав'язування помилкових повідомлень і т.п. Специфіка криптографії полягає в тому, що вона спрямована на розробку методів, що забезпечують стійкість до будь-яких дій зловмисника, в той час як на момент розробки криптосистеми неможливо передбачити всі способи атаки, які можуть бути винайдені в майбутньому на основі нових досягнень теорії і технологічного прогресу.

Криптоаналіз – наука (і практика її застосування) про методи та способи розтину шифрів. Криптографія і криптоаналіз складають єдину галузь знань - криптології, яка в даний час є областю сучасної математики, що має важливі додатки в сучасних інформаційних технологіях.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

КОМП'ЮТЕРНІ ВІРУСИ ТА ЗАХИСТ ВІД НИХ

Д.Л. Коломієць
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Компю'терний вірус: вчора та сьогодні (Що таке комп'ютерний вірус та сучасні засоби захисту від них)

Чому виникають комп'ютерні віруси? Як уберегти свій комп'ютер від них? Чи є антивірусні програми актуальним засобом захисту. І які з них кращі? Ось такими питаннями можна "окреслити" коло проблем, що виникає перед кожним користувачем комп'ютера.

Об'єктом дослідження є програмне забезпечення комп'ютера.

Предметом дослідження є вірусні та антивірусні програми.

Ціль дослідження:

Вивчити алгоритм створення найпростішого комп'ютерного вірусу.

Дослідити реакцію антивірусних програм на невідомий вірус.

Завданням дослідження є вивчення історії появи комп'ютерних вірусів. Виявилося, що перший вірус як це і буває, був створений не для викрадення інформації, а просто заради забави. Був розроблений алгоритм самого найпростішого вірусу. І на його прикладі досліджено алгоритм впровадження вірусних програм. Проведено анкетування, результати якого показали, що більше 20% курсантів не знають свою операційну систему і антивірусні програми. Також наш тест-вірус не був виявлений різними антивірусними програмами, такими як Антивірус Касперського, Avast і Nod 32. Наша гіпотеза не підтвердилася. Звідси висновок простий: програми не можуть повністю захистити комп'ютер, в першу чергу захист залежить від комп'ютерної грамотності самого користувача ПК.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

ЩО ТАКЕ КОДУВАННЯ ТА ДЕКОДУВАННЯ ІНФОРМАЦІЇ?

О.В. Лозко
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Питання про те, що таке кодування і декодування, може виникнути у користувача ПК з різних причин, але в будь-якому випадку важливо донести коректну інформацію, яка дозволить юзеру успішно просуватися в потоці інформаційних технологій далі.

Кодування даних – це обов'язковий етап в процесі збору та обробки інформації. Кодування – це процес складання зашифрованою комбінації у вигляді списку скорочень або спеціальних символів, які повністю передають початковий сенс послання.

При натисканні на клавіатурну клавішу комп'ютер отримує сигнал у вигляді двійкового числа, розшифровку якого можна знайти в кодової таблиці – внутрішньому поданні знаків в ПК.

Кодування різної інформації дозволяє уніфікувати форму її подання, тобто зробити однотипної, що значно прискорює процеси обробки і автоматизації даних при подальшому використанні. В електронно-обчислювальних машинах найчастіше використовують принципи стандартного двійкового кодування, яке вихідну форму подання інформації перетворює у формат, більш зручний для зберігання і подальшої обробки. При декодуванні всі процеси відбуваються у зворотному порядку.

Типи кодування:

- Кодування чисел
- Кодування графічної інформації
- Кодування звукової інформації
- Кодування інформації у двійковому коді

Ми змогли дізнатися, що таке кодування і декодування і для чого його використовують. Можна зробити висновок, що використовувані методики перетворення даних повністю залежать від типу інформації. Це може бути не тільки текст, а ще й числа, зображення і звук.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

КОМП'ЮТЕРНИЙ ХРОБАК

А.В. Лютий
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Завдання дослідження – виявлення та знищення комп'ютерного вірусу – хробак.

Хробак складається з двох різних частин. Один відноситься до комп'ютерних вірусів, а інший до оптичної технології зберігання даних.

Також як і живий хробак, який проробляє собі прохід в грязі і грунті, комп'ютерний хробак робить собі прохід через пам'ять комп'ютера і жорсткого диска. Комп'ютерний хробак є одним з видів вірусу, який відтворює сам себе, але

не змінює ніяких файлів на вашому комп'ютері. Тим більш , хробак може викликати хаос, шляхом множення і ділення себе, стільки разів, що вони займають на комп'ютері, всю доступну пам'ять на жорсткому диску. Якщо хробак споживає пам'ять, то ваш комп'ютер буде працювати дуже повільно. А в залежності від різновиду хробака, це може привести до поломки жорсткого диска, і втрати всіх даних. Якщо черв'як впливає на вільне місце жорсткого диска, у вашого комп'ютера займатиме дуже багато часу, щоб відкрити доступ до файлів або папок.

І в кінцевому підсумку, ви не зможете що-небудь зберегти або створити нові папки, поки хробаки не буде ліквідовано.

Проте є деякі проблемні особливості:

- Хробак дуже швидко розмножується.
- Його важко видалити.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

ЯК СТВОРЮВАЛИ ПЕРШУ В РАДЯНСЬКОМУ СОЮЗІ ОБЧИСЛЮВАЛЬНУ МАШИНУ

О.В. Приймак
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Багато вчених по всьому світу працювало над створенням універсальних обчислювальних пристроїв для державних потреб під час другої світової війни. Так, у Сполучених Штатах Америки у 1945р. вступила в дію обчислювальна машина "ENIAK" (Electronic Numerscal Integrator and Computer) – електронний цифровий інтегратор і обчислювач. Більше 17 тис. електронних ламп об'єднувалося у її складі, розміри машини були: 6 м – у висоту і 26 м – у довжину. "ENIAK" опрацьовував десяткові числа, оскільки конструктори вважали за потрібне, щоб "машина була зрозумілою для людини". Головним недоліком комп'ютера "ENIAK" були труднощі, які виникали при введенні програм. Об'єм внутрішньої пам'яті був зайнятий числовими даними, які використовувалися у розрахунках, а для введення програм в ручному режимі під'єднувалися та роз'єднувалися сотні контактів, що було доволі незручно. В наступній моделі – "EDVAC" (Electronsc Discrete Automatic Variable Computer) – електронний дискретний змінний комп'ютер – внутрішня пам'ять містила не тільки дані, але й програму. Комп'ютер "EDVAC" кодував дані у двійковій системі числення, що дозволило суттєво скоротити кількість електронних ламп.

Перша в Радянському Союзі електронна обчислювальна машина (МЕСМ) була прийнята до експлуатації у 1952 р. в Києві. Проектування, монтування і налагодження ЕОМ за 2 роки (з 1950р. по 1952 р.) виконав колектив із 12 співробітників, а також 15 технічних працівників и монтувальників інституту електротехніки АН України під керівництвом видатного вченого-електротехніка Сергія Олексійовича Лебедєва. Лабораторія директора інституту електротехніки розміщалася у будівлях монастиря, що знаходяться у Феофанії, передмісті Києва. На той час це був потужний і сучасний обчислювальний пристрій. Так, час для виконання операції множення на "ENIAK" складало 5,5 мс, на "EDVAC" – 4 мс, а на МЕСМ – 8-9 мс. У 1952-53 рр. ця ЕОМ була єдиною в СРСР, саме на ній

виконувалися найважливіші науково-технічні завдання, які виникали при дослідженні термоядерних процесів (кер. Я.Б. Зельдович), космічних польотів та ракетної техніки (кер. М.В. Келдиш), дальніх електропередач (кер. С.О. Лебедєв) та ін. У 1956 р. лабораторію С.О. Лебедєва очолив В.М. Глушков. На базі лабораторії для обчислювального центру АН України створили ЕОМ "Київ", а у 1961 р. вже відкрився Інститут кібернетики (імені В.М. Глушкова).

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

ФІЛЬТР БАЙЄРА

А.С. Фльора
Харківський національний університет Повітряних Сил ім. І. Кожедуба

У фототехніці для визначення кольорів від білого до чорного призначені сенсори. Їх функціональність залежить від кількості пікселів. А для розрізнення решта спектра використовуються кольорові фільтри.

"Фільтр Байєра", запатентований в 1976 р. Брюсом Байєром – це масив кольорових фільтрів для світлочутливих елементів датчиків зображення. Відповідно, завдяки даному фільтру стало можливим отримувати кольорові зображення з використанням одного датчика.

Загальний принцип роботи колірних фільтрів такий. Кожен піксель повинен мати свій колір і фільтр, який поміщається над кожним з них. Фотони не відразу потрапляють на відповідний піксель. Перш вони повинні подолати бар'єр у вигляді фільтра, що пропускає лише певний колір. А решта спектрів їм нейтралізуються.

Найбільш потужними є кольорові "фільтри Байєра", які дозволяють досить ефективно отримати потрібний колір шляхом змішування трьох основних. Технологія заснована на просторовому розділенні, де фільтри розташовуються в шаховому порядку, причому фільтрів зеленого кольору рівно в 2 рази більше, ніж червоних і синіх, тобто 25 % червоних, 25 % синіх і 50 % зелених елементів. Така схема відома як RGB. Виходить, що між двома зеленими кольорами полягають синій і червоний. Це співвідношення не випадково й ґрунтується на особливостях будови органу зору людини. Для очей самим розпізнаваним є зелений колір, а шаховий порядок потрібен для забезпечення однаковості одержуваного зображення незалежно від положення фототехніки - вертикального або горизонтального.

Три кольорових фільтри необхідні для того, щоб відтворювати колір з монохромної інформації, що охоплюється сенсором зображення.

До винаходу Байєра для формування кольорового зображення світло поділяли на три потоки і направляли на три окремих сенсори – така схема і сьогодні застосовується в професійній техніці, але вона занадто незручна і дороговартісна для реалізації в масової споживчої техніці.

Байєр запропонував найбільш економний метод імітації сприйняття кольору людським оком. "Фільтр Байєра" використовується практично повсюдно, в переважній більшості сучасних цифрових фото- і відеопристроїв, включаючи камери смартфонів. Придумані пізніше більш прогресивні схеми вимагають більш складних алгоритмів і більш продуктивних процесорів.

"Фільтр Байєра" – початково не тільки найперший варіант розташування фільтрів на матриці, але і найбільш простий в обробці варіант фільтра.

Крім самого фільтра, Байєр розробив алгоритми для зберігання, аналізу, обробки та друку зображень, отриманих цифровими пристроями. Ймовірно, без Байєра розвиток технологій отримання цифрових зображень був би далеко не таким активним.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

ЩО ТАКЕ ОПЕРАЦІЙНІ СИСТЕМИ

А.І. Чернобель
Харківський національний університет Повітряних Сил ім. І. Кожедуба

Операційні системи можуть бути класифікованими за будовою ядра (монолітні, мікроядерні, наноядерні), призначенням (пакетна обробка, інтерактивність, підтримка реального часу тощо), реалізацією захищеності (один адресний простір чи підтримка захищеності пам'яті на рівні апаратури), актуальністю (сучасна чи історична), цільовою апаратною платформою (суперкомп'ютер, мейнфрейм, сервер, робоча станція, вбудований комп'ютер, мобільний пристрій), за типом ліцензії (комерційна чи вільна) та за багатьма іншими параметрами

Операційна система (ОС) – це програма, що забезпечує можливість раціонального використання устаткування комп'ютера зручним для користувача образом.

Найпоширеніші операційні системи світу:

- Windows
- Android
- Ios
- Linux

Для покращення якості операційних систем потрібно постійно виготовляти нові версії ОС або їх прошивки. На даний час дуже багато старих повільно працюючих ПК, яким потрібно виготовити ОС, щоб вона покращила їх багатозначність і швидкість завантаження даних.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.

ШТУЧНИЙ ІНТЕЛЕКТ, ІСТОРІЯ ТА ЙОГО ПРОБЛЕМИ

В.І. Ярошенко
Харківський національний університет Повітряних Сил ім. І. Кожедуба

При вирішенні будь-якої задачі управління здійснюється обробка інформації на рівні спеціаліста з можливим залученням засобів комп'ютерної обробки.

Інформаційне забезпечення повинне забезпечити ефективність обміну інформацією між керівництвом і об'єктом управління. В склад інформаційного забезпечення, звичайно, включають дані, які характеризують різнобічну діяльність підприємств, нормативні та законодавчі акти, що впливають на процеси

господарювання, засоби їх формалізованого опису, програмні засоби ведення і підтримки баз даних.

Швидкі зміни в політичній та економічній сферах країни ще більше підкреслили роль своєчасного інформаційного забезпечення для управління виробництвом. Економічні моделі діяльності часто визначаються не стільки інтересами власника виробництва, а і в значній мірі формуються під впливом дії законів та податкової політики держави. Це і обумовлює необхідність впровадження та мобільного використання експертних систем, які б допомагали орієнтуватися в динамічно змінному середовищі, – на що у менеджерів не вистачає часу через основні обов'язки.

Проте хочеться відмітити такі проблемні питання:

- Підходи і напрямки до розуміння штучного інтелекту.
- Експертні системи як вид систем штучного інтелекту.
- Сучасне тлумачення проблеми штучного інтелекту. Застосування штучного інтелекту в Україні та світі.

У дослідженні йдеться про те, коли нагромаджено досвід в організації технологій переробки інформації, відбувається перехід до створення інформаційних технологій з використанням штучного інтелекту. Вважається, що основні напрями в галузі створення інформаційних технологій і штучного інтелекту пов'язані з винайденням ефективних систем подання знань і організацією процесу комунікації користувачів з ЕОМ, а також з плануванням доцільної діяльності та формуванням глобальної структури нормативної поведінки.

Результати дослідження дозволяють визначити напрямки та сформулювати задачі подальших досліджень.