

- разработка теоретических основ регуляризации распределённых вычислений, методов декомпозиции процессов обработки информации и восстановления информации в условиях критических воздействий на систему;
- поиск эффективных алгоритмов обеспечения конфиденциальности, целостности и доступности информации в условиях разрушения части средств обработки, передачи и хранения информации;
- формирование методологии оценки качества обрабатываемой информации и достигнутой степени устойчивости процесса обработки информации.

Методической основой решения перечисленных задач видятся, прежде всего, теоретико-информационные и теоретико-сложностные подходы, сформированные в рамках современной теории защиты информации; разработка методов представления информации и эффективных алгоритмов её обработки неразрывно связана с алгебраическими методами.

**А.А. Зотов**

Россия, г. Москва, МИФИ

### **БЕЗОПАСНОСТЬ И НАДЕЖНОСТЬ СЕТИ ИНТЕРНЕТ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ**

Всемирная сеть Интернет появившаяся в начале 90-х, сегодня является неотъемлемой частью нашей жизни. Сегодня Интернет это и местом для отдыха и местом где компании зарабатывают деньги. Услугами Интернет на сегодняшний день пользуется десятки тысяч компаний. Степень вовлеченности компаний в Интернет различна. Некоторые компании используют Интернет в качестве справочника, а некоторые компании на 100% связывают свой бизнес с Интернет.

Давайте попытаемся понять, почему Интернет получил такое широкое распространение. Основными критериями являются простота его использования и анонимность. Любой человек без проблем может купить модем, карточку и воспользоваться услугами провайдера для получения доступа в Интернет. Но основное преимущество Интернет является и его основной слабостью. Интернет это анонимная среда, в которой каждый может делать все, что ему захочется.

Бесконечные вирусы, черви, приносящие большой урон компания заставляя задуматься о будущем Интернет. В газете Ведомости от 20 января 2003 года была опубликована статья под заголовком “Интернету осталось недолго”. Автор этой статьи приводит статистику: “По оценкам российской антивирусной компании “Лаборатория Касперского”, объем коммерческого ущерба от вредоносных программ в 2002 г. составил \$14,5 млрд, что на 10% больше, чем в 2001 г.” Он также говорит о том, что на сегодняшний день злоумышленники обладают достаточными средствами для разработки сетевых вирусов технологии DOS (отказ в обслуживании), которые смогут парализовать работу Интернет. Автор статьи приводит высказывание Евгения Касперского, руководителя антивирусных исследований “Лаборатории Касперского”: “Современный Интернет находится на завершающей стадии своего жизненного цикла, еще немного - и он просто умрет”.

Суть последнего высказывания можно трактовать не то, что Интернет исчезнет, а то, что он прекратит существовать в том виде, в котором он существует сейчас. Краткий анализ мировых тенденций развития Интернет, позволяет обнаружить проект GIP. GIP – это проект развития Интернет. Основные тенденции развития заключаются в обеспечении повсеместного доступа и создании доверенной среды передачи информации.

Повсеместный доступ будет обеспечиваться с помощью современных технологий (в частности технологий беспроводного доступа).

Для создания доверенной среды, предполагается создать систему глобальной аутентификации пользователей и систему шифрования передаваемой информации.

**С.Д. Кулик**

Россия, г. Москва, МИФИ

### **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АФИПС**

Автоматизированные фактографические информационно - поисковые системы (АФИПС) [1,2] содержат в своем составе фактографическую базу данных (ФБД), поискового робота (ПР) и человека-оператора (ЧОП) [2]. Эта ФБД может быть подвергнута атаке хакером или вирусом. В результате такой атаки ФБД может содержать искаженные фактографические данные (ФД). Для ФБД были разработаны специальные средства защиты [1] от возможных разрушений, а также средства компенсации влияния различного вида ошибок на конечные результаты фактографического поиска (ФП) в АФИПС путем выбора соответствующих стратегий ФП и их параметров. Иногда эта защита [1] может с успехом противостоять несанкционированным действиям мошенника. Для этого в ФБД вводится некоторая избыточность (например, в области поиска из  $N$  объектов содержится  $M < N$  дублей тождественных запросу объектов) и применяются необходимые алгоритмы распознавания образов (РО). От качества проектирования системы РО зависит и качество проектирование самой АФИПС. Для создания АФИПС с заданными характеристиками, как правило, необходимо иметь модель системы. В результате проведенных исследований была разработана и экспериментально проверена аналитическая модель поискового робота в АФИПС. В модели ПР учитывается ЧОП и алгоритм РО для сравнения описаний объектов при поиске. Этот алгоритм учитывает искажения в ФД, хранящихся в ФБД.

**О.О. Варламов, М.Р. Амарян, В.А. Лысаковский, Л.Е. Адамова**

Россия, г. Москва, ОАО «ЦЕНТРТЕЛЕКОМ»

### **ОСОБЕННОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИИ В АСУ РЕГИОНАЛЬНОГО ОПЕРАТОРА СВЯЗИ**

В докладе показаны особенности защиты информации в компьютерах и рабочих станциях автоматизированной системы управления регионального оператора связи, на примере ОАО "ЦентрТелеком".

Компания электросвязи по роду своей деятельности работает с конфиденциальной информацией, касающейся отдельных граждан или организаций. Принцип защиты персональных данных физических и юридических лиц является одним из важнейших принципов функционирования компании на всех уровнях системы. Причем защита данных должна обеспечиваться как при передаче конфиденциальных данных, так и при их обработке и хранении в автоматизированной системе управления связи (АСУС) регионального оператора электросвязи.

Так как эффективность функционирования любой телекоммуникационной компании сегодня во многом определяется максимальным использованием современных информационных технологий, то внедрение новых технологий является обязательным для развития АСУС. Кроме того, необходимо своевременно разрабатывать и внедрять в АСУС новые и перспективные методы, средства и устрой-