дизельных двигателей на буровой, что в свою очередь позволяет прямо и косвенно контролировать технологические процессы бурения, формировать ежедневные отчеты о работе дизельных двигателей на буровой и расходе дизельного топлива без участия мастеров.

Для контроля оборотов двигателя на этих дизелях используются электрические тахометры. Удаленный мониторинг работы дизельного двигателя производится по данным полученным с тахометра. Для измерения сигналов тахометра и передачи данных используется контроллер UAB TELTONIKA FM4200. Он содержит аналоговые входы для измерения напряжения тахометров дизельных двигателей, напряжения в электросети буровой установки (контроль дизель электростанции) и GPRS канал для передачи данных.

FM4200 это терминал с GPS и GSM соединением, который способен распознавать координаты и передавать их используя ресурсы GSM сетей. Прибор имеет входные и выходные параметры, которые позволяют следить и управлять другими приборами объекта.

Использование микроконтроллера более надежно, так как процесс полностью автоматизирован, производится экономия материальных средств за счет сокращения рабочих кадров, существует доступ к данным в любой момент времени, данные передаваемые по GRPS каналу доступны только администратору, не играет роли человеческий фактор, тем самым сводится к нулю риск кражи топлива, риск получения ложных данных, процесс может контролироваться удаленно, а также контроллер отличается низким энергопотреблением.

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ УСТРОЙСТВ ФАПЧ

Д.Л. ШИЛИН, М.В. ПОЧЕБУТ

Разработанная система представляет собой симметрично-поточную криптосистему, в которой шифрование проводится над каждым байтом исходного текста с использованием гаммирования. Источником гамма-последовательности является система фазовой автоподстройки частоты, работающая в режиме детерминированного хаоса. Безопасность системы полностью зависит от свойств генератора потока ключей. Если он реализуется на конечном автомате, последовательность со временем повторится. Практически все генераторы псевдослучайных последовательностей за исключением одноразовых блокнотов являются периодическими. Поэтому, поток ключей должен иметь более длинный период, чем количество битов, выдаваемых между сменой ключей. Генератор должен выдавать одну и ту же гамма-последовательность и для шифрования, и для дешифрирования. Поэтому важным моментом является однократное использование гамма-последовательности, следовательно, необходима синхронизация передающего и принимающего устройств. Для этих целей предлагается использовать самосинхронизирующееся потоковое шифрование. Так как внутреннее состояние генератора потока ключей является функцией предыдущих N битов шифротекста, то расшифрующий генератор потока ключей, приняв N битов, автоматически синхронизируется с шифрующим генератором. Последовательности чисел, получаемые при помощи генератора на основе устройства фазовой автоподстройки частоты, работающем в режиме детерминированного хаоса, были протестированы на случайность.

Были использованы статистические NIST, DIEHARD. Также тестирование проводилось по критериям сериальной корреляции, частот, интервалов, серий.

В исследовании использовались выборки объемом до 400000 бит. При рассмотрении массива ключей большего объема наблюдалась периодичность выпадения значений.

БЕЗОПАСНОЕ ПРЕРЫВАНИЕ ПРОЦЕДУР МЕТОДА ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ

М.П. РЕВОТЮК, М.К. КАРОЛИ

Процедуры метода динамического программирования, базирующиеся на использовании принципа последовательной декомпозиции задачи, пригодны для естественного распараллеливания на вычислительных сетях. Управление потоками порождаемых подзадач при нерегламентированном режиме доступности рабочих станций на сети общего назначения порождают необходимость надежного решения проблемы грануляции и синхронизации подзадач с гарантией решения исходной задачи. Предмет рассмотрения — способ представления в произвольный момент состояния процесса решения задачи с целью последующего восстановления состояния и продолжения процесса решения на любом доступном узле сети.

Ключевой элемент инварианта представления состояния процесса решения задачи определяется алгоритмом порождения дерева вариантов. Такой алгоритм часто допускает свободу перечисления ветвей дерева, что предлагается использовать для встраивания процедур сохранения и восстановления состояния. Например, цель решения известной задачи коммивояжера — поиск гамильтонова цикла минимальной длины. Рекурсия обхода дерева подзадач здесь реализуется генератором перестановок с мемоизацией состояния.

Предлагается вариант генерации перестановок с минимальным изменением. Набор переменных состояния процесса ветвления, следуя схеме динамического программирования, определяется вектором текущей перестановки. Установлено, что ветвление на любом уровне возможно с сохранением порядка следования элементов перестановок. Глубина ветвления не превосходит значения, поэтому активные ветви дерева порождаемы из вектора состояния генератора перестановок. Отсюда следует, что для возобновления поиска решения после прерывания требуется память объемом, включающая вектор перестановки лучшего гамильтонова цикла, вектор представления вершин пути от корня дерева до листьев и вектор позиций ветвей дерева.

БЕЗОПАСНОЕ ПРЕРЫВАНИЕ ПРОЦЕДУР МЕТОДА ВЕТВЕЙ И ГРАНИЦ

М.П. РЕВОТЮК, П.М. БАТУРА, Р. ХОРМОЗИ

Предмет рассмотрения — способ компактного представления в произвольный момент состояния задачи, решаемой методом ветвей и границ с распараллеливанием, для последующего восстановления состояния и продолжения процесса решения на любом доступном узле вычислительной сети.

В любой момент времени на дереве вариантов можно выделить путь от его корня к листу. Это путь обычно представлен неявно стеком локальных переменных рекурсивно вызываемых функций анализа отдельного узла. Возможность выделения пути от его корня дерева к листу в произвольный момент прерывания появится лишь после дополнения переменных состояния указателем на их предыдущий экземпляр. Предлагается такое дополнение оформить объектом класса в рамках объектных технологий, автоматизируя функциональное замыкание