размещения серверов сервисов, множество мест размещения порталов и матрица пропускной способности; известна производительность серверов и объем трафика каждого из порталов на каждом интервале времени; необходимо выбрать подмножество мест размещения серверов сервисов с назначением приоритета обслуживания порталов при условии баланса производительности и объема трафика. Рассматриваемая задача может быть решена перебором с отсечениями среди множества классических задач Хичкока для всех сочетаний узлов размещения серверов сервисов среди возможных мест на каждом интервале времени. Порождение сочетаний методом вращающейся двери с единичным расстоянием Хэмминга между соседними сочетаниями позволяет заменить полный цикл решения очередной транспортной задачи анализом последствий изменения единственной строки матрицы предыдущей задачи. Используя метод потенциалов[1], удается снизить на порядок вычислительную сложность такого анализа на порядок, а также досрочно прерывать решение задачи для бесперспективного варианта размещения.

Литература

1. Ревотюк, М.П. Реоптимизация решения транспортных задач Хичкока методом потенциалов / М.П. Ревотюк, П.М. Батура, А.М. Полоневич // Доклады БГУИР. – 2010. – № 7(53). – С. 89–96.

АЛГОРИТМЫ КООРДИНАЦИИ СИСТЕМ АГЕНТОВ

М.П. Ревотюк, А.К. Пушкина

Задачи оптимизации управления системами взаимодействующих агентов в общем случае формулируются в терминах задач о динамическом назначении[1]. В процессе координации таких систем необходимо регулярно решать задачу о назначении свободным агентам возникающих задач с учетом реальных ограничений и возможной коррекции плана назначения с учетом текущего состояния. Традиционно задачи координации агентов сводятся к известным задачам дискретной оптимизации, таким как линейная задача о назначении или задача нескольких странствующих коммивояжеров. Однако необходимость учета реальных отношений между агентами и задачами приводит к экспоненциальной сложности алгоритма формирования оптимального назначения и часто делает их практически не реализуемыми.

Предлагается учесть дискретность процесса формирования портфеля заявок, явно используя понятия наиболее раннего и позднего срока начала решения задачи для жадного упреждающего поиска окончательного назначения. Так как процедура назначения дополняет граф оптимального паросочетания при поступлении новых заявок, то задержка времени определяется сложностью обработки последней группы заявок. Реализация предлагаемой схемы возможна на рекуррентных сетевых моделях, состояние которых соответствует графу текущего паросочетания с выделением оптимального решения. Переход между состояниями сети реализуется инкрементальными версиями алгоритмов решения линейных задач о назначении, задачи коммивояжера и поиска кратчайших путей на графах. На параметры таких задач проецируются особенности процессов обслуживания, включая векторные критерии и разнообразные отношения вложенности.

Литература

1. A Comprehensive Taxonomy for Multi-Robot Task Allocation/G.A. Korsah, M.B. Dias, A. Stentz [Electronic resource]. – Mode of access: http://ashesi.org/wp-content/uploads/2016/03/G.-Ayorkor-Korsah.pdf. – Date of access: 24.02.2016.

СИСТЕМА ЗАЩИТЫ ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ МИКРОКОМПЬЮТЕРА RASPBERRY PI

О.Ю. Рыжко, С.А. Зайкова

На сегодняшний день автоматизированные системы являются основой обеспечения большинства бизнес-процессов, как в коммерческих, так и в государственных организациях. Вместе с тем, повсеместное использование автоматизированных систем для хранения, обработки и передачи информации приводит к обострению проблем, связанных с их защитой. Считается, что одной из наиболее опасных угроз является утечка хранящейся и обрабатываемой внутри автоматизированной системы конфиденциальной информации. Все это обуславливает необходимость пристального рассмотрения эффективных способов защиты от

утечки конфиденциальной и корпоративной информации. Защита требует комплексного подхода и учета всех возможных коммуникационных каналов, обеспечение физической безопасности, шифрование резервных копий и информации, покидающей периметр, а также ряда организационных мероприятий. В работе предложено разработать программный модуль анализа сетевого трафика и, таким образом, модифицировать комплексную защиту системы, ее информационную безопасность, предотвратить несанкционированное распространение конфиденциальной информации (на примере филиала ООО "ЮНЛ Солюшнс" г.Гродно). Решены следующие задачи: изучены основные понятия систем предотвращения утечки информации; проанализированы методы анализа информации на предмет содержания конфиденциальных данных; разработан программный модуль анализа информации на языке программирования Ruby; разработана веб-панель управления (с использованием фреймворка Ruby on Rails); развернута система на базе микрокомпьютера Raspberry Pi; проанализирована эффективность программно-аппаратного модуля; даны рекомендации по поддержке, развитию и оптимизации системы защиты от утечек конфиденциальной информации.

Литература

1. Ищейнов, В Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учеб. пособие / В. Ищейнов, М. Мецатунян. – М.: Высшее образование, 2014. – 256 с.

2. Росенко, А Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование / А. Росенко. – Красанд, 2010. – 160 с.

РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ДЛЯ ИСПОЛЬЗОВАНИЯ СТЕГАНОКОНТЕЙНЕРОВ В АУДИОФАЙЛАХ

И.А. Сазановец

В докладе представлены исследования автора, отражающие возможности передачи скрытых данных в аудиофайлах, возможность модификации аудосигнала, а также передачи скрытых данных в текстовых компонентах аудиофайла. Стеганография в звуковых файлах может применяться для внедрения цифровых отпечатков, водяных знаков и как инструмент скрытой передачи данных. Все звуковые файлы можно рассматривать во временной или же в частотной области. Для перехода из временной в частотную область используется дискретное преобразование Фурье.

Во временной плоскости работают методы наименьшего значащего бита и кодирования с помощью бита четности. В частотной плоскости работают методы фазового кодирования, эхо кодирования, кодирования с помощью расширения спектра и кодирования с помощью высокочастотного шума.

Методы, работающие в частотной области, не позволяют скрыть большой объем информации, поэтому они больше подходят для внедрения цифровых отпечатков или водяных знаков. Метод наименьшего значащего бита позволяет скрыть значительно больше информации, но при его реализации могут наблюдаться следующие уязвимости: запись бит в промежутки тишины (в звуковых файлах тишина кодируется нулями), левый и правый каналы в стереофайле могут быть побитно одинаковыми и отсутствие шифрования (кроме того, что исходное сообщение шифруется, шифрование усложняет стеганоанализ). Также метод наименьшего значащего бита подвержен статистическому анализу. Также в докладе представлены методы сокрытия данных в метаинформации звуковых контейнеров.

СРАВНЕНИЕ СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ СТБ 34.101.45-2013 С РАЗДЕЛЕННЫМ СЕКРЕТОМ ПРИ ИСПОЛЬЗОВАНИИ АЛГОРИТМОВ ХЭШИРОВАНИЯ SHA-2 И SHA-3

С.Б. Саломатин, О.А. Селеня

Использование электронно-цифровой подписи для защиты электронного документооборота предполагает надежность всех алгоритмов в ее составе. В основе любой цифровой подписи лежит алгоритм хэширования для обеспечения существенного изменения конечного значения подписи если подписанный документ при передаче подвергся даже