СЕКЦІЯ 11

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМІ УПРАВЛІННЯ ВІЙСЬКАМИ ТА ОЗБРОЄННЯМ

Керівник секції: к.т.н. доцент О.І. Тимочко
Секретар секції: І.Є. Кужель

15.02.2006 р.: 14.30 – 17.30

д.т.н. Ю.И. Лосев, к.т.н. К.М. Руккас

АНАЛИЗ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ С ПРИОРИТЕТАМИ С УЧЕТОМ ФРАКТАЛЬНОСТИ ВХОДНОГО ТРАФИКА

В современных телекоммуникационных системах (ТКС) одной из важнейших задач является обеспечение требуемого качества обслуживания абонентов. Одним из эффективных методов управления качеством является разделение пропускной способности каналов с использованием приоритетов для различных информационных потоков. В современных ТКС информационные потоки имеют фрактальную природу. Особенностью фрактального трафика является существование кластеризации и непостоянство характеристик во всех временных масштабах. Проведен сравнительный анализ систем массового обслуживания M/G/1 с приоритетами и системы G/G/1 с приоритетами. Получено выражение для вычисления времени ожидания в системе массового обслуживания G/G/1 с приоритетами. Показано, что с увеличением самоподобности входящего трафика значительно увеличивается время ожидания сообщений всех приоритетов по сравнению с системой M/G/1 с приоритетами.

М.В. Гудков, А.В. Воронін

АВТОМАТИЗАЦІЯ ПЛАНУВАННЯ БОЙОВОЇ ПІДГОТОВКИ

Авторами роботи розглянутий процес планування бойової підготовки авіаційної частини та визначені напрямки його автоматизації шляхом створення комплексу програмного забезпечення планування бойової підготовки. Практично реалізований комплекс дозволяє значно скоротити час, який витрачається на планування бойової підготовки в авіаційній частині. Виконання операцій зберігання даних, проведення розрахунків, складання та отримання звітних документів, надання даних для аналізу покладено на ПЕОМ та сучасну оргтехніку. Застосування комплексу у військах дозволить суттєво знизити навантаження на органи планування бойової підготовки, підвищити якість та оперативність планування. Комплекс має гнучку структуру. Вона передбачає

можливість настроювання комплексу для використання його в інших родах авіації та видах Збройних Сил України.

к.т.н. А.А. Адаменко

МЕТОД ВИБОРУ ОПТИМАЛЬНИХ СТРАТЕГІЙ ІНФОРМАЦІЙНОГО ВПЛИВУ НА СУПРОТИВНИКА

Як свідчить досвід останніх локальних війн та збройних конфліктів, все більшу актуальність набувають заходи інформаційної боротьби, які також стають важливою складовою потенціалу стримування агресії в мирний час. Одною з задач інформаційної боротьби є інформаційний вплив на супротивника з метою забезпечення прийняття ним саме того рішення, яке необхідне нам. Як правило, ця задача вирішується в умовах нестохастичної невизначеності. Запропоновано метод вибору оптимальних стратегій інформаційного впливу, який передбачає оперувати нечіткими даними за допомогою використання теорії нечітких множин та приймати рішення з необхідною мірою впевненості.

к.т.н. Б.Н. Судаков, к.т.н. Д.Э. Двухглавов, А.В. Першин

ПОДХОД К РАЗРАБОТКЕ ЕСТЕСТВЕННО-ЯЗЫКОВОГО ИНТЕРФЕЙСА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ РЕАЛЬНОГО ВРЕМЕНИ

Рассматривается структура системы поддержки принятия решений (СППР) реального времени, указывается на необходимость применения естественного языка для взаимодействия различных групп пользователей с системой. Предлагаются новые методы и модели, используемые для построения естественно-языкового интерфейса (ЕЯИ) СППР, базирующиеся на математическом аппарате теории категорий и многозначной логике присутствия, позволяющие учитывать неопределенность и противоречивость процессов, протекающих во внешней среде. Обосновывается структура процессора, реализующего ЕЯИ.

к.т.н. В.Л. Петров, Д.В. Антонов

ПІДХІД ДО АНАЛІЗУ ВХІДНИХ ВПЛИВІВ АСУ ДЛЯ ЗАХИСТУ ВІД НЕСАНЦІОНОВАНОГО ДОСТУПУ

Внутрішня структура складних інформаційних об'єктів, таких, як АСУ, Web-ресурси і т.д., може бути представлена у вигляді складного орієнтованого графа, вершини якого являють собою ключові процедури, що виконують наприклад, моніторинг або шифрування інформації, а дуги графа відповідають зв'язкам між вершинами. Найбільш деструктивним вхідним впливом для внутрішньої структури системи керування є несанкціонований доступ до інформації. Система захисту інформації АСУ, залежно від вхідного впливу,

проводить моделювання ступеня цього впливу та оцінює, наскільки сильно він вплине на внутрішню структуру моделі системи керування та на зв'язок між вершинами усередині структури. У результаті моделювання, залежно від вхідного впливу, деякі зв'язки можуть виявитися заблокованими, тому інформаційні потоки підуть в іншому напрямку відповідно до їх цільової функції, що приведе до переорієнтування внутрішньої структури графа. Математично структура графа представлена у вигляді n-вимірних матриць. Модель системи керування, що представлена в такому вигляді, добре підходить для моделювання в термінах Е-мереж Петрі. Процедура прийняття рішення виробляється в результаті рішення матричних ігор із двома та більше гравцями.

А.В. Александров, А.М. Кулабухов

МЕТОД АВТОМАТИЗИРОВАННОЙ ВЫРАБОТКИ РЕКОМЕНДАЦИЙ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ НА УПРАВЛЕНИЕ ОГНЕМ ЗРДН ГРУППИРОВКИ ЗРВ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Предлагается метод, позволяющий расширить круг задач, решаемых автоматизировано в процессе выработки рекомендаций на распределение огня зрдн группировки ЗРВ, за счет использования стратегии рефлексивного управления второго ранга. В отличие от известных, метод предполагает использование гибридной сетевой модели знаний, как основы для математической формализации знаний о процессах выработки рекомендаций на распределение огня зрдн группировки ЗРВ; использование разработанной модели поведения воздушного противника при установлении очередности уничтожения средств воздушного нападения; формализацию знаний о порядке распределения огня зрдн группировки ЗРВ на основе стратегии рефлексивного управления второго ранга; использование модального исчисления предикатов для формализации знаний о порядке реализации замысла командира по осуществлению реальных и фиктивных воздействий по целям.

С.Г. Семенов, В.В. Онищенко, О.Н. Березуцкая, С.Ф. Крывчач

МЕТОДИКА ВЫЧИСЛЕНИЯ КОЭФФИЦИЕНТА ДОЛИ ПОТОКА ИНФОРМАЦИИ ДЛЯ РАСПРЕДЕЛЕНИЯ ТРАФИКА ПО НАЙДЕННОМУ МНОЖЕСТВУ ПУТЕЙ

Существенный недостаток традиционных методов маршрутизации трафика в телекоммуникационных сетях (ТС) заключается в том, что пути выбираются без учета текущей загрузки ресурсов сети. Если кратчайший путь уже перегружен, то пакеты все равно будут посылаться по этому пути. Решить эти проблемы можно, достигая сбалансированной загрузки всех ресурсов ТС

за счет рационального выбора путей прохождения трафика через них. Предлагается методика вычисления коэффициента доли потока информации для распределения трафика по найденному множеству путей, в которую входят алгоритмы начального определения загрузки и распределения возрастающей нагрузки. Методика дает возможность сбалансировать (распределить) нагрузку в линиях связи найденного множества путей. Это позволит уменьшить интенсивности потоков информации в найденных направлениях и соответственно сократить среднее время задержки информации в ТС.

О.В. Воробьев

ИСПОЛЬЗОВАНИЕ ДАННЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ УМЕНЬШЕНИЯ ОБЪЕМА ПЕРЕДАВАЕМОЙ С БПЛА ИНФОРМАЦИИ ОБ ИЗОБРАЖЕНИИ МЕСТНОСТИ

На современном этапе широкое применение в боевых действиях получили разведывательные БПЛА. Но по-прежнему актуальна проблема несоответствия пропускной способности каналов связи и объемов передаваемой информации. Для ее решения используются методы компактного представления информации. Переход к распределенным системам в АСУ и развитие таких геоинформационных технологий дают возможность при применении БПЛА в подсистеме разведки АСУВ часть операций выполнять вне борта и привлечь к их решению значительно больше вычислительных ресурсов. Новые возможности геоинформационных систем (ГИС) позволяют получить изображения участков земной поверхности, приближенные к изображениям, получаемым БПЛА, т.е. можно передать не все изображение, а только те участки, которые представляют информационную ценность. Сформулированное свойство линейности позволяет использовать ортогональное преобразование при обработке разницы значений пикселей текущего изображения и полученного с помощью ГИС. Объем передаваемой информации уменьшается за счет исключения неинформативных блоков изображения и малых по величине коэффициентов преобразования, что позволяет сократить время на передачу информации об изображении без значительной потери качества.

к.т.н. Ю.В. Паржин, к.т.н. А.П. Пашнев, Д.В. Гринев, Н.Ю. Любченко

РАСПОЗНАВАНИЕ ВНУТРЕННЕЙ СТРУКТУРЫ КОНТУРНЫХ ИЗОБРАЖЕНИЙ

Рассматривается подход к построению структурно-лингвистического метода распознавания контурных изображений на плоскости, позволяющего осуществить распознавание объекта не только по его внешнему контуру, но и с учетом его внутренней структуры, сформированной контурами элементов

изображения. Данный подход основан на определении направлений структурного развития подструктур первого уровня вложенности между структурными критическими точками первого и второго рода. Определение данных направлений позволяет сформировать концепты элементов изображения, объединение которых образует концепт всего изображения в целом. Сравнение полученных концептов с эталонными позволяет осуществить классификацию и идентификацию рассматриваемых изображений с вероятностью, превышающей вероятность правильного распознавания с использованием известных структурно-лингвистических методов.

к.т.н. О.В. Сісков, С.І. Сімонов

ВИЗНАЧЕННЯ ЩІЛЬНОСТІ РОЗПОДІЛУ ТОЧОК ПЕРЕТИНУ ПРОСТОРОВИХ ЛІНІЙНИХ РУБЕЖІВ ПОВІТРЯНИМИ ОБ'ЄКТАМИ

Розглянута задача прогнозування інтервалу перетину повітряними об'єктами просторових лінійних рубежів за умов таких припущень та гіпотез: рубіж апроксимується прямою на площині карти місцевості; траєкторії польоту повітряних об'єктів вважаються прямолінійними; похибки вимірювань площинних координат повітряних об'єктів розподілені за нормальним законом. У доповіді обґрунтовано, що відхилення прогнозованого кута перетину повітряним об'єктом просторового лінійного рубежу від 90° (проміж лінією польоту та рубежем) призводить до викривлення нормального закону розподілу точок перетину уздовж рубежу. Для апріорної оцінки ймовірності перетину інтервалів рубежу при довільному куті перетину математично виведено щільність розподілу точок перетину просторових лінійних рубежів повітряними об'єктами.

М.А. Павленко, П.Г. Бердник, А.В. Крыжановский, Н.Н. Бесчасный

МЕТОД РАЗРАБОТКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ СЛОЖНЫМИ ОБЪЕКТАМИ

Деятельность оператора АСУ, связанная с оценкой состояния объекта управления и выработкой управляющих воздействий, возможна при обеспечении его всей необходимой информацией. Для этого в существующих АСУ создана система информационного обеспечения, которая, в частности, включает в себя множество информационных моделей, которые являются основой формирования концептуальной модели ситуации, на основании которой происходит выработка решений на управление системой. Метод разработки системы информационной поддержки принятия решений в АСУ включает в себя следующие этапы: анализ деятельности оператора по управлению сложными и информационного обеспечения процесса принятия решений оператором,

проектирование множества информационных моделей, разработка алфавита информационных признаков, соответствующего особенностям мыслительной деятельности оператора при решении задач управления, выбор и обоснование структуры информационных моделей и структуры рабочего места оператора.

к.т.н. О.О. Лаврут, В.М. Васюк

ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ ЗАСОБІВ ЗВ'ЯЗКУ: МЕТОДИКА ОЦІНКИ ЯКОСТІ

Постійна готовність техніки зв'язку й автоматизації до використання за призначенням досягається правильною організацією технічного обслуговування (ТО), яке є однією з найважливіших складових частин технічної експлуатації. Важливість цієї частини полягає в тому, що саме ТО разом з ремонтом впливають на продовження строку служби засобів зв'язку, що на сьогодні є найбільш актуальним питанням для військ зв'язку. Пропонується методика оцінки якості ТО, яка складається з двох частин: попередня оцінка якості організації ТО в частині, у результаті чого здійснюється перевірка плануючих документів, періодичності й строків проведення ТО; здійснення безпосередньої оцінки якості проведення ТО, що припускає здійснення перевірки наявності та обладнання робочих місць, постів, ділянок, перевірку наявності засобів технічної діагностики, перевірку стану техніки. За допомогою запропонованої методики можна дати точну оцінку якості проведення технічного обслуговування в частині. Це дозволить усунути виявлені недоліки та більш ефективно проводити наступне ТО.

к.т.н. С.В. Дуденко, к.т.н. В.В. Калачова, В.А. Пудов

ТЕХНОЛОГІЇ КОНТРОЛЮ ЗНАНЬ У КОМП'ЮТЕРНИХ СИСТЕМАХ НАВЧАННЯ

Одним з найбільш важливих завдань при створенні комп'ютерних засобів учбового призначення є контроль знань (КЗ). У роботі запропоновано класифікацію методів комп'ютерного контролю знань, а також рекомендації щодо їх застосування при різних видах КЗ. Методи проведення контролю знань можна розділити на три класи: неадаптивні, частково адаптивні, повністю адаптивні. При виборі методу проведення комп'ютерного контролю знань важливо враховувати цілі перевірки, що проводиться, дотримуючись принципу систематичності, який полягає в необхідності проведення контролю на всіх етапах дидактичного процесу – від початкового сприйняття знань і до їх практичного застосування. Пропоновані класифікації методів контролю і оцінки знань можуть бути корисні як розробникам систем комп'ютерного КЗ, так і викладачам при виборі методів проведення КЗ і виставляння оцінки при комп'ютерному навчанні.

к.т.н. О.В. Потій

ЗМІСТОВНА МОДЕЛЬ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ

На сучасному етапі розвитку теорії захисту інформації є дуже актуальною задачею створення наукових та методичних основ управління захистом інформації. При цьому захист інформації розглядається як спеціальна діяльність, яку здійснює персонал організації з метою забезпечення конфіденційності, цілісності, доступності й спостережності інформації та пов'язаних з нею ресурсів, а також гарантій захисту. Пропонується концепція процесного підходу до управління захистом інформації, одним з елементів якої є модель зрілості процесів. Під зрілістю процесів захисту інформації розуміють сукупність спеціальних властивостей процесу, що обумовлюють його здатність досягти запланованої мети та результатів згідно з його призначенням. У доповіді пропонується змістовна модель зрілості, що розроблена шляхом обґрунтування множини властивостей зрілості та визначення зв'язків між таким поняттями, як ознака зрілості, показник зрілості, властивість зрілості, процес захисту інформації.

к.т.н. И.В. Рубан, М.Н. Колмыков, Ю.В. Данюк

АЛГОРИТМ БЫСТРОГО ФОРМИРОВАНИЯ ТРАНСФОРМАНТЫ ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ ХАРТЛИ РАЗМЕРНОСТИ 16×16 ЭЛЕМЕНТОВ

Использование быстрых алгоритмов в ортогональных преобразованиях позволяет уменьшить количество арифметических операций, время выполнения преобразования и упростить техническую реализацию методов обработки информации на основе этих преобразований. С целью повышения эффективности дискретного преобразования Хартли (ДПХ) предлагается алгоритм быстрого формирования трансформанты ДПХ размерности 16 × 16 элементов, который включает в себя следующие этапы: 1) перестановка порядка вычисления коэффициентов ДПХ; 2) расчет промежуточных переменных; 3) вычисление коэффициентов с использованием промежуточных переменных; 4) формирование выходного массива элементов трансформанты в соответствии с их адресным размещением. В результате применения алгоритма при расчете трансформанты 16 × 16 можно сократить количество операций умножения на 70 %, сложения/вычитания – на 60 %.

к.т.н. А.В. Лєншин

ОСОБЛИВОСТІ ОЦІНКИ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ

Об'єктивною рисою, притаманною задачі оцінки зрілості процесів захисту інформації, є неможливість визначення лише кількісних показників та крите-

рій, внаслідок присутності ступеня невизначеності. Природа невизначеності обумовлена як недетермінованістю процесів захисту, так і неможливістю врахування всіх існуючих уразливостей захисту інформації. Іншою особливістю проведення оцінки зрілості процесів захисту інформації є великий обсяг інформації, який необхідно обробляти (під обробкою розуміється збір, розрахунок узагальнених оцінок та значень кількісних показників, ранжирування результатів, зберігання і накопичування інформації тощо), та значна кількість рутинної роботи. Все це зумовлює необхідність автоматизації діяльності з оцінки зрілості процесів. Вимогою до аналітичного апарату, що має використовуватися як формальна основа проведення обчислень в автоматизованій системи, є його можливість забезпечувати надання оцінок, які враховують цю невизначеність, та коректно їх обробляти. На роль такого аналітичного апарату можуть претендувати методи нечітких множин, апарат суб'єктивної логіки, логіко-імовірнісний підхід тощо.

16.02.2006 р.: 10.00 – 13.00

д.т.н. О.В. Лемешко, О.А. Дробот, О.М. Усачов

МЕТОДИКА РОЗПОДІЛУ МЕРЕЖНИХ РЕСУРСІВ ДЛЯ ТРАФІКІВ РІЗНОМАНІТНИХ СЛУЖБ З УРАХУВАННЯМ QOS-ВИМОГ

Інтенсифікація розвитку мережних технологій та інтеграція різних телекомунікаційних служб сприяє підвищенню актуальності задачі оптимального розподілу (перерозподілу) доступних мережних ресурсів. Розв'язання цієї задачі повинне проводитися відповідно до встановлених вимог щодо якості обслуговування за швидкісними та ймовірнісно-часовими показниками.

Запропонована методика розподілу мережних ресурсів для трафіків різноманітних служб з урахуванням вимог щодо якості обслуговування (Quality of Service, QoS). Методика має ієрархічну структуру, ґрунтується на використанні тензорних моделей телекомунікаційних мереж та ітераційних алгоритмах "вибору топології", "вибору пропускних здатностей трактів передачі" та "розподілу потоків".

к.т.н. И.В. Рубан, Ю.В. Долгий

ЗАДАЧИ, РЕШАЕМЫЕ ДИНАМИЧЕСКОЙ СИСТЕМОЙ УПРАВЛЕНИЯ ПОТОКАМИ ИНФОРМАЦИИ И ВЗАИМОДЕЙСТВИЕМ ПРОЦЕССОВ, В СЕТИ АСУ ВОЙСКАМИ И ОРУЖИЕМ

Анализ этапов жизненного цикла сети АСУ войсками и оружием позволил выделить следующие основные задачи, решаемые динамической систе-

мой управления потоками информации и взаимодействием процессов, в сети АСУ войсками и оружием: 1) управление решением задач и использованием вычислительных ресурсов сети в условиях ее деградации; 2) управление маршрутизацией сообщений с обеспечением заданной скрытности передачи информации в сети; 3) оценка пропускной способности в условиях деградации сети; 4) обеспечение адаптивного к изменяющимся потокам заданий управления в узлах сети; 5) оценка состояния сети и восстановление сети в случаях отказов ее функциональных элементов. Решение данного комплекса задач в сетях АСУ специального назначения должно осуществляться в масштабе реального времени, определяемого циклом обновления информации в сети.

к.т.н. К.С. Смеляков, к.т.н. О.М. Попов

СЕГМЕНТАЦИЯ ГРАНИЦ СЛАБО КОНТРАСТНЫХ ИЗОБРАЖЕНИЙ

Для выделения границ контрастных изображений использование существующих масок и критериев является достаточно эффективным. При этом для построения границ изображения по его сегментированным пикселям также используются достаточно эффективные методы прослеживания контуров. Однако применение этих масок и критериев для выделения слабо контрастных изображений не обеспечивает устойчивости и адекватности сегментации ввиду недостаточной адаптируемости масок и критериев сегментации к тополого-геометрическим особенностям объектов и уровням контрастности изображения. Таким образом, для эффективного решения широкого класса прикладных задач, связанных с автоматизацией анализа видеоданных в реальном масштабе времени, актуальной является проблема разработки унифицированной системы моделей изображений нерегулярного вида, включающей тополого-геометрическую и яркостно-контрастную подсистемы, и соответствующих ей устойчивых методов сегментации границ слабо контрастных изображений, основанных на использовании настраиваемых в достаточно широком диапазоне параметрических масок и критериев.

к.т.н. О.Ю. Стрюк, І.А. Сорокін

АНАЛІЗ ОСОБЛИВОСТЕЙ СТАНДАРТУ XML ТА РЕКОМЕНДАЦІЯ ЙОГО ЗАСТОСУВАННЯ ДЛЯ СТРУКТУРИЗАЦІЇ ДАНИХ

Недосконалість мови гіпертекстової розмітки HTML призвела до бурхливого розвитку протягом останнього часу XML-технологій. Збільшується кількість програмних продуктів, оперуючих з даними у форматі XML, що надає стандартну можливість кодування змісту інформаційних документів, забезпечуючи при цьому гнучкість у створенні структур даних. Один з перспективних напрямків використання XML є структурування бібліографічних даних, яке дозволяє здійснити контроль коректності записів на рівні перевірки XML-документа.

XML може бути застосовано для створення системи обміну формалізованими повідомленнями. Повідомлення, які циркулюють у військових інформаційних системах, складаються з заголовка, текста повідомлення, заключної частини. Авторами доводиться, що така структура цілком узгоджується з моделлю XML-документа та може бути реалізована й використана на практиці. Враховуючи переваги формалізованих текстових повідомлень при передачі інформації в інформаційних системах військового призначення, розробка і прийняття в експлуатацію у ЗСУ системи формалізованих повідомлень є доцільною.

к.т.н. К.А. Спорышев, к.т.н. В. Н. Федорченко, А.С. Постольный

ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ШУМОПОДОБНЫХ СИГНАЛОВ, ИСПОЛЬЗУЕМЫХ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Проведен анализ существующих методов формирования шумоподобных сигналов (ШПС). Принцип работы устройств ШПС состоит в "распределении" радиосигнала в широкой полосе частот. Распределение осуществляется при помощи псевдослучайной последовательности. В настоящее время используются два наиболее популярных способа формирования ШПС: метод со скачками по частоте и метод прямой последовательности. В методе со скачками по частоте приѐмник и передатчик синхронно перестраиваются на различные несущие частоты в соответствии с алгоритмом, задаваемым псевдослучайной последовательностью. В методе с прямой последовательностью в передаваемый в радиоканале сигнал вносится значительная избыточность путем передачи каждого бита информации одновременно в нескольких частотных каналах. Сравнивая эти два метода, можно видеть, что вариант со скачками по частоте в общем случае обеспечивает лучшую избирательность по соседнему каналу. Однако существующие правила требуют использования большого числа каналов с псевдослучайной перестройкой частоты для обеспечения равномерной загрузки частотного диапазона.

к.т.н. Г.А. Кучук

МАТЕМАТИЧНА МОДЕЛЬ МЕРЕЖНОГО ТРАФІКА З ВЛАСТИВОСТЯМИ МАСШТАБНОЇ ІНВАРІАНТНОСТІ

Мережний трафік сучасних телекомунікаційних систем досить складно інтерпретувати за допомогою класичних методів статистичного аналізу, характерних для усталених режимів роботи мережних додатків. Тому необхідна розробка адекватних конструктивних математичних моделей мережних процесів, що враховують особливості, які є істотними для цілей дослідження, з метою подальшого використання цих моделей для оптимізації процесу функціонування високошвидкісних комп'ютерних мереж. У доповіді наводиться підхід до розробки такої математичної моделі у випа-

дку, коли аналізований мережний трафік має властивості масштабної інваріантності, що дозволяє застосовувати різні імовірнісні методи для оперативного прогнозування процесів за допомогою мінімальної кількості настроюваних параметрів. Також наведені результати оцінки адекватності запропонованої математичної моделі.

к.т.н. Д.В. Сумцов, О.Ф. Тарасов, к.т.н. А.М. Ткачов

АНАЛИЗ ПОДХОДОВ К СЖАТИЮ ДИНАМИЧЕСКИХ ИЗОБРАЖЕНИЙ

Проведен анализ существующих подходов к сжатию динамических изображений. Было выяснено, что основной процедурой, влияющей на время обработки изображения, является оценка и компенсация движения. Одним из основных недостатков стандартного подхода к анализу движения является необходимость использования значительной вычислительной мощности. В связи с этим сформулированы подходы к разработке высокоэффективных алгоритмов, позволяющих достичь снижения количества операций вычислений. Перспективными являются задачи: выбора наименьшего числа точек, наилучшим образом передающих изменение рельефа детали объекта и анализа движения этой детали только с использованием ее характерных точек; использование корреляционных свойств векторов движения соседних макроблоков; упрощение процедуры сравнения блоков или снижение необходимого числа таких сравнений; адаптация размеров блока к характеристикам изображений.

к.т.н. С.В. Осієвський, к.т.н. О.В. Щербаков, к.т.н. С.В. Алексєєв

АНАЛІЗ МОЖЛИВОСТЕЙ І ХАРАКТЕРИСТИК СПЕЦІАЛІЗОВАНИХ CASE-ЗАСОБІВ ПРОЕКТУВАННЯ БД

Проведено аналіз спеціалізованих CASE-засобів проектування БД: S-Designor фірми Sybase і Oracle Designer/2000 фірми Oracle. Визначено, що вони мають розвинені сервісні і візуальні засоби опису структур БД. Проте аналіз можливостей і характеристик даних систем показав, що їм властиві істотні недоліки. Зокрема, це відсутність засобів оптимізації логічних і фізичних структур БД за різними експлуатаційними критеріями ефективності функціонування інформаційних систем; відсутність засобів оптимізації розміщення БД на пристроях зовнішньої пам'яті, а також розміщення МБД і РБД по вузлах обчислювальної мережі; орієнтація систем на проектування тільки реляційних структур локальних БД і відсутність методів та засобів проектування МБД в архітектурі "Клієнт-Сервер", РБД і ООБД; відсутність засобів оцінки структур БД, що генеруються, при виконанні інформаційно-пошукових процесів – обслуговування запитів користувачів і транзакцій, тобто формовані структури БД не відображають динамічних характеристик предметних областей. Дані системи не містять методів і засобів проектування структур БД за критеріями достовірності і захисту структур даних від несанкціонованого доступу.

В.Ю. Ковтун, И.Е. Кужель, А.М. Гиневский

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ СКАЛЯРНОГО УМНОЖЕНИЯ В АДДИТИВНОЙ ГРУППЕ С ПРЕДВЫЧИСЛЕНИЯМИ

Построение современных информационно-телекоммуникационных систем специального назначения (ИТС СН) немыслимо без подсистемы защиты информации, одним из составных функциональных элементов которой является программно-технический комплекс криптографической защиты преобразований информации (ПТК КЗИ). Возрастающие объемы передаваемой информации, повышение требований к оперативности обслуживания абонентов выдвигают высокие требования к производительности всей ИТС СН, в том числе и к ПТК КЗИ. Как известно, криптографические преобразования с открытым ключом составляют основу ПТК КЗИ и обладают наименьшим быстродействием. На сегодня в Украине в качестве стандарта цифровой подписи используется стандарт ДСТУ 4145-2002, основывающийся на преобразованиях в группе точек эллиптической кривой (ЭК). Таким образом, вопрос повышения быстродействия криптопреобразований на ЭК является актуальным. Операция скалярного умножения базовой точки ЭК (образующей группу большого простого порядка) составляет основу криптопреобразований на ЭК. В работе предлагается уменьшить вычислительную сложность этой операции за счет специальным образом выполненной компоновки результатов предвычислений. Предлагаемая компоновка предвычислений требует увеличения объемов предвычислений в два раза, но позволяет снизить вычислительную сложность операции скалярного умножения на 5,3 %, что в свою очередь позволит на столько же уменьшить вычислительную сложность операций формирования и проверки электронной цифровой подписи.

к.т.н. Н.П. Благодарный, М.А. Калашник

СКОЛЬЗЯЩЕЕ РЕЗЕРВИРОВАНИЕ МОДУЛЕЙ МАТРИЧНЫХ СПЕЦПРОЦЕССОРОВ С ДЕЦЕНТРАЛИЗАЦИЕЙ ФУНКЦИЙ ПЕРЕКЛЮЧАЮЩЕГО УСТРОЙСТВА

Рассматривается решение задачи повышения эффективности скользящего резервирования высокоинтегрированных матричных спецпроцессоров реального времени за счет децентрализации функций переключающего устройства. Приводятся результаты исследований зависимости вероятности безотказной работы распределенного переключателя от степени децентрализации его функций, объема дополнительно вводимого оборудования, размерности матричного спецпроцессора (числа процессорных модулей), запаса временной избыточности при применении спецпроцессора по назначению. Предложена методика определения степени децентрализации переключающего устройства, максимизирующая значение вероятности успешной реконфигурации матричных спецпроцессоров в реальном масштабе времени в условиях жестких ограничений на массогабаритные и динамические характеристики.

В.П. Лысечко, А.С. Жученко, Ю.А. Семеренко

АНСАМБЛЕВЫЕ СВОЙСТВА СЛОЖНЫХ СИГНАЛОВ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С МИНИМАЛЬНЫМ ЭНЕРГЕТИЧЕСКИМ ВЗАИМОДЕЙСТВИЕМ

Рассматривается задача формирования больших ансамблей сложных сигналов для систем радиосвязи с кодовым разделением каналов. Были синтезированы ансамбли сложных сигналов с улучшенными взаимокорреляционными свойствами на основе последовательностей коротких видеоимпульсов с минимальным энергетическим взаимодействием во временной области. Исследования ансамблевых свойств таких сигналов показало, что, применяя разработанные методы формирования, можно синтезировать ансамбли сигналов с улучшенными взаимокорреляционными свойствами (по сравнению с известными сигналами), объем которых существенно превышает аналогичные характеристики известных сигналов.

д.ф.-м.н. В.К. Иванов, к.т.н. Г.А. Кучук, А.С. Васильев

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОБРАБОТКИ РАДИОЛОКАЦИОННЫХ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

В докладе рассматривается схема обработки радиолокационных данных дистанционного зондирования Земли (приема, дальнейшей обработки, архивации и доставки конечному потребителю) посредством широко распространѐнных в данный момент IP-сетей и глобальной сети "ИНТЕРНЕТ". Проводится анализ возможных случаев нарушения нормального функционирования IP-сети при обработке данных в режиме реального времени, которые препятствуют своевременной доставке данных дистанционного зондирования Земли потребителю. Предлагаются возможные механизмы устранения рассмотренных случаев нарушения процесса функционирования посредством модификации существующих алгоритмов и протоколов маршрутизации в IP-сетях.

к.т.н. С.В. Хуторненко, В.Н. Савченко, А.В. Пономаренко

ПАРАМЕТРЫ ЭКВИВАЛЕНТНОЙ ЭЛЕКТРИЧЕСКОЙ СХЕМЫ ПЬЕЗОРЕЗОНАТОРА С МЕЖЭЛЕКТРОДНЫМ ЗАЗОРОМ

На основе полученной математической модели полной проводимости пьезокварцевого резонатора с массонагрузкой (электродом) на одной из поверхностей кристаллического элемента и зазором между второй поверхностью и электродом выведены параметры эквивалентной электрической схемы пьезорезонатора. В качестве эквивалентной электрической схемы использована наиболее распространенная схема Ван-Дейка (ГОСТ 18869-73). Проведено сравнение известных и полученных соотношений для параметров эквивалентной электрической схемы пьезорезонатора.

д.ф.-м.н. В.К. Іванов, к.ф.-м.н. О.О. Можаєв,
к.ф.-м.н. О.М. Стаднік, к.ф.-м.н. С.Є. Яцевіч

ДИСТАНЦІЙНЕ ЗОНДУВАННЯ ЛІСІВ З БОРТУ ЛІТАКА

У доповіді розглянуті питання дистанційного зондування лісних масивів, характерних для сходу України, у широкому частотному діапазоні з борту літака. Наведено ряд електродинамічних моделей, які використовуються у даному випадку багаточастотними поляриметричними та інтерферометричними радіолокаційними станціями. При аналізі характеристик лісних масивів використовується багаточастотна інформація, яка отримана синхронно радіолокаторами бокового огляду літака у діапазоні довжин хвиль від міліметрів до метрів при різній поляризації випромінювання та прийому. Проведена відповідна статистична оцінка та наведено ряд прикладів.

Ю.В. Стасев, А.А. Кузнецов, А.А. Юкальчук

МЕТОД ПОСТРОЕНИЯ ВЫСОКОНЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

Перспективным направлением в развитии теории защиты информации является разработка и исследование методов построения высоконелинейных булевых функций. Их практическое использование позволяет, за счет применения развитого математического аппарата булевой алгебры, конструировать блоки нелинейных подстановок и исследовать основные показатели стойкости синтезируемых криптоалгоритмов. Предлагается метод построения булевых функций с высокими показателями нелинейности, обладающих максимально достижимой алгебраической степенью и удовлетворяющих строгому лавинному критерию. Исследованы свойства функций, построенные в соответствии с предложенным методом.

А.А. Кузнецов, С.П. Евсеев, В.И. Грабчак

КАСКАДНЫЕ КОДОВЫЕ СХЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разрабатываются каскадные кодовые схемы защиты информации для обеспечения достоверности и информационной скрытности передачи данных в АСУВ. Формулируются и доказываются теоремы, которые устанавливают зависимость между параметрами обобщенных каскадных кодов и параметрами построенных на их основе каскадных теоретико-кодовых схем. Выводятся основные аналитические выражения, позволяющие проводить оценку объема служебных (ключевых) данных, размерности входного текста и формируемых кодограмм, относительной скорости передачи данных и других показателей.

А.А. Кузнецов, О.Н. Одарущенко, В.Е. Чевардин

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ МЕТОДОВ КЛЮЧЕВОГО ХЕШИРОВАНИЯ НА ОСНОВЕ АРИФМЕТИКИ АЛГЕБРАИЧЕСКИХ КРИВЫХ

Применение эллиптических кривых в криптографии открыло новые возможности для разработчиков криптографических систем. Это обусловило смену существующих стандартов цифровой подписи, схем аутентификации на основе RSA-преобразований новыми стандартами и методами на эллиптических кривых. В связи с этим появились новые проблемные вопросы интеграции таких криптосистем в стеке протоколов TCP/IP и подключения новых библиотек, содержащих необходимые функции и процедуры, реализующие преобразования над группою точек эллиптической кривой. Предлагается способ применения разработанных методов ключевого итерационного хеширования на основе арифметики алгебраических кривых в стеке протоколов TCP/IP. Представляется сравнительная оценка вычислительных затрат системы при использовании предложенных методов ключевого итерационного хеширования.

к.т.н. А.И. Тимочко

АНАЛИЗ ПРОЦЕССА НЕЧЕТКОГО ВЫВОДА ПРИ ВЫБОРЕ ПАРАМЕТРОВ ПЛАНИРУЕМОГО ПЕРЕХВАТА

Математической моделью описания процесса выбора параметров планируемого перехвата является логико-лингвистическая продукционная модель, в основе функционирования которой лежит операция нечеткого логического вывода. Процесс нечеткого вывода состоит в выполнении: этапа фазификации – учет вклада входного четкого числа в каждое правило логико-лингвистической продукционной модели; этапа нечеткого вывода – вычисление значения истинности для предпосылки каждого правила на основании конкретных нечетких операций, соответствующих конъюнкции или дизъюнкции; этапа композиции – формирование единственного нечеткого выходного множества; этапа дефаззификации – преобразование нечеткого набора значений выводимых лингвистических переменных в точные значения.

д.т.н. В.С. Харченко, А.А. Фурманов

ОБЕСПЕЧЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ И УСТОЙЧИВОСТИ WEB-ПРИЛОЖЕНИЙ ОТ СЕТЕВЫХ АТАК ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ ДИВЕРСНОГО ПОДХОДА

Высокий уровень развития современных технологий обусловлен фактором стремительного увеличения информационных потоков. На сегодняшний день высокая скорость распространения информации является одним из следствий глобализации всемирной сети Интернет и все большей распространѐнности Web-приложений. Следствием стремительного распространения Web-прило-

жений является проблема увеличения сетевых атак, связанная с несовершенством сетевых технологий, не рассчитанных на их использование злоумышленниками. В связи с этим актуальной является задача разработки усовершенствованных архитектур Web-систем с целью обеспечения высоких показателей отказоустойчивости и устойчивости Web-приложений от сетевых атак. Одним из вариантов такого решения является использование принципа диверсности при построении архитектуры системы.

В работе проанализированы виды сетевых атак, проведена их классификация и разработана IMEA-таблица (Intrusion Modes and Effect Analysis). Предложен вариант диверсной архитектуры Web-приложений, которая способна противостоять некоторым видам сетевых атак, а также увеличивать общую отказоустойчивость системы. На основании предложенной архитектуры построена таксономия уровней диверсности и построены матрицы совместимости современных компонент Web-систем. Результатом работы является граф вариантов Web-систем, построенных с использованием предложенной диверсной архитектуры, позволяющий выбирать конфигурацию будущей системы для достижения максимального уровня диверсности системы.

Ю.А. Крыхтин

РЕШЕНИЕ ЗАДАЧИ ОПТИМИЗАЦИИ ПАРАМЕТРОВ БИНАРНОГО СИГНАЛА ПО КРИТЕРИЮ МИНИМУМА РАЗБРОСА АМПЛИТУД ПОЛЕЗНЫХ ГАРМОНИК МЕТОДОМ ПОСЛЕДОВАТЕЛЬНОГО КВАДРАТИЧНОГО ПРОГРАММИРОВАНИЯ

Синтез оптимальных полигармонических сигналов (ПГС) по определенному набору критериев требует решения достаточно сложной задачи оптимизации параметров ПГС. При этом целевые функции в такой постановке, как правило, нелинейные, а процесс нахождения оптимума сопровождается дополнительными ограничениями на переменные или на интегральные показатели ПГС, такие как полезная мощность, среднее значение полезных гармоник и др. Наиболее эффективным (с точки зрения быстроты и сходимости) методом решения такого типа задач является метод последовательного квадратичного программирования. В докладе проводится рассмотрение ряда особенностей данного метода, а именно: конечно-разностная аппроксимация градиента, квазиньютоновское обновление матрицы вторых производных (гессиана) и поддержание ее положительной определенности, стратегия активного набора ограничений, квадратичное программирование и линейный поиск.