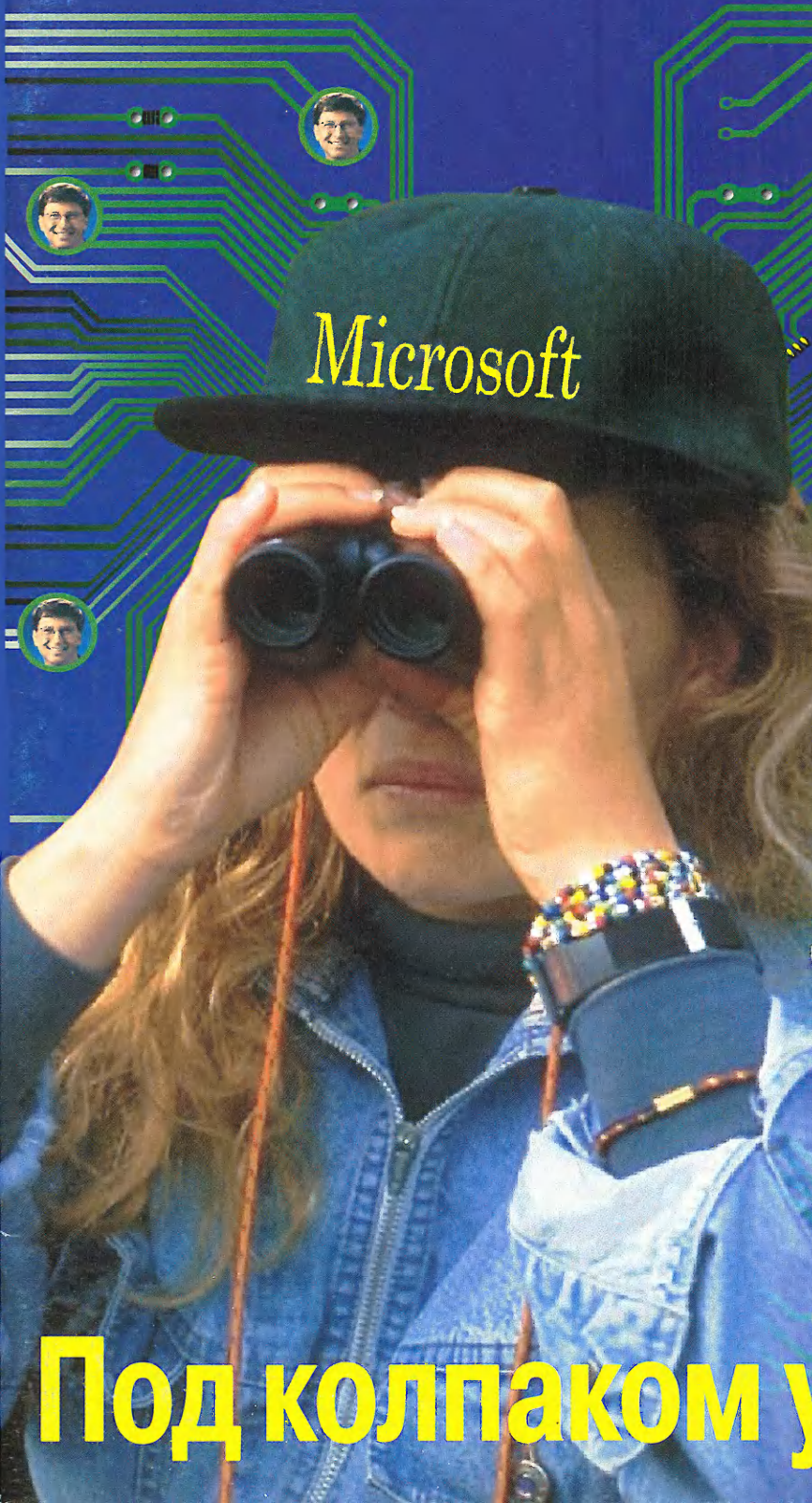
ПРЕСС ТехнО

Журнал для пользователей ПК

№ 10 / октябрь '98

магия ПК



Интеллект... искусственный?

Исповедь вирмейкера

Спецслужбы в Интернет

Электронная тайнопись

Кевин Митник, человек-легенда

Компьютер — композиторам

Под колпаком у Microsoft

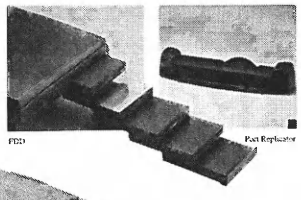
ПРЕСС ТЕХНО

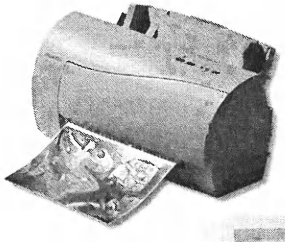
Журнал для пользователей ПК

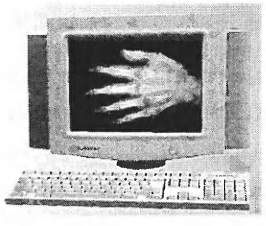
№ 10/октябрь '98

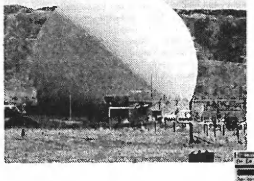
магия ПК

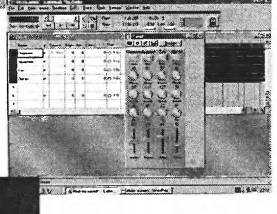
Содержание











КОМПЬЮТЕРЫ

Интеллект... искусственный? А что, нам нравится! 2
Транзистор — продукт внеземной технологии? 6
Ответ Гамлету: 3D or not 3D? 9
FAT32 — дисковое пространство без проблем 11
Между ценой и престижем 13
Ноутбуки Chicony: расширение без ограничений 14
Ethernet против Token Ring 16

ОРГТЕХНИКА И ПЕРИФЕРИЯ

На чем печатать фотографии 18

НАЧИНАЮЩИМ

Сам себе доктор 21
Исповедь вирмейкера 22

ВАШЕ ЗДОРОВЬЕ

Болезнь ювелиров 25
Минздрав предупреждал 26

HOMO COMPUTERUS

Кевин Митник, человек-легенда 28

ИНТЕРНЕТ

Поиск работы в Интернет 31
Спецслужбы в Интернет 33

БДИ!

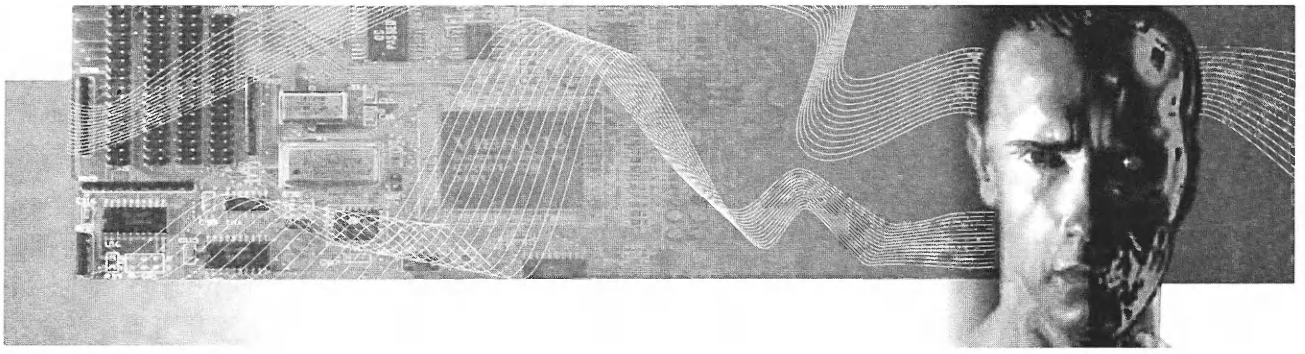
Электронная почта и перехват информации 36
Электронная тайнопись 40
Под колпаком у Microsoft 43
Безопасность информации при радиосвязи 45
Шлюзы безопасного бизнеса в Интернет 46

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Кому нужна Windows'98? 49
Опять девяносто пять! 50
Компьютер — композиторам 52

МУЛЬТИМЕДИА

Тибериумное солнышко 55



Интеллект... искусственный? А что, нам нравится!

Владимир Буслаев

И в процессе вычислений создается впечатление, что цифры оживают и творят ...

Немного истории

Проблема искусственного интеллекта всегда привлекала внимание не только исследователей, но и писателей-фантастов. Многие энтузиасты стремились создать "думающие" машины, которые справлялись бы с поставленными задачами так же успешно, как и люди.

Первоначально и очень долгое время развитие систем искусственного интеллекта ассоциировалось с созданием устройств, являющихся механическим подобием человека. Более двух тысяч лет назад Герон Александрийский в "Трактате о пневматике" описал ряд автоматов, которые представляли собой движущиеся фигуры и поющих птиц. Примерно в 1500 г. Леонардо да Винчи построил для Людовика XII механического льва, который при въезде короля выдвигался и, раздирая когтями грудь, обнажал герб Франции. В конечном счете (с изобретением в начале 50-х годов нашего века механического манипулятора) создание автоматов, которые двигались бы подобно людям или животным, превратилось в одно из направлений современной кибернетики — робототехнику.

В XVII веке Паскаль и Лейбниц создали системы, которые нельзя назвать роботами, но которые стали следующим шагом к созданию искусственного интеллекта — первые механические вычислительные машины.

После появления первой ЭВМ (уже в середине нашего века) неоднократно предпринимались попытки конкретизировать задачу создания "думающих" машин, а также выработать концепцию их построения. Однако, несмотря на все усилия, перевести эту проблему в практическую область долгое время не удавалось.

Термин "искусственный интеллект" предложил Джон Маккарти летом 1956 года (позднее он основал две ведущие в мире лаборатории в области исследований искусственного интеллекта). Понятие искусственного интеллекта как научного направления сформировалось в 60—70-е годы в общем комплексе кибернетических исследований. Мощным толчком к возникновению этого направления послужило бурное развитие средств вычислительной техники и расширение областей применения ЭВМ.

Ах, интеллект, интеллект...

Несмотря на то, что история исследований в области искусственного интеллекта насчитывает к настоящему времени уже несколько десятилетий, единого общепризнанного определения этого понятия еще не существует. Это прежде всего связано с тем, что данная область знаний достаточно молодое и все еще бурно развивающееся направление мировой науки. Тем не менее, достаточно полно существо этого понятия раскрывается в следующих трактовках.

В широком смысле слова искусственный интеллект — научное направление, в рамках которого ставятся и решаются задачи аппаратного или программного планирования тех видов человеческой деятельности, которые традиционно считаются интеллектуальными (или разумными, творческими). В узком смысле это программная или аппаратная система, имитирующая на компьютере мышление человека и опирающаяся

на знания, которые хранятся в памяти системы.

Вообще же к сфере искусственного интеллекта относятся те весьма различные области, в которых человек действует, не имея абсолютно точного метода решения проблемы.

Еще в 1971 году крупнейший специалист по искусственному интеллекту Н. Нильсон написал: "Моя точка зрения состоит в том, что искусственный интеллект представляет собой (или будет представлять) инженерную дисциплину, поскольку его первоначальной целью является создание конструкций". Он, прежде всего, имел в виду создание интеллектуальных роботов.

Долгие годы системы искусственного интеллекта находились в тени из-за большой сложности, высокой стоимости и невостребованности рынком. Однако в последнее время положение в этой области существенным образом изменилось — системы вплотную приблизились к потребностям науки и промышленности.

Основные классы систем

К настоящему времени сформировалось несколько основных направлений разработки систем искусственного интеллекта, в рамках которых исследования доведены до практических результатов.

Не претендуя на исключительную полноту и учитывая, что число систем искусственного интеллекта и сфер их применения постоянно растет, рассмотрим основные классы...

1. Системы, имитирующие действия человека при решении различного рода задач.

В данном направлении под термином "решение задач" понимаются методы поиска таких решений. Использование опыта и знаний человека позволяет говорить о возможности применения не алгоритмических, а эвристических методов решения задач, число шагов в которых определяется неявным образом с учетом полученных промежуточных результатов.

Одним из механизмов поиска решений в этих системах может быть метод проб и ошибок. При таком подходе задачи решаются посредством поиска в некотором пространстве возможных решений. Значительным событием в данном направлении стало создание в 1959 году Ньюэллом, Шоу и Саймоном "универсального решателя" задач, который оперирует с задачей примерно так же, как и человек.

На сегодняшний день достижения в этой области носят ограниченный характер.

2. Системы восприятия и адекватной оценки окружающей среды.

К этому классу в первую очередь относятся системы распознавания образов. Хотя они и получили наиболее широкое распространение, в последнее время испытывают "второе рождение".

В общем виде модель распознавания образов можно представить в виде трех взаимодействующих элементов: датчика, устройства выделения признаков (рецептора) и классификатора (идентификатора).

Датчик воспринимает воздействия внешней среды (например, акустические сигналы) и преобразует их в вид, удобный для машинной обработки. Основную трудность при восприятии составляет огромное число возможных описаний-кандидатов, которые в дальнейшем могут представлять интерес для системы. Далее рецептор по заранее заданным признакам производит отбор информации, а классификатор — идентификацию данных.

Неотъемлемой частью таких систем, обеспечивающих "понимание увиденного или услышанного" является наличие "серьезной" базы знаний, предназначенной, в первую очередь, для обработки сложных наборов входных данных.

Наиболее развитыми в настоящее время являются системы, обеспечивающие восприятие и классификацию зрительных образов. Однако такие системы "машинного зрения", как правило, являются частью другой, более общей системы, взаимодействующей с внешней средой.

3. Системы, обеспечивающие общение на естественном языке.

В конце 60-х годов в исследованиях по искусственному интеллекту сформировалось самостоятельное направление, связанное с разработкой методов и систем, реализующих процесс общения пользователей (речь идет о так называемых неподготовленных пользователях) с ЭВМ на естественном языке. Для интерпретации текста такие средства используют комбинацию синтаксиса, структурных особенностей языка и семантики.

Системы искусственного интеллекта, позволяющие общаться, находят применение в медицине, в системах юридической консультации, при обработке различного рода текстовой документации. Такие системы обеспечивают восприятие запросов пользователей на "живом" языке (например, "Что будет, если..." и т. п.) и готовят ответную информацию, а могут использоваться как интерфейсы естественного языка для предварительной обработки данных.

4. Экспертные системы.

Такие системы и инструментальные средства их разработки — наиболее многочисленный и широко используемый класс систем искусственного интеллекта.

Экспертная система представляет собой программное обеспечение, предназначенное для решения

определенного круга конкретных задач из некоторой прикладной области. Причем алгоритм их решения подобен действиям эксперта в этой сфере. Такая система включает в себя базу знаний с набором фактов в интересующей области, набор правил для выработки суждений и механизм вывода суждений.

Самостоятельным и обширным направлением в этом классе являются системы автоматического (визуального) программирования.

Огромный интерес к экспертным системам вызван следующими причинами:

- ориентация на решение достаточно широкого круга задач в неформализованных областях, на приложения, которые еще совсем недавно считались недоступными для вычислительной техники;
- предоставление специалистам, не знающим программирования, таких возможностей, которые позволят самостоятельно разрабатывать интересующие приложения;
- обеспечение экспертными системами таких возможностей при решении практических задач, которые сравнимы, а иногда и превосходят возможности самих экспертов.

Кроме того, следует отметить, что в экспертных системах большинство важнейших достижений искусственного интеллекта были удачно объединены в одну целостную систему, способную решать не модельные, а вполне настоящие, реальные задачи.

Многие экспертные системы с успехом применяются в клиниках — ставят диагноз по многочисленным заболеваниям внутренних органов человека. Экспертная система-химик в течение многих лет интенсивно используется во всем мире, помогая устанавливать структуры сложных высокомолекулярных соединений. С помощью экспертной геологической системы в США было открыто точное местоположение запасов молибдена, оцениваемых в 100 млн долларов. А ведь существуют еще экспертные системы в биологии, математике, финансовые и юридические системы, — сейчас уже трудно указать области, в которых возможности экспертных систем не были опробованы!

5. Системы извлечения полезной информации.

Данный класс систем искусственного интеллекта предназначен для целенаправленного поиска и отбора необходимой пользователю информации из больших массивов неструктурированных данных.

Такие системы появились сравнительно недавно, но уже нашли широкое применение — они позволяют выявить корреляцию между различными атрибутами элементов в базах данных, оценить вероятность появления тех или иных ситуаций (например, тенденций на финансовом рынке и т.п.).

Разновидностью систем данного класса являются системы, предназначенные для автоматического построения связных информационных материалов на заданную тему из фрагментов исходных текстов. Представьте, уважаемый читатель, ситуацию: вы решили написать книгу или обзор (например, в наш журнал). Имея под рукой такую систему и ворох текстов по выбранной тематике, это станет делом каких-то нескольких часов. Останется только добавить название и фамилию автора...

Для фискальных и налоговых органов интересной сферой применения систем интерпретации и анализа данных (отыскание в базе данных зависимостей, в том числе и многофакторных) может стать возможность выявления подлогов.

Можно привести в качестве примеров еще массу самых разных систем искусственного интеллекта, применяемых в управлении, промышленности, образовании, медицине и других областях, однако и в этом случае список будет неполным.

Теперь и у нас

До массового внедрения на российском рынке систем искусственного интеллекта пока далеко, но уже сейчас наметились направления их наиболее перспективного применения:

- системы контроля и управления позволяют отслеживать, например, состояние производственного процесса и эффективно управлять им;
- диагностические системы предназначены для обнаружения и идентификации определенных состояний контролируемого объекта, например, для обнаружения неисправностей электронного оборудования, сбоя работы конвейера в промышленном производстве, диагностики состояния пациента и т.п. Уже созданы отечественные экспертные системы диагностики наследственных заболеваний, технического состояния оборудования и некоторые другие;
- системы интерпретации и анализа данных выявляют взаимосвязь между значительными объемами данных, представленными в электронном виде. Например, система ГИПЕРФОЛИО выделяет из текстового материала существенную для пользователя информацию с учетом его потребности, выраженной в виде списка текстовых формулировок (понятий, определений, задач, проблем и т. п.);
- системы анализа и планирования (прогнозирования), как правило, ориентированы на информационную поддержку принятия решений в политической или внешнеэкономической области, анализ и обоснование инвестиционных проектов, комплексную оценку финансового состояния предприятия и тенденции его дальнейшего развития. Уже созданы система финансового анализа и разработки бизнес-планов "ТЭО-ИНВЕСТ" (Институт проблем управления РАН) и одноименный комплекс программных продуктов для финансистов, аналитиков и консультантов (фирма "Альт");
- системы обработки визуальной информации находят широкое применение в геологии, при анализе состояния окружающей среды, климата, картографии, в метеорологии, гидрологии, океанографии и т. п.;
- системы распознавания образов используются во многих практических областях, начиная от комплексов военного назначения до приложений, связанных с мультимедиа и с машинной графикой (разновидностью таких систем являются системы машинного перевода);
- системы проектирования охватывают разработку как отдельных элементарных устройств, так и целых промышленных комплексов, автоматизированных систем управления и обеспечивают оценку (управление) качеством проектирования.

Большинство систем, построенных на использовании элементов искусственного интеллекта, работают в среде Windows 3.1 (3.11) или Windows'95 на ПК от 486 до Pentium, с оперативной памятью, как правило, не менее 16 Мб.

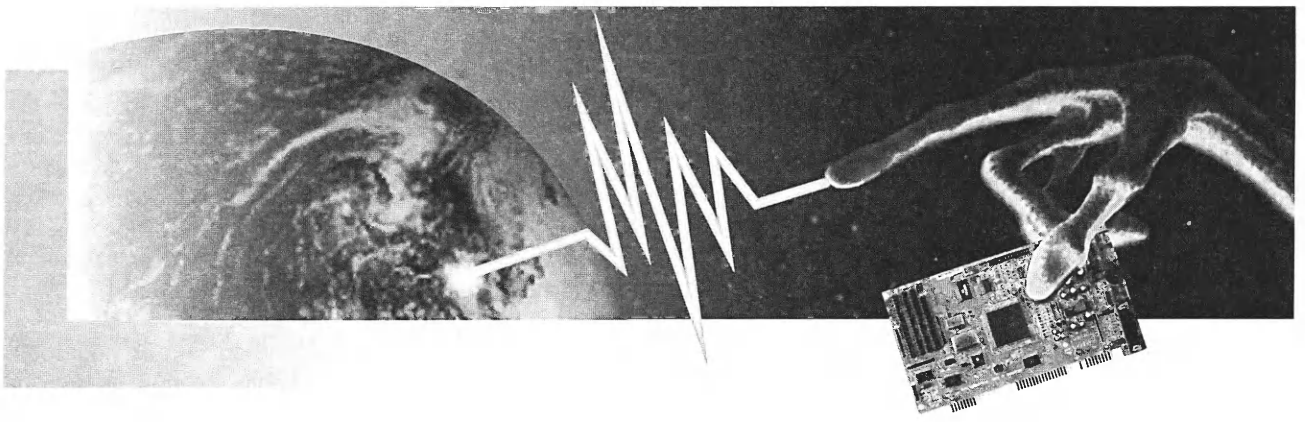
Цены на упомянутые комплексы программ составляют примерно от 500 до 1000—1500$, при этом стоимость сетевых версий, как правило, на порядок выше. Основными разработчиками таких систем являются зарубежные компании, а среди отечественных — московские (в основном) и петербургские компьютерные фирмы.

Подводя итог

Существующие интеллектуальные системы в подавляющем большинстве ориентированы на промышленное производство, банковское дело, финансы, то есть далеки от интересов домашнего пользователя. Да и в этих секторах российского рынка говорить о массовом их использовании пока преждевременно, хотя прецеденты есть, и количество фирм, разрабатывающих и использующих такие системы, постоянно растет.

Прорыв интеллектуальных систем в сектор домашнего применения, скорее всего, произойдет в направлении использования компьютерных систем для управления домашними электронными приборами, а также повышения уровня "интеллектуальности" самих этих устройств.

Хотите верьте, хотите нет



Алексей Богдановский

Транзистор — продукт внеземной технологии?

Сенсационное заявление сделал глава компании American Computer Джек Шульман: транзистор был скопирован фирмой Bell Systems с обломков НЛО, разбившегося в Розуэлле (шт. Нью-Мексико) в 1947 году. Если эта история окажется истиной, то на компьютеры мы будем теперь смотреть совсем другими глазами!

Знаменитый фильм о вскрытии инопланетянина (показанный и в нашей стране), книга военного физика Стентона Фридмана "Crash at Corona" и куча прочей бумажной, аудио- и видеопродукции — все это побочные продукты главной загадки американского континента, так и не разрешенной в течение пятидесяти лет.

Действительно ли в штате Нью-Мексико, в местечке Корона, потерпел аварию неопознанный летающий объект? Действительно ли обломки иноземного корабля были собраны персоналом базы ВВС США в Розуэлле и скрываются до сих пор в ангарах так называемой "Зоны-51"?

Очередной шаг в споре сделали американские компьютерщики.

В начале года Джек Шульман, глава весьма процветающей фирмы, специализирующейся на поставках мэйнфреймов, анонсировал выпуск полупроводникового устройства под названием транспозитор (transpasitor, или TCAP, — производное от transfer capasitor). Транспозитор — следующий шаг в полупроводниковой технике, "переходная емкость", названный по аналогии с транзистором (transfer resistor —"переходное сопротивление"). По словам Шульмана, прибор использует изотропное кристаллическое вещество, обладающее свойством бистабильного резонанса и возможностью квантового хранения информации. Принцип работы транспозитора не совсем ясен и находится на грани опровержения фундаментальных законов физики.

Шульман заявил, что на основе транспозитора уже созданы опытные образцы микросхем памяти емкостью до 2 терабайт. И добавил фразу, от которой у всех уфологов мира волосы встали дыбом: в American Computer попали отчеты компании Bell, касающиеся изучения обломков НЛО, разбившегося в Розуэлле в 1947 году — в них и были найдены эскизы транспозитора!

Все это сильно смахивало на первоапрельскую шутку, но пресс-конференция Шульмана проходила совсем не первого апреля. Кроме того, ни повышенного интереса к летающим тарелкам, ни страсти к розыгрышам American Computer раньше не проявляла.

Чуть позже на сайте American Computer появилась страничка "Розуэлл" (http://www.accpc.com/roswell.htm). Там написаны вещи еще более шокирующие: фирма Bell Systems скопировала транзистор с обломков НЛО, разбившегося в Розуэлле в 1947 году!

Дело было так.

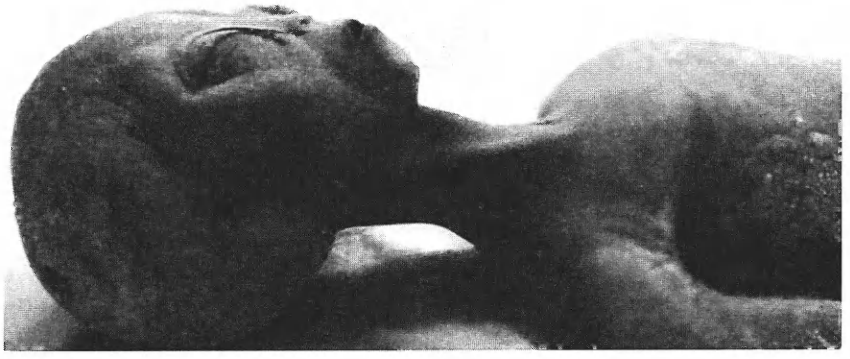
НЛО разбился в районе Розуэлла недалеко от базы ВВС США в июле 1947 года. Отчеты, составленные командованием базы, оказались рассекреченными, потому что были неосмотрительно переданы сотрудникам отдела по связям с общественностью. Появились репортажи, заявляющие, что трупы погибших пришельцев были вскрыты Surgeon General's office и что вскрытие было заснято на кинопленку (а фильм помещен в Национальный военный архив).

Позже начала всплывать история о том, что ВВС США делали с упавшим инопланетным кораблем в августе—октябре 1947 года. Ядерные силовые установки, продвинутые коммуникации и компьютерные устройства, опережавшие на сотни лет технологии II мировой войны, были сняты с обломков НЛО и отправлены для изучения в лабораторию Bell Systems. Там их подвергли микроанализам и эвристическим тестам. Видимо, в ходе тестирования было установлено, что переключающие устройства с уникальными электрическими характеристиками сделаны из кремния и мышьяка, уложенных в микроскопические корпуса.

Исследователи Bell и Министерства обороны США выяснили, что необычные устройства могли вести себя и как высокоскоростные электронные переключатели, и как усилители. Они решили назвать это устройство транзистором (transfer resistor), потому что оно могло изменять сопротивление в зависимости от величины приложенного к нему тока, то есть усиливать ток.

Выяснилось также, что упрощенные варианты инопланетных установок можно изготовить, если немного усовершенствовать существующие технологии. Тогда президент Трумен приказал изготовить "копии" устройства и засекретить всю историю.

Ходят слухи, что в 1947—1949 годах в горах неподалеку от Мюррей Хиллз, где располагались лаборатории Bell Systems, ВВС США спешно возвели противовоздушную батарею, усиленную противоракетными системами, опасаясь отнюдь не атак со стороны Советского Союза, а чтобы защитить лабораторию от космического вторжения. Сегодня эти батареи брошены и частично застроены зданиями местной высшей школы.



Представители American Computer опросили людей, живших в то время неподалеку от ракетной базы и работавших на ней в качестве гражданских специалистов. Выяснилось, что командованию части поступали сообщения об усилении активности НЛО, особенно в летном коридоре Нью-Джерси. Регулярно проводились учения, причем расположение учебных мишеней было таким, что версия о защите именно от космического, а не от советского вторжения кажется наиболее правдоподобной.

В самом конце 1947 года Bell Systems выпустила серию пресс-релизов: "После двухлетних широкомасштабных исследований ученые Белл Системс открыли транзистор". Вероятно, исследования были завершены талантливыми учеными Шокли, Бардином и Брэттайном под руководством вице-президента Bell Labs доктора Джона Мортона.

Джон А. Мортон был изобретателем, в 1943 году запатентовавшим, среди прочего, "сверхвысокочастотный вакуумный триод". В 1947 году он начал работать над транзистором, впоследствии разработал "логическую микросхему" — прототип транзистора. В начале 70-х годов Мортон трагически погиб: разбившаяся машина и мертвый ученый были найдены на шоссе.

Суммируем сказанное: инопланетные кремниевые усилители/переключатели, протестированные в октябре—ноябре 1947 года, "открыли" с ненормальной скоростью. Они на сотню лет опережали простые диоды и выпрямители того времени.

До 1947 года не было ни одной публикации о полупроводящих свойствах легированного мышьяком кремния. Для твердотельных диодов применялся только селен. Не было и идеи транзистора — полупроводникового аналога электровакуумных ламп-усилителей. Патенты на германиевый и кремниевый транзисторы были получены в 1948 и 1949 годах соответственно. Такая скорость исследований действительно кажется умопомрачительной.

Bell анонсировала свои первые транзисторы как "германиевые", поскольку германий применялся в существовавших выпрямителях. Это было сделано, чтобы защитить секретную кремниевую формулу. Однако, фактически Bell начала выпускать кремниевые транзисторы раньше, чем германиевые!

Технологии, разработанные Bell Systems после первых десяти лет изучения обломков НЛО, включают полупроводниковый лазер, другие твердотельные компоненты электрических схем, широкий спектр контрольных систем и телекамеры высокого разрешения.

В 50-х и 70-х годах Министерством юстиции США против Bell Systems было применено антитрастовое законодательство с отсрочкой применения. Bell Systems было предложено продать технологию производства транзисторов и интегральных микросхем другим компаниям. Интересно, почему за 20 лет после рассекречивания транзисторной технологии в 50-х годах ни одна другая фирма даже близко не подошла к созданию следующих по сложности устройств — микросхем, тогда как Bell потребовалось на это всего 10 лет?

Некоторые установки с разбившегося инопланетного корабля остались загадкой до сих пор, в частности, высокоэнергетический микроволновый усилитель, обладающий

эффектом разрушения твердых тел на молекулярные составляющие; схемы, работающие на иной энергии, нежели электрическая, и применяющие частицы с очень коротким периодом полураспада в естественном пространстве (мюоны); огромный индукционный генератор — спиральная система диаметром 50 футов, которая представляется инструментом для получения уникальных летных характеристик, свойственных НЛО (полагают, что это установка "гравитационного обнуления").

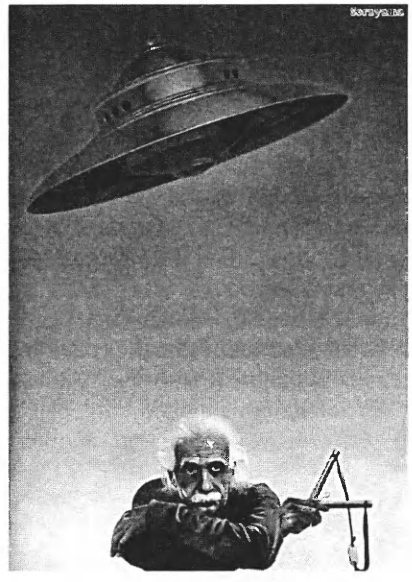
Специалисты AT&T считают, что транзистор разрабатывали как военный прибор в течение II мировой войны. Однако из документов того времени следует, что никакие военные установки не предполагали существования транзистора вплоть до начала 50-х годов. В дистанционных взрывателях, применявшихся в противовоздушном оружии в течение II мировой и даже в корейской войне в 50-х, использовались крайне ненадежные схемы на миниатюрных лампах, разработанные Silvan Corporation и AT&T для слуховых аппаратов.

Любопытно, что еще в 1946 году все специалисты Bell упорно работали над созданием прочной миниатюрной электровакуумной лампы-триода, о чем имеются соответствующие научные отчеты, а о транзисторах и не думали. Если же транзистором в то время занималось другое подразделение, почему имена тех, других не попали в патент 1949 года?

В советских технологиях вплоть до 70-х годов применялись миниатюрные электровакуумные приборы. Что мешало Советам совершенствовать высокие технологии, попытавшись скопировать транзистор? Может быть, просто с 1951 года секретами владели Bell Labs и Western Electric, и русские без обломков корабля из Розуэлла были просто неспособны их разгадать?

И вот, совсем недавно в Штатах вышла-таки книга подполковника Филипа Корсо, которая подтверждает информацию American Computer. Подтверждение можно считать независимым, поскольку Джек Шульман и Филип Корсо никогда не были знакомы, а книга "Day after Roswell" к моменту легендарной пресс-конференции Шульмана была еще в печати.

Увенчанный многими орденами 86-летний подполковник утверждает, что в 50-х годах он был привлечен к работе с обломками розуэллского корабля, лично видел заспиртованные трупы пришельцев и отвечал за контакты Министерства обороны США с фирмой Bell. Министерство обороны молчит, но в августе ассоциация "Граждане против секретности НЛО" (см. ссылки на http://www.mufon.com) начали судебный процесс, требуя рассекретить подробности розуэллского инцидента.



В ходе первого слушания Корсо подтвердил свои показания под присягой.

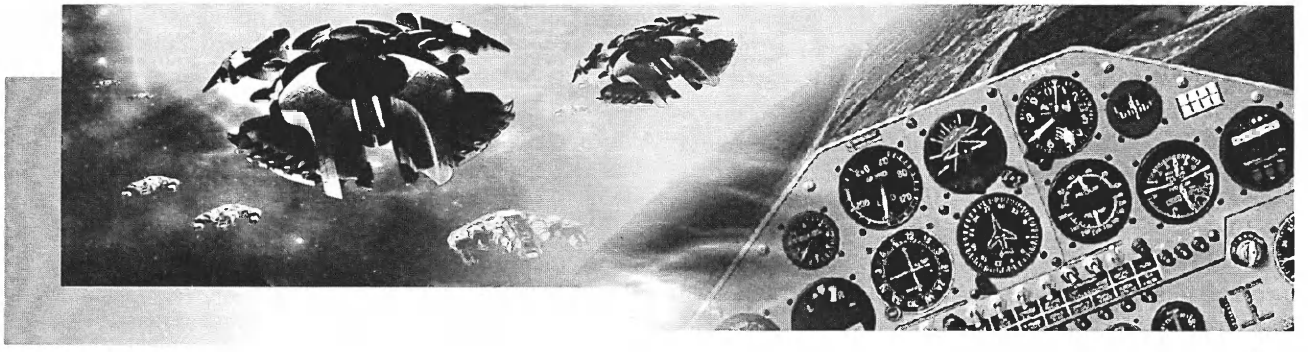
Одновременно стала проясняться история с фильмом о вскрытии инопланетянина. Нет сомнений, что фильм был снят и проявлен до 1956 года: в 1956 году фирма Kodak перестала выпускать пленку на основе ацетат-пропионата, перейдя исключительно на триацетат, а пленка со вскрытием была именно ацетат-пропионатной. В наши дни невозможно отснять фильм на старой пленке, потому что срок ее годности очень небольшой. Можно сразу отбросить рассуждения о манекенах и комбинированных съемках: в те годы не было латекса, силикона и прочих материалов, используемых мастерами по спецэффектам. Судя по маркировке на пленке и степени ее усыхания, фильм был снят именно в 1947 году. И, похоже, мы скоро узнаем, кто его снял.

В том, что оператор жив, никто не сомневается. Рэй Сантилли (нынешний владелец пленки) как-то раз проговорился, что оператор в детстве переболел полиомиелитом и что ему сейчас 86 лет. Полиомиелит — болезнь, плохо отражающаяся на конечностях. И действительно, судя по перемещениям оператора, снимавшего вскрытие, у него была больная нога. Дальше все просто: надо только расспросить бывших военных кинооператоров, кто из их коллег хромал. Такой оказался только один; сейчас он живет во Флориде и ему действительно 86 лет. Те, кто знают это, выдавать его пока не собираются. Дело в том, что оператора разыскивают и американские власти. Им-то хорошо известно, кто снимал вскрытие пришельца, но они не знают, где он живет: досье на оператора сгорело во время пожара в военном архиве.

Тем временем оператор "засветился" с другой стороны. Его сын взялся снять для Рэя Сантилли интервью со своим отцом, расфокусировав камеру, чтобы нельзя было разобрать его лицо. Но изображение все равно получилось достаточно четким. Рэй Сантилли должен был затушевать его "квадратиками", но почему-то этого не сделал. В декабре 1996 года интервью было показано по японскому телевидению, и кадры из него разошлись по сети Интернет. Теперь оператора могут узнать просто на улице.

Так что вполне возможно, история American Computer — действительно правда, и нынешней компьютерной революции мы обязаны инопланетянам!

По материалам журналов Fate (http://www.fatemag.com) и UFO Magazine (ufomagazine.com)



Ответ Гамлету: 3D or not 3D?

Сергей Голубев, "Верга Компьютерс"

Продолжение. Начало см. в "Магии ПК" N9

OpenGL ускорители для Пентиум II

ASUS 3Dexplorer V3000. Чипсет nVidia Riva 128. Мощный 3D-ускоритель, долгое время являвшийся основным конкурентом Voodoo Graphics. На Пентиум 200 MMX их скорость приблизительно одинакова, но на PII Riva 128 уже значительно быстрее. Существует PCI- и AGP-варианты этой карты. AGP-версия примерно на 20—30% быстрее. Riva 128 имеет 128-битную архитектуру, кэш текстур и вершин на чипе объемом 12 Кб и поддержку фиксированно 4 Мб SGRAM на плате. Выполняет рендеринг только в hicolor. Как AGP-, так и PCI-платы умеют хранить текстуры в системной памяти. На сегодняшний день Riva 128 — единственный 3D-ускоритель, дающий такую возможность. Максимальное разрешение в 3D — 960x720x16bit. Поддерживаются API Direct3D и OpenGL (ICD). Достоинства: высокая скорость 2D и 3D, поддержка DiME (хранение текстур в системной памяти с подгрузкой через AGP), полный драйвер OpenGL. Теперь о недостатках. Прежде всего — нестыковка текстур (щели). В OpenGL Riva 128 не поддерживает мипмэппинга, что вызывает раздражающий муар, хотя детализация картинки остается очень высокой. Отсутствие truecolor. Рекомендуется как 3D-ускоритель начального уровня для Пентиум 2, либо для старших моделей Пентиум при условии скорой модернизации на PII, а также для компьютеров на основе процессора AMD K6-2. Пожалуй, наиболее предпочтительно приобретение AGP-версии из-за низкой скорости Riva 128 на младших моделях Пентиум.

ATi Xpert@Play. Чипсет ATi Rage Pro. Компания ATi находится на первом месте по объему продаж 3D-ускорителей. Наиболее современный чип от ATi — полноценный 3D-ускоритель с отличным 2D и качественной поддержкой MPEG. Карточка Xpert@Play отличается от своего собрата Xpert@Work наличием качественного TV-выхода. Выпускается как в AGP-, так и в PCI-вариантах. Объем памяти 4 или 8 Мб SDRAM. Максимальные разрешения в 3D: для 4 Мб — 800x600x16bit, 720x480x32bit, для 8 Мб — 1280x1024x16bit, 1024x768x32bit. Поддерживаются API — Direct3D и OpenGL (MCD). Достоинства: широкое распространение, качественный TVOUT, поддержка DiME и ACPx2. Недостатки: плохая реализация dithering'а, невысокая скорость. Рекомендуется как видеокарта для мультимедиа-ориентированных компьютеров на базе Пентиум-166 MMX —Пентиум II-400, а также для всех желающих иметь качественный 3D TVOUT.

Expert Color 740. Чипсет intel 740. Фирма Expert Color зарекомендовала себя на нашем рынке как сильный конкурент Diamond Multimedia, выпуская платы, аналогичные даймондовским, но более дешевые и не уступающие им по качеству. Поэтому выбор intel 740 для чипсета 3D-ускорителя не

случаен. На этом же чипе собрана плата Diamond Stealth II G460. Intel 740 имеет 64-разрядную архитектуру и поддерживает до 8 Мб SGRAM или SDRAM. Оптимизирован под Pentium II, и только на нем гарантируется беспроблемная работа. Максимальное разрешение в 3D — 1280x1024x16bit. Несмотря на отсутствие truecolor, качество рендеринга очень высокое — превосходит, пожалуй, все имеющиеся сейчас на рынке игровые ускорители. Поддерживаются API Direct3D и OpenGL (ICD). Достоинства: поддержка DiME, AGPx2, больших текстур (1024x1024), отличное качество картинки. Недостатки: проблемы с поддержкой Soket7, невозможность хранить текстуры в видеопамяти, отсутствие truecolor. Рекомендуется как 2D/3D плата для компьютеров на базе процессоров Пентиум II.

Diamond 3Dmonster 2. Чипсет 3Dfx Voodoo2. Самый быстрый 3D-ускоритель на сегодняшний день. Поддерживает API — Glide, Direct3D, OpenGL (ICD). Объем локальной видеопамяти — 4 Мб фреймбуфер и 4—8 Мб текстурной памяти. Таким образом, Voodoo2 поддерживает от 8 до 12 Мб EDO-памяти. Diamond выпускает платы Voodoo2 только для шины PCI, но в принципе чипсет способен работать на AGP. Glide — собственный API Voodoo 2 — имеет широкую поддержку у разработчиков игр. Несмотря на то, что эпоха собственных API подходит к концу, все еще появляются игры без поддержки Direct3D или OpenGL (тот же Unreal). В Glide-игры могут играть только владельцы плат на чипсетах компании 3Dfx. Покупая плату Voodoo 2, можно не беспокоиться, что какая-нибудь новая игра на ней не запустится. Главное отличие Voodoo 2 в том, что они являются дочерними платами, которые умеют работать только с 3D. Voodoo 2 подключается к основной 2D-плате через сквозной аналоговый кабель. Для Voodoo 2 подходит совершенно любая 2D-плата. Подобная реализация имеет как плюсы, так и минусы. С одной стороны, можно использовать Voodoo 2 в компьютерах с большим 20-дюймовым монитором и дорогой 2D-платой почти так же, как и в компьютерах с 14-дюймовым монитором и дешевой видеоплатой. С другой стороны, это неэкономично: сам по себе принцип дочерней платы увеличивает стоимость видеосистемы. К тому же существует влияние сквозного кабеля на качество видеосигнала от 2D-платы. Чем выше разрешение 2D-платы и частота развертки, тем больше искажается сигнал. На разрешении 1280x1024 возникает необходимость использовать BNC-шнур ценой до $50.

Voodoo 2 поддерживает все ключевые 3D-функции, имеет очень хороший dithering, поэтому качество изображения практически не имеет погрешностей. Единственный недостаток — некоторое размытие изображения на низких разрешениях, но он нейтрализуется на разрешении 800x600 и, тем более, на 1024x768. Максимальное разрешение одной платы в 3D — 800x600x16bit.

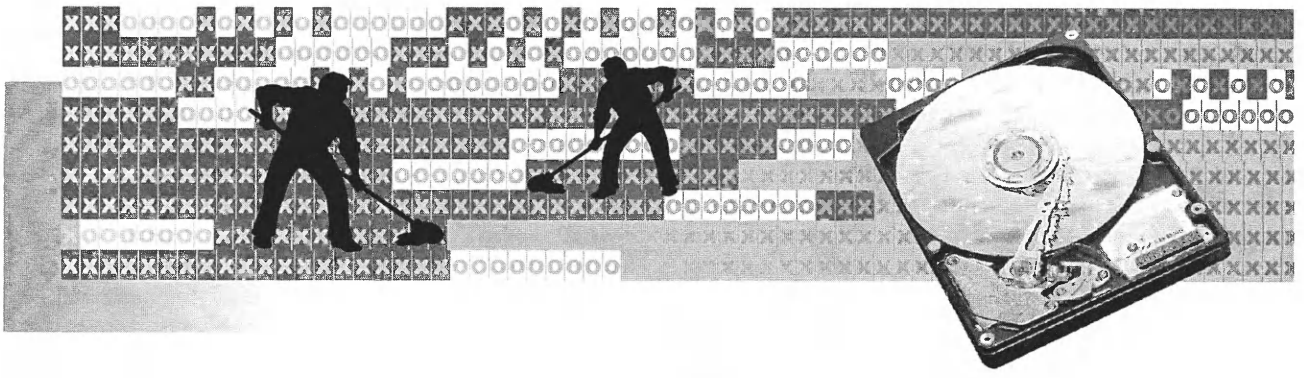
Две одинаковые платы могут работать совместно в режиме SLI. Они соединяются ленточным шлейфом. SLI-конфигурация удваивает объем фреймбуфера, и максимальное 3D-разрешение становится 1024x768, а также удваивает fillrate. Скорость, однако, в большинстве случаев возрастает гораздо меньше, чем вдвое. Кроме того, в режиме SLI остается неизменным объем текстурной памяти, так как ее содержимое у двух плат дублируется. К примеру, если соединяются две платы с 12 Мб, то SLI-конфигурация имеет 8 Мб фреймбуфер и 8 Мб текстурной памяти.

Достоинства: полная поддержка производителями игр, высокая скорость. Недостатки: высокая цена, влияние сквозного кабеля, а также отсутствие truecolor, оконных режимов и DiME. Рекомендуется как 3D-ускоритель для игровых компьютеров на базе любых процессоров.

Профессиональные OpenGL ускорители

Diamond FireGL 1000 pro. Чипсет 3Dlabs Permedia 2. FireGL-1000 pro — единственный среди профессиональных ускорителей, сравнимый по цене с игровыми. Он имеет хорошо отлаженный OpenGL (ICD), неплохо поддерживает оконные режимы и вообще в основном предназначен для работы в 3DSMAX и подобных программах. Но если он все равно стоит в машине, то можно попробовать поиграть и на нем. Максимальный объем видеопамяти — 8 Мб SGRAM. Максимальные разрешения в 3D — 1280x1024x16bit и 1024x76832bit. Поддерживаются API Direct3D и OpenGL (ICD). Достоинства: качественный драйвер OpenGL(ICD), поддержка оконных режимов. Недостатки: низкая скорость, плохое качество картинки в играх. Рекомендуется как дешевая плата для работы с 3D-пакетами, для игр советуем поставить в соседний слот Voodoo2.

3D ускоритель	Чипсет	Шина	API	Игры	Качество рендеринга (OpenGL)	Скорость работы на Пентиум	Скорость работы на Пентиум II	Цена (Ориент.)
Eagle 375 (2/4Mb)	S3 VirgeDX	PCI	Direct3D	Turok_D3D	-	*	*	27/42
Ati 3D Charger (2/4M)	ATi Rage II	PCI, AGP	Direct3D	Turok_D3D	-	**	**	60/76
Matrox Mistique (2/4Mb)	MGA 1064	PCI	Direct3D	Turok_D3D	-	**	**	60/75
Diamond 3Dmonster (4Mb)	3Dfx Voodoo Graphics	PCI	glide, OpenGL(ICD) Direct3D	Turok_D3D, Flight_Unlimited_2, Quake_2, Unreal	*****	******	****	100
Matrox m3D (4Mb)	VideoLogic PowerVR PCX2	PCI	PoverSGL, OpenGL(MCD) Direct3D	Turok_D3D, Quake_2, Unreal	****	*****	****	75
Diamond Stealth II S220 (4/8Mb)	Renditions Verite2100	PCI	RRedLine, Speedy3D, Direct3D, OpenGL(ICD)	Turok_D3D, Quake_2	******	******	*****	75/90
ASUS 3Dexplorer V3000 (4Mb)	nVidia riva128	PCI, AGP	Direct3D, OpenGL(ICD)	Turok_D3D, Quake_2	******	****	*******	65
Ati Xpert@Play (4/8Mb)	Ati Rage pro	PCI, AGP	Direct3D, OpenGL(MCD)	Turok_D3D, Quake_2	*****	****	*****	65/85
Expert Color 740 (8Mb)	intel 740	AGP	Direct3D, OpenGL(ICD)	Turok_D3D, Quake_2	**********	?	*******	65
Diamond 3Dmonster 2 (8/12Mb)	3Dfx Voodoo2	PCI, AGP	glide, OpenGL(ICD) Direct3D	Turok_D3D, Quake_2, Unreal	********	*******	**********	255



Кирилл Кириллов

FAT32 — дисковое пространство без проблем

Свободное место на винчестере — это то, чего постоянно не хватает. Между пользователем и компьютером идет постоянная борьба за этот ресурс. Всегда трудно решить, каким из приложений можно пожертвовать, чтобы установить другое. Совсем плохо, когда под рабочие приложения места не остается и приходится жертвовать любимыми играми.

Но недостаток дискового пространства возникает не только из-за установленных приложений. Некоторую его часть "съедает" фрагментация.

В операционных системах MS-DOS — Windows'95 информация о диске хранится в FAT 16 (File Allocation Table) — шестнадцатиразрядной таблице размещения файлов. Логически поверхность магнитного диска разбита на сектора (как в школьной геометрии) размером 512 байт. Для чтения информации сразу с нескольких секторов их объединяют в кластеры, и чем больше размер диска, тем больше размер кластера. Эти кластеры являются единицей хранения информации, то есть, чтобы записать один бит информации, нужно занять целый кластер. Размер кластера определяется размером диска. Например, для диска размером больше 512 Мб один кластер имеет размер 16 Кб. Файл размещается на диске в последовательности смежных кластеров, но нет никакой гарантии, что он точно уложится в размеры кластера. А если хотя бы малая часть его попадет в следующий кластер, он будет считаться занятым. Большое количество таких кластеров и называется внутренней фрагментацией (в отличие от внешней, когда при стирании и записи файлов на диске остаются пустые фрагменты, слишком малые, чтобы туда поместилась какая-либо информация). При больших размерах диска и наличии множества небольших файлов фрагментация может занять до 30% дискового пространства. Чтобы уменьшить размер кластера и снизить потери, приходится разбивать винчестер на несколько логических устройств.

Естественно, разработчики системного программного обеспечения не могли обойти своим вниманием проблему внутренней фрагментации. Для машин на платформе PC решением стал FAT 32 — усовершенствованная тридцатидвухразрядная таблица размещения файлов. Она позволяет поддерживать размер кластера в 4 Кб для дисков размером в несколько гигабайт, что существенно экономит место. Для примера можно сказать, что конвертирование FAT16 в FAT32 позволяет высвободить около 100 Мб на каждые 500 Мб записанной на диск информации. Результаты говорят сами за себя.

До появления Windows'98 особого желания "переконвертить" диск в FAT32, при всех его положительных качествах, не возникало. Программы, позволяющие это сделать, мягко говоря, не впечатляли. В основном для этого использовались либо пугающая своей простотой команда format в OSR2 (кто же доверит свои файлы какой-то непонятной программе?), либо слишком "навороченная" Partition Magic. Тем более, что при конвертации с помощью этих программ вероятность потери всей информации на винчестере была достаточно высока. Поэтому пользователи воспринимали работу с FAT32 как очередной "закидон" слишком умных разработчиков.

В Windows'98 для конвертации в FAT32 сделан простой и понятный мастер, очень настойчиво предлагающий произвести конвертацию. Более того, сама Windows'98 — первый программный продукт, оптимизированный под FAT32. Загрузка программ с винчестера под Windows'98 при использовании FAT32 производится значительно быстрее, и компьютер использует меньшее количество ресурсов системы.

И все же без некоторых недостатков не обошлось. Если вы преобразуете ваш жесткий диск в формат FAT32, используя встроенный

конвертер диска, то вернуться к использованию FAT16 уже не сможете. Поэтому и в дальнейшем придется использовать только Windows'98, ведь никакая другая операционная система этот формат диска не распознает. По идее, если "девяносто восьмые" вам не понравились совсем, можно будет использовать OSR2, но упоминания о возможности ее установки в фирменной документации от Microsoft не встречается.

По мысли разработчиков Windows'98, уж если ты начал работать с этой операционной системой в целом и с FAT32 в частности, обратной дороги уже не будет. С одной стороны, это обеспечивает пользователей самыми последними техническими новинками, но с другой — обидно, что это обновление осуществляется насильственно.

Старое программное обеспечение сжатия дисков (Drive Space) несовместимо с FAT32. Если диск им уже сжат, вы не можете обновить таблицу. Старый Drive Space нужно удалить или заменить на новый, версии 3.0.

Если вы преобразуете съемный диск и используете диск с другими операционными системами, которые не поддерживают FAT32, то при использовании другой операционной системы он также не будет виден. Хотя на большинство программ, по заявлению Microsoft, преобразование FAT16 к FAT32 никак не воздействует, некоторые дисковые утилиты, написанные под FAT16, перестанут работать, о чем система вас вежливо предупредит.

Если вы преобразуете ваш жесткий диск в FAT32, использующий конвертер диска, то больше не сможете использовать раздельную начальную загрузку, чтобы выполнить более ранние версии Windows (Windows 3.x, Windows'95, Windows NT 4.0). Однако более ранние версии Windows могут получать доступ к жесткому диску FAT32 через сеть.

В заключение хочется сказать: то, что у нас продают под видом "полностью русской" Windows'98, не является таковой и не имеет переведенных хелпов, а почитать их перед такой ответственной операцией, как конвертация FAT16 в FAT32, очень даже неплохо.

Алгоритм и алгебра

"Когда я увидел, что индийцы составляли из девяти букв любое свое число благодаря расположению, которое они установили, я пожелал раскрыть, если будет угодно богу, что получается из этих букв..."

Ал-Хорезми

Похожие два слова, не правда ли? Оба начинаются на "ал", как и имя автора приведенной цитаты. Интуиция не обманула вас, уважаемый читатель. В их происхождении очень много общего.

Как известно, до эпохи раннего средневековья в Европе пользовались римскими цифрами, а на Востоке писали названия цифр полностью, либо обозначали их буквами. Введение десятичной позиционной нумерации стало одной из важнейших заслуг багдадской школы ученых.

В начале IX века Багдад был развитым культурным и научным центром. Сюда съезжались ученые из разных стран, покоренных арабами. В этом городе по образцу Александрийского музея был построен Дом мудрости (Бейтал-Хикма), представлявший собой нечто вроде академии наук.

В 815 году Дом мудрости возглавил выдающийся математик своего времени ал-Хорезми. Из его математических работ до нас дошли в более или менее цельном виде два трактата — арифметический и алгебраический.

Трактат по арифметике (его заглавие можно перевести как "Книга о сложении и вычитании на основе индийского счета"), в сущности, является первым в мире руководством по обучению счету. Основные разделы трактата — нумерация, действия с простыми числами и учение о дробях. В этой работе ал-Хорезми подробно описал сложение, вычитание, умножение, деление и извлечение квадратного корня. В число арифметических действий он включил отдельно удвоение и раздвоение (умножение на 2 и деление на 2), которые использовались при извлечении корня.

В арифметическом трактате ал-Хорезми описал также девять индийских цифр и "маленький кружок, чтобы по нему знали, что разряд пуст" (ноль по-арабски называется "сыфр" — пустой). В Европу трактат попал в конце XI — начале XII века через мавританскую Испанию (его изложение на латинском языке хранится в библиотеке Кембриджского университета). Вскоре индийские цифры, занесенные в Багдадский халифат в конце VIII века, в Европе стали называть "арабскими", хотя арабы лишь добавили к ним десятую цифру — ноль. А слово "сыфр" стало во всех европейских языках означать сначала "цифру", а затем и "шифр".

Латиноязычный список трактата начинался словами "Сказал Алгоритми...". Больше шести столетий это Algorithmi представляло собой загадку для европейских ученых, и лишь в сороковых годах прошлого века было правильно расшифровано как искажение арабского имени ал-Хорезми. Полное имя ученого — ал-Хорезми Абу Абдулла Мухаммад ибн Муса ал-Маджусси, а слово "Хорезми" указывает на происхождение: родом он из среднеазиатского государства Хорезм.

И хотя далее средневековое Algorithmus правильно понималось как собственное имя, оно все-таки осталось нарицательным — названием позиционной системы счисления и искусства счета в ней с использованием индийских цифр, сохранившись до настоящего времени в виде термина "алгоритм". Сначала алгоритмом называли правила сложения, вычитания, умножения "столбиком" и деления "уголком". Впоследствии термин "алгоритм" приобрел более широкий смысл — всякий регулярный вычислительный процесс, дающий решение за конечное число шагов.

Второй математический трактат ал-Хорезми, посвященный алгебре, помимо прочего содержит учение об уравнениях первой и второй степеней, правила решения некоторых геометрических задач. Приведение подобных членов уравнения называлось в книге "противопоставление", а перенос отрицательных членов уравнения в противоположную часть с обратным знаком — "восстановление" (существование отрицательных членов в уравнении на Востоке считалось ненормальным явлением). Само название трактата "Книга о восстановлении и противопоставлении" (Китаб ал-джабар валь-мукабала) и дало название науке: от слова "ал-джабар" — восстановление — произошло слово "алгебра".

Владимир Буслаев

Между ценой и престижем

Андрей Смирнов

Коль ошибся с материнкой, жди с апгрэйдами заминки...

Актуальность темы апгрейда в последнее время многократно возросла: в связи со стремительным ростом цен меньше всего хотелось бы потратиться на барахло. Итак, вы решили обновить компьютер. Для начала надо аргументировать — зачем? Если вы работаете с офисными приложениями, то кроме увеличения емкости винчестера вам, наверное, ничего и не надо. Ну, а если ваш компьютер слишком долго "думает", а иногда даже зависает при расчетах, игры тормозят до невозможности и возникают сложности с работой модема, звуковых или других плат расширения? Допустим, часто не в компьютере дело, а в программах, но вы сломались и пошли выбирать. Выбирать что?

Солидные фирмы продают компьютеры как бытовые приборы, а не как набор комплектующих. По этой схеме работают, например, Acer и Packard Bell. Но у этих фирм есть один недостаток — они не производят техники специально для России. Например, в 1996 году я пришел в известную фирму, который продает Packard Bell:

— Хочу, чтобы все!!!

— OK, но вот только фирменный модем на наших линиях не потянет, рекомендуем USR Sportster.

— Ладно.

— Но тогда у вас не будет работать дистанционное управление, наша фирменная фишка.

— Ладно.

— И, поскольку звуковая карта стоит на фирменном модеме, ее советуем поменять на Creative.

— А что остается от фирменного компьютера?

— Корпус, монитор и, конечно, цена...

После этого я пошел в первый попавшийся магазин и купил свой Pentium 100.

Время шло, появился MMX, а за ним и P-II. Как выяснилось, моя материнская плата не поддерживала не только MMX, но и PnP, из-за чего у меня под Windows NT4.0 не работал PnP SoundBlaster, а модем пришлось "привязать" на COM2 (он тоже PnP, но все можно установить и вручную). Я поставил WaveTable, который иногда подвисал — воспроизводимая нота не переставала звучать до выключения компьютера (как мне объяснили, тоже из-за материнской платы).

Тогда я поднакопил денег и решил заменить свой Pentium 100 на Pentium II 300. Начал с обзвона фирм, занимающихся апгрейдом. В той фирме, где два года назад я купил свой ящик, мне ответили, что подобная замена не является апгрейдом и что мне проще купить новый компьютер или обратиться в другую фирму. Денег у меня было не много, и я решил рискнуть — позвонил в фирму "А", хотя ходят слухи, что эта фирма торгует старьем.

Корпус моего ПК сразу забраковали: "Ну, не товарный у него вид", и предложили забрать на память. Материнскую плату, процессор и 32 метра памяти оценили в сотню баксов (в других фирмах за них вообще ничего бы не дали). Новая материнка, Pentium II (Celeron) 300, 64 метра памяти и новый корпус тянули на пять сотен. Итого четыре сотни за апгрейд, что меня вполне устраивало. Из старой комплектации остался S3Virge с 4 метрами, Creative SB 16 PnP, два винчестра, CD-ROM Acer x8 и, конечно, мой трудяга факс-модем USR Sportster Voice 33,6 PnP.

На следующий день я в приподнятом настроении приехал за этим чудом техники. Все работало с ощутимым ускорением (довольно нехилого размера картинку он упаковал мгновенно, я даже не поверил и посмотрел ее — действительно записал). Один из моих винчестеров оказался с поддержкой UltraDMA, и принтерный порт был битрониксом, что также увеличивало скорость.

На старой плате, под управлением NT4.0, нельзя было пользоваться PnP-устройствами, новая плата

сама все конфигурирует в процессе загрузки и NT, только предлагает установить драйверы на найденные устройства. С Win'95 и OSR2 не было никаких проблем, но вот с Win'98 пришлось повозиться. Мой S3Virge (325) стал намного быстрее крутить MPG-файлы — с 26 до 76 fps без потери качества.

А теперь — о процессоре. Celeron 300 не имеет кэша 2-го уровня, но это самый выгодный вариант комплектации. Он быстрее большинства Pentium MMX и намного дешевле полноценного Pentium II. Если вы установите его на хорошую материнку типа BX, то он нормально работает. А 100 МГц DIMM частично компенсируют недостаток кэша 2-го уровня. Кстати, большинство тестовых программ опознали мой Celeron 300 как Pentium Pro с поддержкой MMX.

Я не навязываю свой вариант апгрейда, но если у вас 386, 486, Pentium (не MMX) или вам нужен современный компьютер с весьма отдаленным сроком следующего апгрейда по доступной цене — моя комплектация оптимальна. Владельцам MMX могу посоветовать AMD 3D Now 300 —данная модель при меньшей цене превосходит Pentium II 233—300 и, что немаловажно, поддерживает работу на платах с 100 МГц шиной и AGP. Немаловажная особенность процессоров AMD — постоянное развитие новых технологий и использование всех ресурсов старых технологий.

Основные советы всем, кто докупает платы расширения или делает апгрейд:

1. Заархивируйте все ценное (оригинальные и созданные вами файлы, копий которых нет ни у вас, ни у ваших друзей). Вообще резервное копирование — это то, о чем все забывают и больше всего потом страдают.

2. Если вы опасаетесь, что что-то из ваших данных может быть украдено, обязательно удалите это с винчестера, предварительно сохранив в надежном месте. Не забудьте про пароль для доступа в Интернет. Один мой друг после апгрейда был немало удивлен, когда увидел свой баланс часов в Интернете. Скопировать пароль для профессионала — дело пары минут, даже в вашем присутствии!

3. Требуйте, чтобы вам отдельно записали все драйверы для вашего оборудования, установленного на компьютер, но отсутствующего в базовой поставке (имеются в виду как оригинальные драйверы, так и обновленные версии стандартных. Конечно, все можно найти в Интернете на страницах производителей компьютерной техники, но если драйвер лежит на странице другой фирмы, не исключено, что это дополнение, позволяющее добиться наибольшей производительности, иногда ценой качества. Отдельная копия драйверов поможет вам сэкономить время и нервы в случае полного уничтожения информации с вашего диска, а от этого никто не застрахован.

4. Не поленитесь первые сутки (без перерыва) погонять компьютер на тестах и со всеми используемыми вами программами. Обращать внимание надо на сбои в работе (потеря связи с устройством, зависание, некорректная работа), наличие шумов, высокую температуру (более 40°C). Например, моя материнская плата грелась до 42°C, а иногда и до 50°. CD-ROM при температурах 20—55°C переставал обнаруживаться виндами, и даже если обнаруживался, очень плохо читал диски. Я обратился в фирму, сделавшую апгрейд, они протестировали машину и поставили дополнительный вентилятор охлаждения. Теперь у моего компьютера температура колеблется от 37 до 40°C и все нормально работает.

5. Перед апгрейдом протестируйте машину каким-нибудь тестом (подойдет и Winbench, и Sysinfo, хотя для многих более показательна работа их основных программ — графические пакеты, Word или навороченные игры). После апгрейда повторите тот же тест и сравните результат. Как правило, не должно быть хуже.

Успехов в освоении этих железных монстров, убивающих ваше время...

Так уж сложилось на российском компьютерном рынке, что портативный компьютер приобретается для решения каких-то узких, специальных задач. Его покупают инженеры для работы "в поле", то есть для установки и настройки оборудования на удаленных объектах, бизнесмены или менеджеры, вынужденные в бесконечных командировках постоянно иметь под рукой мобильный офис, коммивояжеры или разработчики крупных проектов, которым необходимо провести презентацию своей продукции на выезде, в офисе потенциального клиента.

В общем, ноутбук — это дорогостоящая "рабочая лошадка", которая, как правило, не предназначена для отдыха и развлечений. Безусловно, есть и исключения: целый класс ноутбуков даст фору настольным компьютерам и по мощности процессора, и по объему памяти, и по качеству экрана, и по мультимедийным возможностям, но...

Но вся эта роскошь в портативном компьютере достигается гораздо большими финансовыми вложениями, чем в настольном ПК.

Компания "Диалектика" предлагает "золотую середину" — мощную мультимедийную систему на базе ноутбука и при этом без больших денежных затрат.

Как этого достичь?

Пусть ваш портативный компьютер остается легким, не очень дорогим инструментом для решения повседневных задач. Не тратьте огромные суммы на модернизацию его до мощной графической или игровой станции. Приобретите ноутбук с Docking Station. Что это такое?

Docking Station — это специальная "подставка под ноутбук", которая подключается непосредственно к шине компьютера с помощью специального разъема на корпусе. Поскольку связь осуществляется именно по шине, после подключения Docking Station она и ноутбук становятся единым организмом, действующим на одной частоте и полностью контролируемым BIOS компьютера и операционной системой.

Ноутбуки Chicony: расширение без ограничений

В зависимости от модели разные Docking Station предоставляют разные возможности, но, как правило, это:

— звуковая стереосистема с колонками, разнесенными по углам Docking Station;

— расширитель портов — последовательные, параллельный, игровые, выход на внешний монитор, PS/2, USB, часто video-in и video-out;

— один или несколько разъемов для стандартных устройств PCI, в которые вы можете разместить любые PCI-карты — 3D-акселераторы, SCSI-адаптеры, видеобластеры, скоростные сетевые контроллеры, TV-приемники и многое другое, то есть все то, что для портативных компьютеров стоит гораздо дороже или еще недоступно в массовом производстве;

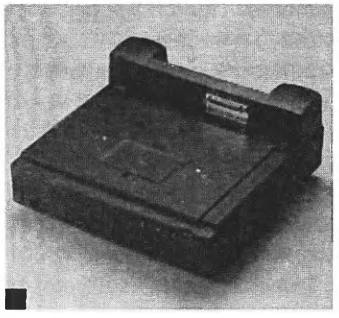
— отсеки для дополнительных стандартных накопителей HDD, ZIP-drive, CD-ROV, магнитооптики или даже полузабытого дисковода 5,25".

Безусловно, во время работы общее питание системы осуществляется через Docking Station, а аккумулятор ПК заряжается (кстати, в некоторых моделях Docking Station есть отсек для одновременной зарядки второго аккумулятора).

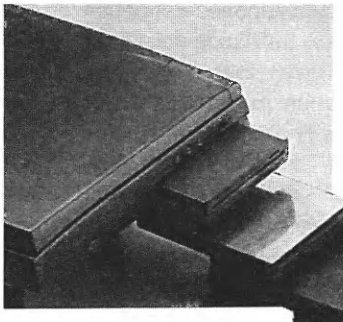
Для демонстрации работы такой системы-кентавра компания "Диалектика" установила в одну из Docking Station 3D-акселератор Diamond Monster. Docking Station работает в паре с портативным компьютером Chicony 979. Поиграв вечером в Quake последней версии на 20-дюймовом мониторе, подключенном к Docking Station, утром вы сможете путем установки в Docking Station мощной сетевой карты и магнитооптического привода получить отличное рабочее место для своего офиса.

Кстати, именно фирма Chicony, ранее известная на российском рынке только как производитель комплектующих и устройств ввода, предлагает ноутбуки с широчайшим ассортиментом дополнительных устройств. Одно из них — Port Replicator. Отличие его от Docking Station заключается в невозможности установки внутренних устройств, но при этом обеспечивается то же количество внешних подключений и звуковая стереосистема, причем по цене в три раза ниже.

Однако все это — "наружное" расширение ноутбука. Если же вам необходимо хранить большие объемы данных непосредственно в мобильный системе и переносить их с компьютера на компьютер, то в компании "Диалектика" для ноутбуков Chicony вы можете приобрести ZIP-drive (100 Мб) или LS-120-drive. Оба эти устройства используют стандартные носители соответствующих форматов и по цене сопоставимы с аналогичными устройствами для настольных компьютеров. Модульный конструктив ноутбуков Chicony позволяет быстро установить эти накопители вместо "штатного" floppy-дисковода (что особенно удобно в случае с LS-120).



Docking station



FDD

Port Replicator

Та же модульность делает возможной установку второго аккумулятора вместо накопителя. Это очень удобно при долгой работе на удалении от электросети.

Для тех, кто привык идти в ногу со временем и использовать самые последние достижения в компьютерных технологиях, будет интересна возможность замены CD-ROM на DVD-drive. Высококачественные 13- и 14-дюймовые активные матрицы ноутбуков Chicony вместе с DVD-drive составляют отличную видеосистему с высоким разрешением и стереозвуком.

"Диалектика"
Тел.: (812) 327-8117, 327-8268

Ethernet против Token Ring

Кирилл Кириллов

Худой сетью рыбы не наловишь

Из нескольких десятков типов систем проводных соединений в локальных вычислительных сетях (ЛВС) сегодня наиболее распространены два стандарта — IEEE (Institute of Electrical and Electronic Engineers) 802.3 (Ethernet) и IEEE 802.5 (Token Ring).

Эти стандарты снискали широкую популярность потому, что являются открытыми и не контролируются какими-либо конкретными разработчиками оборудования.

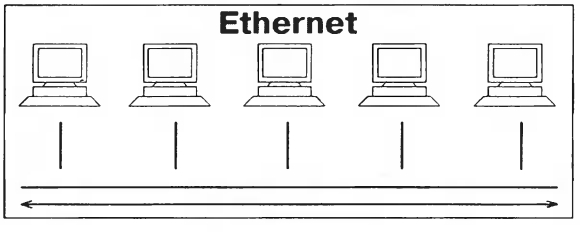
Система 802.3 не является Ethernet в классическом виде. Она унаследовала свое название от системы, достаточно давно разработанной тремя фирмами: Intel (набор микросхем), Xerox (программное обеспечение) и Digital Equipment (тестирование и внедрение). Новые версии стандарта 802.3 разрабатываются и принимаются до сих пор.

Ethernet была создана в 1975 году и сразу же получила огромное признание. Основным достоинством новой тогда системы стала возможность обеспечивать высокую производительность при относительно низкой стоимости. В течение десяти последующих лет Ethernet развивался, оставив далеко позади всех конкурентов. Он стал неотъемлемым компонентом архитектуры вычислительных сетей многих поставщиков и, в частности, таких гигантов, как DEC и AT&T. Ethernet, как и Token Ring, — однополосная сеть, то есть может передавать не более одного сообщения в единицу времени. Поначалу разработчики хотели приспособить Ethernet для широкополосной передачи (несколько сигналов по одной физической линии).

Для описания работы Ethernet был придуман специальный технический термин Carrier Sense Multiple Access with Collision Detection (CSMA/CD) — множественный доступ к опрашиваемой несущей с возможностью разрешения конфликтов. Множественный доступ означает, что любой абонент в любой момент времени может начать передачу данных в сети. Опрос несущей предполагает, что абонент должен подождать, пока линия освободится, и только после этого начать передачу. Обнаружение конфликтов дает возможность разрешить ситуации, когда два пользователя сети начинают "перебивать" друг друга. В этом случае протокол сети отключает всех участников передачи данных и некоторое время не пускает их обратно. Затем передача сообщений по сети возобновляется.

Отсюда вытекает первый недостаток Ethernet. При скорости обмена 10 Мбит/с и небольших объемах и интенсивности передачи информации конфликтные ситуации маловероятны, но, если множество абонентов начнут одновременно посылать сообщения, то значительная часть времени работы сети уйдет на обнаружение и разрешение конфликтов. Такие ситуации часто встречаются в масштабах среднего и крупного предприятий, где количество абонентов сети может превышать несколько сотен.

Второй недостаток Ethernet в том, что топология сети выполнена как общая шина. Это означает, что все станции сети подключаются к одному физическому проводу. Помимо невысокой надежности (при разрыве кабеля из строя выходит вся сеть), каждое сообщение в сети приходит ко всем абонентам, но принимает его только адресат, остальные это сообщение



игнорируют. Это ведет к усложнению оборудования и программного обеспечения, к большим временным затратам.

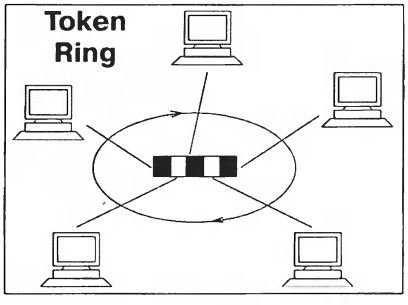
Чтобы установить сеть на основе Ethernet, необходимо иметь достаточно длинный кусок коаксиального кабеля с сопротивлением 50 Ом (сопротивление телевизионного "коаксиала" 75 Ом), ограниченный двумя терминаторами (железными наконечниками), и сетевые карты, монтируемые обычно внутри компьютера. Сеть легко и быстро наращивается путем подключения новых сегментов кабеля с подключенными станциями, но с увеличением размера сети становится очень трудно найти неисправности и повреждения общей шины. Несколько портит общую картину и то, что сеть Ethernet нельзя наращивать до бесконечности. При прохождении по кабелю сигнал затухает, и для нормальной работы необходимо устанавливать повторители через определенное число сегментов повода.

К небольшим неприятностям Ethernet можно отнести и то, что на эту систему существует три стандарта (обычно их так и называют — Ethernet 1, 2 и 3), и их сетевые карты несовместимы друг с другом. При покупке карт на это надо обратить самое серьезное внимание.

В 1992 году фирма Grand Junction предложила систему, позволяющую достичь в сети Ethernet скорости 100 Мбит/с. Она получила название 100BaseX. Сети Ethernet с такой скоростью передачи уже предлагались некоторыми разработчиками, но 100BaseX уникальна тем, что позволяет интегрировать отдельные участки сети, выполненные по технологии 100 Мбит/с, в сеть на 10 Мбит/с.

Хотя система Ethernet и стала невероятно популярной, ее недостатки прибавили много седых волос сетевым администраторам. С таким положением никто, конечно, мириться не хотел, но и достойной альтернативы тоже не было, пока в 1985 году не появился Token Ring. IBM буквально ворвалась на рынок с новым стандартом, который, благодаря чисто технических новшествам, должен был потеснить Ethernet на рынке вычислительных сетей. Надо признать, что у IBM редко что-нибудь не получалось. Не просчитались они и на этот раз.

Token Ring была создана для того, чтобы преодолеть очевидные недостатки Ethernet. Само название этой системы (в переводе с английского — маркерное кольцо) раскрывает принципы ее работы. В сети циркулирует один маркер (последовательность бит), который передается от одной станции к другой в одном направлении. Если у станции нет сообщения, которое нужно послать, она пропускает маркер, а если есть — она захватывает его и удерживает до тех пор, пока не получит подтверждение приема сообщения от адресата. После этого станция передает маркер дальше по кольцу.



Поскольку сообщение может посылать только обладатель маркера, в сети начисто отсутствуют конфликты, характерные для Ethernet. Станция, "захватившая" маркер, имеет исключительное право доступа в сеть. Механизм передачи маркера гарантирует регулярную отправку сообщений для каждой станции через определенные промежутки времени. Однако и Token Ring не лишена недостатков. Если маркер по каким-то причинам будет утерян, станции могут ждать его до бесконечности, не имея возможности ни передавать, ни получать сообщения. Чтобы избежать такой ситуации, одну рабочую станцию назначают активным монитором (Active Monitor-AM). Активный монитор следит за состоянием сети и контролирует прохождение маркера через себя. Если за определенный промежуток времени маркер не появляется в его "поле зрения", он просто генерирует новый и обеспечивает дальнейшую работу в сети.

Token Ring имеет достаточно сложные механизмы разрешения многих проблем, таких как вхождение или выход из кольца новой станции, корректировка ошибок, поиск неисправностей и т.д. Но при всей своей сложности эта сеть обеспечивает скорость передачи данных 16 Мбит/с и возможность создавать большие сети в масштабах крупных предприятий. Расширение сети осуществляется с помощью нового концентратора (MAU) с подсоединенными станциями, устанавливаемого в монтажный шкаф вместе с другими концентраторами. Максимально возможным считается установка 9 MAU в один монтажный шкаф и присоединение к ним 72 рабочих станций при общей длине проводов до 300 м. Если длина проводов больше, необходимо устанавливать повторители.

Другое преимущество Token Ring состоит в том, что отдельные компоненты этой сети имеют диагностические способности. Станция способна выполнить самопроверку по подключенным кабелям и в случае обнаружения неисправности автоматически исключить себя из сети. Станция посылает активному монитору сигнал об аварии, и тот автоматически реконфигурирует сеть.

Надо отметить, что Token Ring является кольцом только на логическом уровне. На физическом же она представляет собой топологию звезда. В центре системы находится концентратор, к которому отдельными проводами подключены все рабочие станции, поэтому исключение одной из них не приведет к разрыву сети.

Для установки Token Ring необходимо иметь сетевую интерфейсную карту, кабельную систему и концентратор. В сумме это обходится несколько дороже, чем Ethernet, но надежность управления и легкость устранения неисправностей делают Token Ring одним из самых перспективных типов сетей.

Компьютер для фотографа.

На чем печатать фотографии

Николай Богданов-Катьков

В первой статье этой серии я рассказал о процессе цветной печати и сложностях, возникающих при попытках улучшить ее качество. Теперь рассмотрим технологии печати, используемые в современных принтерах.

Как преодолевают трудности

Каждая фирма, производящая принтеры, стремится к наивысшему качеству печати. Если еще два—три года назад высокое качество печати было свойственно только самым дорогим моделям, то сейчас даже относительно дешевые принтеры, "принтеры начального уровня", судя по рекламе, печатают по "новым уникальным технологиям, обеспечивающим..." и т.д.

Это верно, но только отчасти. Действительно, каждая фирма сейчас сама совершенствует технологию печати, и каждый метод можно называть уникальным. С другой стороны, набор средств ограничен, он диктуется особенностями струйной печати.

При ***струйно-пузырьковом*** способе капля чернил, находящаяся в капилляре, выталкивается из сопла пузырьком пара, который образуется при нагреве капилляра. Объем капли определяется размером капилляра, изменить его сложно. Кроме того, для мгновенного образования пузырька пара требуется очень быстрый нагрев до высокой температуры, обычно около 500°C. Часть растворителя испаряется на стенках капилляра, и в объеме капли образуются сгустки красителя. В результате наносимая точка получается плохой — неравномерной по окраске, далеко не круглой формы, а иногда вокруг точки появляется много мелких точек, клякс. Об этом подробно написано в предыдущей статье.

При ***пьезоэлектрическом*** способе печати капля выбрасывается при сжатии стенок капилляра, когда пьезоэлемент деформируется под действием электрического поля (импульса). То же самое электрическое поле, только более слабое, чем при подаче импульса, может изменять форму и объем капилляра, а значит, этот способ дает больше возможностей для регулировки размера капли. На практике можно получить каплю объемом в несколько процентов от максимального.

Пьезоэлектрическими технологиями печати пользуются фирмы Calcomp (California Computers) и Epson. Струйно-пузырьковые принтеры выпускают большинство других фирм — Hewlett-Packard, Canon, Lexmark, Olivetti.

Самый простой путь — увеличить разрешающую способность принтера. При разрешении 600 x 600 dpi на каждый квадратный миллиметр приходится 560 точек, при 440 x 720 dpi — 1600, а при 1200 x 1200 dpi (максимальное разрешение, достигаемое в некоторых моделях Lexmark) — даже 2230 точек. Это позволяет избежать блочности изображения, но... снижает надежность. Дело в том, что повышение разрешающей способности требует очень точной работы механических узлов: для нанесения точек печатающая головка должна перемещаться с шагом 0.02 мм, обеспечивая при этом высокую скорость печати. Такое сочетание точности и скорости десять лет назад имели только прецизионные физические приборы! К сожалению, все движущиеся детали со временем изнашиваются, а значит, и точность в процессе эксплуатации принтера будет снижаться.

Кроме того, чем меньше размер капли, тем труднее нанести хорошую точку — круглую, не расплывающуюся, без клякс. Поэтому разрешающую способность принтера нельзя увеличивать все больше и больше — это уже не приведет к повышению качества.

Считают, что разрешение 1200 x 1200 dpi — предельное для струйно-пузырьковой технологии. Технология печати MicroPiezo, рекламируемая фирмой Epson, является сочетанием

методов MicroDot (микроточка) и MicroWeave (микропереплетение). Это означает, что печатающая головка наносит точки определенного (изменяемого по мере надобности) размера в строго определенные места. При этом получается изображение, показанное на рисунке 1.

На рисунке показаны примеры нанесения точек в углах квадрата (1 а) и в вершинах равностороннего треугольника (1 б). Меньшие точки наносятся в промежутках, оставленных большими точками. В первом случае соотношение площадей точек разных цветов будет равно примерно 1:5, а во втором — 1:40. Но в обоих случаях размер ячейки (блока) фактически будет равен размеру большей точки. Это означает, что при таком способе печати отдельные ячейки не будут заметны даже при разрешении 300 x 300 dpi.

Чтобы получить тот же эффект нанесением точек одинакового размера, потребуется ячейка размером не менее 3 x 3 и 7 x 7 точек соответственно, а значит, полученное изображение неизбежно будет иметь заметную блочность.

Аналогичная технология, разработанная фирмой Calcomp, известна под торговой маркой CristalJet. Несмотря на то, что при струйно-пузырьковом методе печати регулировать размер капли чернил значительно сложнее, такие технологии в последние год—два все же начали появляться. Примером может служить технология PhotoRetII фирмы Hewlett-Packard. Фирма Canon назвала свой метод "технологией модуляции капли" (Drop Modulation Technology). Суть всех этих методов сводится к одному — регулирование размера и местоположения (точность позиционирования) каждой капли чернил. Это дает ощутимые результаты. Принтер HP690 — шестицветный, а HP720 — четырехцветный. Их номинальная разрешающая способность одинакова, 600 x 300 dpi. Казалось бы, первый скорее способен дать фотографическое качество, но HP720, в отличие от более старой модели HP690, работает по технологии PhotoRetII и дает значительно более высокое качество фотопечати (журнал PC Magazine удостоил его оценки "Редакция советует").

Если же мы возьмем две модели, печатающие по одинаковой технологии, то шестицветный принтер, конечно, будет иметь преимущество перед четырехцветным. Ранее приводился пример с моделями HP670 и HP690. Так же различаются две модели фирмы Lexmark — 7000 и 7200. Оба принтера дают очень высокое разрешение, 1200 x 1200 dpi, и, соответственно, очень высокое качество. Отпечатанные диаграммы, технические фотографии можно рассматривать в лупу, никаких дефектов вы не заметите. Пейзажные фотографии также получаются очень качественными. Но шестицветный Lexmark 7200 — "принтер для белых людей". Он имеет значительное преимущество при печати портретных фотоснимков.

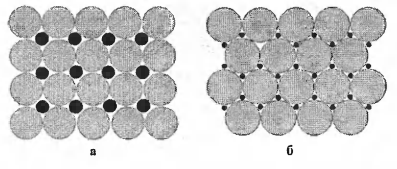


Рис. 1. Пример изображения, получаемого нанесением точек разных размеров.

Пьезоэлектрическая технология способна дать более качественную печать, чем струйно-пузырьковая. Четырехцветные принтеры Epson Stylus 400, 600 и 800 дают исключительно высокое качество цветной печати (последний из них PC Magazine также удостоил отличия "Редакция советует"). До недавнего времени фирма Epson довольствовалась этим, однако за последние два года качество печати струйно-пузырьковых принтеров резко возросло. Фирма стала более осторожна: по ее оценке качество печати — всего лишь "близкое к фотографическому". Для настоящей фотографической печати были все-таки разработаны шестицветные принтеры — Epson Stylus Photo и более поздняя модель Epson Stylus 700.

Но все же субъективные оценки качества печати не всегда совпадают с объективными. Так, HP720, несмотря на "ошеломляющее" качество получаемых фотографий, по объективным тестам находится на одном из последних мест. Качество точки плохое, разрешение и четкость — приемлемые. Пьезоэлектрические принтеры, напротив, дают хорошие результаты по всем объективным тестам. Но раз так, следует ли вообще считаться с объективными критериями? Ведь нужен-то конечный результат! Следует. Такие достоинства, как высокое качество точки и линии, четкость, разрешение непременно понадобятся, как только вы перейдете от любительских фотографий к профессиональным.

Универсальный или специализированный

Большинство упомянутых выше принтеров относится к универсальным устройствам. Основное назначение Epson Stylus 600 и 800, Lexmark 7000 и 7200, HP 690 и 720 — печать текстов, деловой графики. Печатать фотографии они, разумеется, тоже могут, и достаточно хорошо. Но существуют специализированные принтеры, которые предназначены главным образом для печати цветных фотографий.

Кроме упомянутых Epson Stylus Photo и Epson Stylus 700, к специализированным фотопринтерам относится HP Photosmart. Все они печатают гораздо медленнее, чем универсальные принтеры, и их рекомендуется использовать только для печати фотографий, но не документов. Строго говоря, универсальные принтеры фотографии тоже печатают медленно. В рекламе и технической документации приводится максимально достижимая скорость печати в черновом режиме. Для печати фотографии с максимальным разрешением принтеру может понадобиться несколько минут.

Может показаться, что технология цветной печати действительно достигла того предела, за которым дальнейшее совершенствование уже невозможно. Да, технологии струйной печати доведены до совершенства, близкого к максимальному. Однако существуют и иные

технологии печати, позволяющие вообще отказаться от псевдосмешения и избежать всех связанных с ним трудностей и ограничений.

300 = 2400?

В рекламных изданиях можно встретить такую строку:

Olimpus P-300, фотопринтер, 300 dpi = 2400 dpi струйного принтера.

Что это — рекламный трюк? Нет. Причудливая арифметика фирмы Olimpus — всего лишь количественное выражение тех характеристик, которыми обладают специализированные фотопринтеры. Прежде, чем перейти к сублимационной и термовосковой технологиям цветной печати, кратко остановимся на лазерной, хотя именно для печати фотографий она подходит в минимальной степени.

Лазерные принтеры используют электрофотографическую технологию. Печатаемое изображение наносится на фоторецепторный барабан — металлический цилиндр, покрытый слоем светочувствительного полупроводника. Рядом с фотобарабаном находится коронирующий провод, тонкая проволока, на которую подается высокое напряжение. С провода на барабан стекает отрицательный электрический заряд, и барабан электризуется. Лазер при помощи системы линз и зеркал (отклоняющая система) освещает отдельные участки барабана, и электрический потенциал засвеченных участков изменяется. Частицы красящего вещества (тонера) поступают из картриджа на поверхность другого барабана, девелопера. При его вращении частицы отрываются и притягиваются к фотобарабану в засвеченных местах. Так на поверхности барабана получается изображение. Чтобы перенести это изображение на бумагу, ее надо зарядить положительно, и при соприкосновении с барабаном частицы пристают к бумаге. Когда бумагу нагревают, частички тонера расплавляются и намертво прилипают к бумаге, после чего изображение уже нельзя стереть или смыть, так как связующее вещество тонера не растворяется ни в воде, ни в растворителях.

Тонер лазерного принтера представляет собой электризующийся порошок, состоящий из красителя и легкоплавкого связующего. Поскольку краситель может быть любого цвета, нетрудно получить тонеры всех используемых цветов — пурпурного, голубого, желтого, черного. Цветная лазерная печать становится делом техники — три или четыре фоторецепторных барабана, точное бумагопротяжное устройство, обеспечивающее совмещение всех изображений, вот и все. Но самое важное то, что при таком способе печати точки можно совмещать, то есть в каждую точку наносить краситель не одного какого-то цвета, а нескольких.

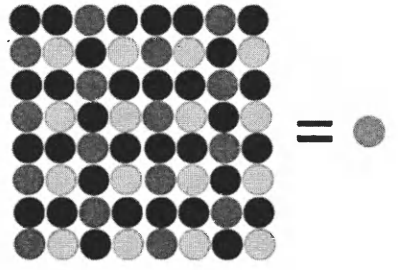


Рис. 2.
Ячейка псевдосмешения 8 x 8 точек.

Получается не псевдосмешение, а самое настоящее смешение красителей. В отличие от двухуровневого смешения (bilevel dithering), используемого в струйниках, этот способ называют многоуровневым смешением (multilevel dithering). Иногда используют другое название — contone. Мало того, точки могут различаться по размерам, а значит, интенсивность каждого цвета можно варьировать. Пределы изменения размера точки (количества тонера, наносимого на фотобарабан в каждой точке) могут быть довольно широкими.

Вот пример. Цветной лазерный принтер Xerox DocuPrint C55mp имеет 16 цветовых уровней; количество красителя в точке варьируется от 1 до 16. Он способен выводить более одного оттенка в каждой точке, но не несколько миллионов. При печати все равно приходится использовать приемы псевдосмешения, однако в режиме contone это менее заметно. Принтер способен работать в различных режимах, и если отпечатать изображение с разрешением 600 x 600 dpi в обычном режиме и с разрешением 600 x 300 dpi в режиме contone, во втором случае качество будет значительно лучше, а значит, возрастет ***эффективное разрешение***.

Именно за счет увеличенного эффективного разрешения 300 точек на дюйм фотопринтера Olimpus оказываются равны 2400 точкам струйника. В самом деле, если каждая точка фотопринтера будет содержать столько же оттенков, сколько ячейка псевдосмешения струйника размером 8 x 8 точек, то получится, что 300 x 8 = 2400! (рис. 2).

Сублимационные, термовосковые и прочие

Большая группа технологий печати известна под общим названием технологий с ***термическим переносом красителя***.

Сублимационная технология печати используется в большинстве профессиональных фотопринтеров. Суть ее заключается в следующем. Лента, на которую нанесен краситель, прижимается к бумаге и нагревается. При нагреве краситель проникает в толщу бумаги (диффундирует). Точнее, даже не в саму бумагу, а в нанесенный на ее поверхность полимерный слой. Этот слой достаточно прочен, нерастворим ни в каких растворителях и имеет глянцевую поверхность, так что изображение получается очень устойчивым и похожим на обычную фотографию.

Сублимационная технология — единственная, которая не нуждается в приемах псевдосмешения для вывода изображения. Даже если точки будут иметь фиксированный, а не переменный размер, возможность создать по 256 (!) градаций каждого из трех основных цветов позволяет получить при печати 256 x 256 x 256 > 16.7 миллионов цветов и оттенков. Этого с избытком хватит даже для самого чувствительного глаза.

Один из самых современных сублимационных принтеров — Eastmen Kodak DS 8650.

Термовосковая технология (thermal wax) похожа на сублимационную и по принципу работы, и по аппаратурному оформлению. Воск или подобное ему вещество, содержащее краситель, расплавляется при нагреве и переносится на бумагу с полимерным покрытием. Этот способ может дать до 64 оттенков каждого цвета; в результате получается 64 x 64 x 64 > 260 тысяч цветов. Это тоже немало, но при печати фотографий может оказаться недостаточным. Поэтому термовосковые принтеры тоже используют псевдосмешение. В качестве примера можно привести принтеры Fargo Pictura 310e и Tally SpectraStar 280. До появления последних моделей струйных и сублимационных принтеров термовосковые обеспечивали наиболее высокое качество фотографической печати. Однако сейчас эту технологию считают устаревшей.

Тем не менее, и она продолжает совершенствоваться. Фирма Alps Electric разработала модификацию термовосковой технологии, названную ***Micro Dry***. Вместо воска здесь используется краситель на основе полимерной смолы. Принтер Alps MD-2300 может работать в двух режимах — сублимационной печати и Micro Dry при стандартном разрешении 600 x 600 и максимальном — 1200 x 600 dpi.

Другое направление совершенствования термовосковой технологии — технология с переменным размером точки. Она была разработана фирмой Mitsubishi и используется в принтере Tally SpectraStar T8050.

Принтеры с твердым красителем существуют в двух вариантах — традиционном и барабанном. В первом случае твердый воскообразный краситель расплавляется и разбрызгивается на бумагу так же, как раствор красителя в обычном струйнике. Во втором краситель сначала наносится на барабан, который потом прокатывается по бумаге. По первому принципу работает Tektronix Phaser 300X, а по второму — Tektronix Phaser 380.

Все эти принтеры могут печатать на обычном листе бумаги формата A4 (210 x 297 мм) или Legal (210 x 355 мм). Принтеры Tektronix рассчитаны на больший формат — до 323 x 457 мм. Они используются и для печати фотографий, но не только. Основное их назначение — графические и дизайнерские работы.

Принтеры для печати на фотокарточках — не столько профессиональные, сколько узкоспециализированные. Один из них, Aztech DPD-100, печатает на карточках размером 148 x 100 мм и обеспечивает разрешение 640 x 480 точек. Но не точек на дюйм! 148 миллиметров по вертикали заполняются 640 точками, получается менее пяти точек на миллиметр или немногим более ста на дюйм. Поскольку он дает непрерывный спектр тонов, этого хватает. Точки можно заметить лишь при очень внимательном разглядывании. Чтобы отдельные точки были незаметны, необходимо разрешение не менее 7—10 точек на миллиметр. Упоминавшийся Olimpus P-300, который дает 300 точек на дюйм (12 на миллиметр) без каких-либо признаков псевдосмешения, вероятно, наилучшая из моделей фотопринтеров, имеющихся в широкой продаже.

Вот теперь мы рассмотрели все типы принтеров, пригодных для печати фотографий.

Сам себе доктор

CD-ROM

Самое неприятное, что может случиться с компакт-диском, это царапина. Причем, если царапина идет поперек дорожки, это еще полбеды. Некоторые приводы CD-ROM способны не только пропустить такую царапину, но и восстановить путем экстраполяции информацию с поврежденного места. Если царапина идет вдоль дорожки, это может привести к "нечитаемости" отдельных участков диска.

Лучше всего, конечно, постараться диск не царапать, но если это все же случилось, владелец диска обычно старается как-то восстановить информацию. И тут народные умельцы предлагают применить простое средство — зубную пасту.

Считается, что если заполировать царапину зубной пастой, то диск снова станет читаемым. Возможно, но навряд ли. Чтобы заполировать царапину, необходимо снять слой пластмассы, равный глубине этой самой царапины. При полировке оптики (что в данном случае почти то же самое) применяют абразивы, поочередно с различными размерами зерна. Зубная паста состоит из маленьких комочков разных размеров, и по сути царапину она не заполирует. Просто вместо одной царапины возникнет множество мелких. Естественно, в конечном счете все зависит от того, какая зубная паста, чем ее втирать, как долго, насколько равномерно и т.д. Не исключено, что диск после этой операции начнет читаться, но товарный вид он потеряет окончательно и бесповоротно. Необходимо также помнить, что при глубоком повреждении защитного слоя может начаться окисление алюминия, на котором записана информация, и диск "развалится" окончательно.

Так что лучше использовать специальные составы для восстановления диска (например, фирм Verbatim, TDK и др.), у которых показатель преломления/отражения такой же, как у пластмассы диска, и которые не полируют царапины, а равномерно заполняют их собой, после чего загустевают. Царапину на диске CD-ROM воспринимает как ошибку и пытается перечитать заново, а замазанное место — как участок диска без информации. Так что, данные составы позволят вам сэкономить не только время, но и нервы.

Исповедь вирмейкера

Сергей Янин

Сделал гадость — сердцу радость

Подогреваемый прессой интерес к компьютерным вирусам стал причиной того, что даже люди, впервые севшие за компьютер, сразу же спрашивают: "А как создать собственный вирус?". Они считают, что вирус — это вершина компьютерного мастерства и что если ты написал вирус, то ты крут. Им не терпится как можно быстрее стать "вирмейкерами" — создателями вирусов. Пускай в их первом вирусе будет много ошибок, пускай он не выводит никаких спецэффектов, главное — создать нечто, что можно назвать "вирусом", гордо ударив при этом себя пяткой в грудь. Обычно их опыт вирмейкерства заканчивается сразу, как только первая же жертва (чаще всего близкий друг) узнает, кто создал ту заразу, которая грохнула у него на компьютере любимую игру вкупе со всеми остальными файлами.

Есть люди, которые всю жизнь пытаются сделать то, что могут сделать очень немногие, а другие не могут вовсе. Кто-то пытается покорить горы, кто-то морские глубины, а кто-то пишет вирусы. Эти люди одержимы одной идеей — они хотят самоутвердиться. Как правило, все

* * *

Во многих CD-ROM со временем ухудшается качество чтения дисков. После протирания линзы с помощью специального чистящего диска CD-ROM Cleaner или поворота подстроечника (и, следовательно, изменения тока на головке) качество чтения восстанавливается, но через полгода—год опять начинаются те же проблемы.

Линза — это лишь малая доля оптической системы, большая ее часть расположена в глубине аппарата. А, как известно, загрязнение любой части оптической системы ведет к нарушению ее работы. Поэтому проблема скорее всего кроется в загрязнении именно внутренней оптической части, а не линзы. Подъемом тока лазера удается "пробить" помутневшую оптику, но со временем все возвращается на круги своя.

Единственное лечение в этом случае одно — чистка ВСЕЙ оптики, однако на большинстве моделей CD-ROM это очень непросто: сбивается юстировка или нарушается полупрозрачное зеркальное напыление, а дальше... разве что на помойку.

Вывод напрашивается сам собой: на периферии лучше не экономить, а покупать устройства известных, проверенных фирм.

* * *

Иногда CD-ROM начинает вести себя непонятно и неприятно. Если в "кармане" долгое время находится диск, при попытке его извлечь, нажав на кнопку выдачи, лампочка наличия диска гаснет и устройство перестает откликаться — "молчит" даже при перезагрузке операционной системы и начинает работать только после включения/выключения компьютера. После этого CD-ROM работает некоторое время, а потом может выключиться, потухнув всеми лампочками, сам по себе.

Не вдаваясь в конструктивные особенности, так сказать на бытовом уровне, можно предположить, что неприятности начинаются при перегреве нижней части корпуса устройства. "Лечение" — соответствующее. Первым делом надо переставить CD-ROM в верхний отсек корпуса или винчестер в нижний (иными словами, "разнести" их в пространстве), а также отдалить CD-ROM от других источников тепла. Ну, а в "клинических" случаях можно попробовать приладить на нижнюю сторону CD-ROM дополнительный вентилятор охлаждения (например, кулер от процессора). Не панацея, конечно, но иногда помогает.

Кирилл Кириллов

они молоды и амбициозны. В конце концов одни срываются со скал, другие захлебываются, а третьи попадают в тюрьму.

Однако такой подход пропагандируется фильмами, книгами и прочими художественно-компьютерными произведениями. На самом деле, если ты написал вирус, то это вовсе не значит, что еще через месяц работы у тебя появится счет в швейцарском банке с кругленькой суммой. Именно поэтому, разочаровавшись в вирусах, многие и начинают просто делать подлости и гадости всем, кого встретят на просторах компьютерных сетей, а иногда и своим близким друзьям. Суть их интересов становится ясна без всяких вирусов.

С трудом открыв глаза часов в двенадцать дня, студент N начинает вспоминать события вчерашней вечеринки. После пятой неудачной попытки дотянуться до почти пустого бокала ему это удается, и он с жадностью допивает остатки мутной жидкости. У него появляется желание добраться до умывальника, но стул, стоящий около компьютера, оказывается, как назло, ближе. N протягивает дрожащую руку к заветной клавише "POWER", смахнув с мышиного коврика недоеденный бутерброд, и начинает искать на диске свою любимую игру.

Через пять минут N убеждается, что компьютерные монстры гораздо умнее его, выходит из игры и думает, чем бы еще заглушить головную боль. Тут ему в голову приходит поговорка: "Не главное, чтобы гора упала с плеч; главное, чтобы при падении она придавила соседа!" Поскольку N не в состоянии что-либо соображать, он берет уже готовый алгоритм, вписывает в него свою новую кличку, компилирует и отсылает по электронной почте очередному "клиенту". Все это он проделывает с отработанной года за три точностью.

Вот и ответьте теперь мне на вопрос: "Зачем пишут вирусы?"

Вам это надо? Ну что же, терзайте! Но учтите, что люди, которые получат вашего "домашнего питомца" в подарок, могут в конце концов найти вас и прийти к вам домой, и реальный, а не виртуальный Mortal Combat вам гарантирован.

Пособие для начинающих вирмейкеров

Для того, чтобы написать вирус, вовсе не надо изучать языки программирования высокого уровня. Чаще всего из-за такого подхода вирусы и получаются громоздкими и неработоспособными. Уж если вам так хочется написать вирус, то пишите его профессионально, с чистого листа, а не сливая в один файл куски разных вирусов. Во-первых, ничего хорошего из этого не выйдет, а во-вторых, вас просто засмеют в кругах вирмейкеров за такую халтурную работу.

Чтобы не повторяться, советую прочитать полностью описание известных вирусов. К примеру, подобный файл есть в поставке DRWEB'а. Даю гарантию, что там вы увидите свою идею, уже готовую и действующую.

Типы вирусов

Вирусы делятся на два основных типа: резидентные и нерезидентные. Резидентные вирусы "садятся" на одно или несколько прерываний вашего компьютера, после чего ждут нужного им события, чтобы исполнить свою работу. Нерезидентные вирусы активизируются после того, как пользователь запустит инфицированный файл.

Нерезидентные вирусы

Эти вирусы написать довольно просто. Данный тип немногочислен и не отличается таким широким спектром диверсий, как у резидентных вирусов. Чаще всего это первенцы начинающих вирмейкеров, и поэтому используют довольно примитивный метод заражения — перезаписывают свое тело поверх инфицируемого файла, хотя существуют и такие вирусы, которые заражают файлы корректно. Нерезидентные вирусы пытаются произвести сразу много действий, так как во второй раз инфицируемый файл вряд ли запустят, а скорее удалят, да еще и антивирусом прогонят. К тому же пользователь не так часто запускает много файлов, а для того, чтобы сильно заразить систему, надо инфицировать их как можно больше. Яркие представители этого типа: Abraxas.1304, Als.335, HLLC.Chainik, NoRemorse.1319, Witching.1400.

Резидентные вирусы

Это более продвинутая модель вируса. Не всегда при запуске инфицированного файла такой вирус пытается что-нибудь натворить. Оставаясь резидентным, он перехватывает нужное прерывание. Резидентных вирусов подавляющее большинство, и они совершают самые разнообразные диверсии, начиная от безобидного мигания экрана и кончая уничтожением всей информации в определенное время.

Объекты заражения

Вирусы заражают все исполняемые файлы (*.EXE, *.COM и т.п.), а также документы текстового редактора Microsoft Word (*.DOC) — в документах этого формата есть возможность создавать макросы. Кроме того, заражению подвергаются загрузочные сектора винчестера и дискет.

Принцип заражения

Взяв управление на себя, вирус ищет на всех доступных дисках (иногда только на дисках A: и C:, если создателю лень было написать функцию определения всех доступных дисков в системе) определенное количество файлов, заражает их, выводит какое-либо сообщение для устрашения пользователя и передает управление зараженной им программе. После появления программируемого BIOS некоторые вирусы пытаются в первую очередь заразить именно его — ведь, как известно, BIOS энергонезависима, и вирусу можно будет не впадать в "спячку" до следующего включения

компьютера. Однако практически у всех вирусов это не получается, так как определенного стандарта на BIOS нет, и хорошо такой вирус работает только на компьютере хозяина. Существуют вирусы, которые ничего не выводят на экран и ничего не разрушают, а только занимаются саморазмножением.

Некоторые резидентные вирусы заражают файлы иначе: когда пользователь открывает файл нужного типа и/или запускает исполняемый файл, вирус заражает именно его. Загрузочные сектора вирус пытается заразить сразу, как только получает управление. Это обеспечивает ему гарантированную возможность получить управление при запуске компьютера.

Приемы сокрытия своего присутствия

Вирус довольно просто обнаружить путем элементарного просмотра файла. Поэтому некоторые вирусы скрывают свое присутствие в системе. Это так называемые Stealth-вирусы. Являясь резидентом, такой вирус контролирует открытие каждого файла и, видя вперед пользователя свое тело в файле, удаляет его, а во время операции закрытия файла вновь восстанавливает.

Многие полиморфные вирусы шифруют свое тело разным образом, что позволяет вирусу иметь больше "лиц" и повышает его устойчивость к уничтожению. Некоторые вирусы пытаются не изменять размер зараженного файла, оставляя его работоспособным. Если вирус и изменяет размер файла, то на минимальную величину, чаще всего на 600—800 байт. Чтобы скрыть свое присутствие, вирусы пытаются оптимизировать код инфицируемой программы и записать на освободившееся место свое тело. Одну из лазеек для вирусов сделала всеми любимая фирма Microsoft. Тот участок программы под Windows, который выводит сообщение "This program cannot be run in DOS mode" (при запуске этой программы из-под DOS), довольно большой, и, оптимизировав его, можно записать на освободившееся место тело вируса, не изменив размер файла.

Некоторые вирусы идут в своей защите еще дальше и препятствуют действию антивирусов. Способы разнообразны: от простого завешивания системы во время попытки обнаружения вируса до уничтожения программы-антивируса.

Любой вирус довольно сложно излечить без потери информации. Нужен антивирус, который "знает" этот вирус. Именно поэтому новые вирусы, еще не известные антивирусам, могут безнаказанно "плодиться" по винчестеру.

Инструментарий

Многие начинающие вирмейкеры задают вопрос: "А на чем их пишут, эти вирусы?" Ответ довольно прост — конечно, на ассемблере. Этот язык дает возможность делать исполняемые файлы маленького размера и открывает доступ ко всем ресурсам компьютера. Правда, есть такие индивидуумы, которые пишут вирусы на языках высокого уровня, объясняя это тем, что им лень выводить строку текста на экран на ассемблере. Притом в основном они пишут на Паскале. Вирус получается громоздким, 2—3 Кб как минимум. К тому же он довольно медленно работает. Таким "умельцам" просто лень учить ассемблер. Точнее говоря, разобравшись в нем немного, они понимают, что для работы с ним надо еще знать все прерывания и т.п., а посему быстро сматывают удочки. Уж если на то пошло, надо использовать связку Си-Ассемблер. Профессионалы же используют только ассемблер, к тому же перепробуют компиляторов пять, пока найдут тот, который делает наименьший размер исполняемого файла. На Паскале вирусы чаще всего если и получаются работоспособными, то обладают очень малым набором функций. Они могут разве что уничтожать файлы с расширением *.asm, чтобы испортить немного крови ассемблерщикам. Правда, те тоже хороши и не раз устраивали охоту на файлы с расширением *.pas.

Написать хороший вирус можно только полностью зная устройство компьютера, а не выпрашивая у друзей алгоритмы — как заразить файл, как "сесть" на прерывание и т.п. Советую почитать книжки наподобие "MS-DOS для программиста" или что-нибудь похожее, где рассказывается об устройстве FAT-таблицы, BOOT-секторов и прочего. Вы получите более чем полный инструментарий для создания вируса.

Писать вирусы — дело неблагодарное, трудное и к тому же опасное. Но интересное. Вам будет приятно сознавать, что где-то кто-то громко ругает вас (точнее — ваш псевдоним). А до того момента, как это произойдет впервые, вы будете ежечасно звонить другу и спрашивать, как ведет себя его компьютер, не пропала ли FAT-таблица и т.п., и через несколько часов ваш БЫВШИЙ друг сообщит, что идет к вам слушать ваши предсмертные вопли...

Николай Богданов-Катьков

Болезнь ювелиров

В средние века появился термин "болезнь ювелиров". Люди этой профессии проводили по много часов сидя. К тому же, поскольку ювелирная работа требовала "ювелирной точности" и значительного усилия кисти и пальцев, они постоянно находились в напряжении. Это порождало целую группу заболеваний — различные виды артритов, сосудистые нарушения, синдром канала запястья. Примерно тем же страдали представители другой распространенной тогда профессии — переписчики книг. И не только они. Когда знаменитый французский философ и математик Рене Декарт обратился к врачу с жалобами на онемение руки, возникающее при долгой работе, тот посоветовал ему меньше писать и больше заниматься фехтованием и верховой ездой.

Воздействие компьютера на организм человека в последнее время стало одной из самых распространенных тем в компьютерной прессе. Со всеобщей компьютеризацией связано не только широкое распространение целого ряда профессиональных заболеваний, характерных для работников "сидячих" профессий. Появляются и новые, ранее неизвестные виды психических и психофизических патологий. Мало того, компьютер способен очень сильно воздействовать на интеллектуальные способности человека.

Сделать компьютер абсолютно безопасным для пользователя так же невозможно, как и сконструировать автомобиль, не способный задавить пешехода. Однако время идет, санитарные органы различных государств принимают нормативы, которые призваны обеспечить безопасность (хотя бы относительную) работников всех профессий. Есть такой норматив и в России. Это Санитарные правила и нормы — СанПиН 2.2.2.542-96. Его полное название "Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы".

Этот основательный документ охватывает практически все аспекты работы на ПК, регламентирует массу требований, многие из которых на первый взгляд кажутся непонятными и ненужными. Чего стоит, например, детальное описание кресла работающего! Но за каждым требованием, за каждой цифрой стоят не только серьезные исследования, но и опыт нескольких столетий. Главная задача этого норматива — максимальное уменьшение вредного воздействия на человека так называемых факторов риска.

Профессиональные заболевания пользователей ПК можно разделить на следующие группы:

— заболевания опорно-двигательной системы;

— заболевания сердечно-сосудистой системы;

— глазные заболевания;

— заболевания нервной системы, периферической и центральной.

Кроме того, встречаются неспецифические заболевания, которые нельзя определенно связать с конкретными факторами риска, такими как длительное пребывание в сидячем положении, рентгеновское и электромагнитное излучение и т.п.

Синдром застоя

При любом движении мускулы периодически сокращаются и расслабляются, что ускоряет кровообращение. При усиленном кровообращении мускулы получают больше кислорода, что позволяет им вырабатывать больше энергии (химической), которая снова расходуется на механическую работу.

Но это при движении. Если человек стоит на месте, он не совершает работы, но его мускулы находятся в состоянии статического напряжения. Это означает, что процесс вырабатывания энергии в мускулах замедляется и, как следствие, усталость наступает гораздо быстрее.

Хуже другое — уменьшение кровотока со временем приводит к необратимым изменениям сосудистой системы. Самое известное из них — варикозное расширение вен, профессиональное заболевание продавцов, парикмахеров — всех тех, кому приходится подолгу стоять (именно стоять, а не ходить).

Другая группа сосудистых заболеваний — склеротические изменения — не связана напрямую с неподвижностью. Отложение холестерина на стенках сосудов начинается при нарушении обмена веществ. Но если кровоток замедлен, этот процесс резко ускоряется. Статические нагрузки на позвоночник возникают при длительном сидении в одной позе, особенно напряженной. Профессиональное заболевание машинисток — остеохондроз — характеризуется истончением межпозвонковых хрящей и отложением кристаллов солей. При этом снижается гибкость позвоночного столба и появляются боли при движении.

Эргономика в цифрах

Что можно предусмотреть для максимального уменьшения застойных явлений? Разумеется, оборудовать рабочее место так, чтобы можно было сидеть, не напрягаясь. Это называют "рациональной рабочей позой". А еще? Заставить человека двигаться, хотя бы время от времени.

Вот какие требования предъявляет СанПиН к рабочему креслу:

Рабочий стул (кресло) должен быть подъемно-поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также — расстоянию спинки от переднего края сиденья. Конструкция его должна обеспечивать:

— ширину и глубину поверхности сиденья не менее 400 мм;

— поверхность сиденья с закругленным передним краем;

— регулировку высоты поверхности сиденья в пределах 400—550 мм и углов наклона вперед до 15° и назад до 5°;

— высоту опорной поверхности спинки 300 + 20 мм, ширину — не менее 380 мм и радиус кривизны горизонтальной плоскости — 400 мм;

— угол наклона спинки в вертикальной плоскости в пределах 0 + 30°;

— регулировку расстояния спинки от переднего края сиденья в пределах 260—400 мм;

— стационарные или съемные подлокотники длиной не менее 250 мм и шириной 50—70 мм;

— регулировку подлокотников по высоте над сиденьем в пределах 230 + 30 мм и внутреннего расстояния между подлокотниками в пределах 350—500 мм.

Рабочее место должно быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

Зачем нужно так много подробностей? Ответ на этот вопрос дает другой пункт норматива:

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ВДТ и ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) должен выбираться в зави-

Минздрав предупреждал...

Санитарные нормы с длинным названием "Гигиенические требования к видеодисплейным терминалам и персональным электронно-вычислительным машинам и организации работы с ними" — документ серьезный, детально разработанный. Он ежегодно обновляется и дополняется, а это говорит о том, что о несчастных юзерах и программерах помнят и заботятся.

Вероятнее всего сей важный документ предназначен не только для заботливых работодателей, которые только и мечтают о том, чтобы сделать жизнь своих сотрудников поистине райской, но и для осторожных компьютеровладельцев, старающихся уберечь свое здоровье и здоровье своих близких от пагубного влияния ВДТ и ПВЭМ. И им бы это удалось, если бы они сумели воплотить в жизнь эти в высшей степени человеколюбивые инструкции. Но, увы, все не так просто — попробуйте, к примеру, сказать ребенку младшего школьного возраста, что ему положено играть на компьютере не больше 10 минут в день, и вы сами в этом убедитесь.

Впрочем, не соответствующее СанПиН использование домашнего компьютера не может повредить никому, кроме его владельца, поэтому я не буду касаться этой категории пользователей. Моей целью было выяснить, в каких условиях работают люди, по своей профессии связанные с использованием компьютера. Путем телефонного опроса мне удалось получить сведения об условиях труда программистов и операторов в 20 государственных и частных питерских предприятиях.

Выяснился отрадный факт: 45% опрошенных слышали о существовании "Гигиенических требований...", 40% их даже читали, и лишь 15% вообще не подозревали о существовании такого полезного документа. Уда-

симости от характера и продолжительности работы с ВДТ и ПЭВМ с учетом роста пользователя.

В самом деле, когда человек начинает уставать, он принимается двигаться, вертеться на стуле, откидываться на спинку и снова наклоняться вперед, менять высоту сиденья, угол наклона спинки. При этом статическое напряжение сменяются нормальной работой мышц и суставов.

Эти меры помогают снизить утомляемость, частично снимают статическое напряжение, но всех проблем не решат. Человек должен активно двигаться.

"Смените перо на шпагу!"

Французский медик во многом был прав: философу Декарту действительно следовало вести более подвижный образ жизни. Но по современным воззрениям движение без нагрузки снимает усталость от статического напряжения гораздо лучше, чем интенсивная физическая нагрузка, такая как фехтование. Да и едва ли редактор нашего журнала по нескольку раз в день станет фехтовать или боксировать с наборщиком. Какие еще есть способы?

Вспомните, как 8 — 10 лет назад по рабочим дням в одиннадцать утра по радио шла производственная гимнастика. В состав комплекса входили, как правило, неспецифические упражнения, которые были пригодны для людей и сидячих, и стоячих профессий. Они повышали двигательную активность, стимулировали деятельность мышечной, дыхательной, нервной, сердечно-сосудистой систем.

В санитарном нормативе даны комплексы упражнений для физкультурных пауз. Целых три. Не поленитесь, загляните.

Для особо торопливых, кому не выделить 5—10 минут для полноценных упражнений, даны более короткие комплексы — по 1—2 минуты. Кроме того, предусмотрены и комплексы специфических упражнений:

— для улучшения мозгового кровообращения;

— для снятия утомления с плечевого пояса и рук;

— для снятия утомления с туловища и ног.

Дано по четыре варианта всех комплексов.

Есть еще и комплексы упражнений для глаз (три варианта). В отличие от физкультурных пауз и минуток их можно выполнять, сидя на рабочем месте, достаточно лишь отвернуться от монитора.

Если вы будете неукоснительно выполнять все обязательные требования и рекомендации норматива как по организации рабочего места, так и по обеспечению правильного режима работы, то очень скоро почувствуете, что устаете значительно меньше. Вероятность возникновения профзаболеваний также снизится.

лось также установить, что на относительно приличных машинах имеют счастье работать 60% опрошенных. Критериями соответствия были негорелый монитор, клавиатура с не западающими клавишами и наличие хотя бы антибликового покрытия на экране (вы представляете, в каких условиях работают остальные 40%?). А что касается соответствующего СанПиН микроклимата (то есть наличия в помещении отопления, лампочки и форточки, а также не очень высокого уровеня шума и задымленности), то такими условиями были обеспечены целых 65% опрошенных. Средняя продолжительность непрерывной работы на ПК составила 8 часов в день (разброс от 3 до 12 часов). Кстати, распространенное мнение о том, что на государственных предприятиях условия труда соответствуют санитарным нормам, — не более чем миф. Они примерно одинаковые везде.

Те, кто считает, что слухи о вреде компьютера — это происки современных "луддитов", в корне не правы. В ходе опроса выяснилось, что 40% участников за время работы с ЭВМ приобрели заболевания позвоночника, у 30% ухудшилось зрение, 10% начали набирать лишний вес, у 5% появились заболевания рук и 40% заявили, что такие условия труда отражаются на состоянии их нервной системы. И это при том, что большинство опрошенных — не старше 25 лет.

В оправдание работодателей можно сказать только то, что 70% участников опроса довольны своей работой, и несоответствие условий санитарным нормам, по их мнению, вполне компенсируется содержанием труда или высокой оплатой. Такое отношение, безусловно, очень удобно для тех работодателей, которые стремятся избежать лишних, по их мнению, затрат на улучшение условий труда своих работников. Но программисты и операторы, которые соглашаются жертвовать своим здоровьем ради интересной работы и высоких заработков (а таких большинство), редко задумываются о том, что подобные жертвы могут в дальнейшем привести если не к потере трудоспособности, то, по крайней мере, к серьезным проблемам в дальнейшей профессиональной самореализации.

А ведь Минздрав предупреждал...

Ирина Давыдова

Кевин Митник, человек-легенда

Савва Мотовилов

Я из породы благородных жуликов, которым нравится раскрывать секреты. Я прочитаю ваше завещание, ваш дневник, положу их на место и, не тронув деньги, закрою сейф. Я сделаю так, что вы никогда не узнаете о моем визите. Я сделаю это потому, что это красиво, это вызов.

"The Fugitive games" о Кевине Митнике

Говоря о компьютере, мы чаще всего говорим о комплектующих, программах и прочих неодушевленных составляющих, но без человека, который за ним сидит и управляет, компьютер — лишь навороченная железяка. Среди людей, которые в то или иное время прославились в компьютерном мире, особое место занимают так называемые хакеры, ведь не будь их, возможно, процесс развития программного обеспечения и систем безопасности шел бы намного дольше. В этой статье речь пойдет о самом знаменитом человеке компьютерного мира, хакере №1 в мире, который, несмотря на свое сегодняшнее пребывание в американской тюрьме, еще не только не забыт, но и все более популярен. Это Кевин Митник. Человек, который является величайшим из хакеров, достигнув в этом деле недосягаемых высот.

Кевин Митник родился в 1964 году в Норт Хилз (США). Когда ему было всего 3 года, его родители развелись. Он жил в Лос-Анджелесе с мамой, которая работала официанткой и уделяла ребенку не так много времени. Кевин начал искать другой, более дружелюбный к нему мир, и вскоре увлекся общением в компьютерных сетях со своими сверстниками. Освоившись в новом для него виртуальном мире, он стал быстро наверстывать упущенное и уже в 16 лет совершил свой первый компьютерный взлом. Это была административная сеть школы, в которой он учился. Но Митник не стал исправлять оценки, хотя сделать это было очень просто. Ему нужно было только признание его друзей, хакеров-сверстников, среди которых он уже приобрел немалый авторитет. А меньше чем через год Кевин взломал компьютерную систему североамериканской противовоздушной обороны в Колорадо, и у него начались первые конфликты с законом. Многие его друзья тоже развлекались, например, присваивая домашнему телефону соседа номер таксофона, и каждый раз, когда хозяин поднимал трубку, голос, записанный на пленку, просил опустить 20 центов. Но это были невинные шалости в сравнении с "подвигами" Митника.

Больше всего Кевину нравилась область телефонных коммуникаций, но так как вся информация о них держалась в секрете, Митник проник в корпоративные компьютеры Pacific Bell, крупнейшей американской телефонной сети, чтобы завладеть руководствами и некоторыми специальными программами. После этого долго гулять на свободе ему не пришлось — вскоре его вместе с друзьями сдала подружка одного из членов хакерского общества. Митника приговорили к трем месяцам перевоспитания и одному году условно, но, совершив через некоторое время взлом пентагоновской сети APRANet, Кевин сел в тюрьму уже на шесть месяцев. Все эти шесть месяцев он упорно изучал материалы, добытые с таким трудом из Pacific Bell, и, выйдя из тюрьмы, знал о работе этой сети не меньше, чем лучшие специалисты Bell Labs. Он научился создавать бесплатные номера, звонить с любого номера, соединять и разъединять любых абонентов и подслушивать чужие разговоры. Он стал неуловимым Джеймсом Бондом для телефонной компании с нигде не учтенным номером, оканчивающимся на 007.

На протяжении 80-х годов Митник успешно уклонялся от встреч с властями и осел в тихом Калифорнийском городке Thousand Oaks с девушкой, с которой он познакомился на компьютерных курсах. В 1987

году Митника вновь арестовали по обвинению в краже компьютерных программ из Santa Cruz Operations. Ему дали три года условно, но уже через год снова арестовали, теперь уже за кражу компьютерного кода из исследовательской лаборатории Digital Equipment Corp. На этот раз условием освобождения были запрет на использование компьютера и модема. Тем не менее, сразу после выхода Митника на свободу стали твориться странные вещи, как то: самопроизвольные отключения телефона его надзирателя-инспектора, непонятные операции с банковским счетом судьи, а из полицейского компьютера разом исчезли все упоминания об арестах Кевина Митника.

После этих событий Митник стал вести здоровый образ жизни, скинул лишний вес и даже стал вегетарианцем, но смерть его брата в 1992 году сильно повлияла на него, и он опять занялся взламыванием сетей, ориентируясь главным образом на сети телефонной связи. В ноябре на Митника был объявлен федеральный розыск — после того, как стали известны факты пребывания Митника в секретных компьютерных досье ФБР. Однако Кевин исчез.

О нем вспомнили летом 1994 года, когда из компании Motorola кто-то скопировал программное обеспечение для контроля за сотовой связью, и техника атак, по словам специалистов, была похожа на "почерк" Митника. Власти почти замкнули кольцо поиска в ноябре, но Митник ушел и на этот раз. Полиция нашла в Сиэтле только квартиру, которую он снимал под вымышленным именем, а в ней — несколько перепрограммированных сотовых телефонов со сканером (устройством, которое позволяет перехватывать идентификационные коды сотовых телефонов, когда они выходят в эфир, после чего происходит "подсадка" на телефоны, чьи коды были перехвачены).

И вот, наконец, кульминационный момент истории о Митнике. Его самый дерзкий вызов. Произошло все 25 декабря 1994 года, в рождественскую ночь. Кевин Митник вторгся в компьютер ведущего американского специалиста по компьютерной безопасности — Цутому Шимомуры. Многие оценивают этот поступок как бессмысленный, дерзкий и непонятный, но он так же непонятен, как и вся предшествующая жизнь Митника. Когда Шимомура поехал на рождество в Неваду, Кевин проник в его домашний компьютер в Калифорнии (Солана Бич) и начал копировать зашифрованные и запа-

роленные файлы. Однако он не мог предусмотреть, что в университете Сан-Диего случайно задержится один из студентов, который и заметит изменения log-файлов на домашнем компьютере Шимомуры, продублированных на университетском сервере. Увидев непонятные изменения, студент позвонил Шимомуре, который незамедлительно приехал в Калифорнию. Пока Цутому разбирался с кражей файлов, последовал новый вызов: искаженный голос ехидно надсмехался на ним. Этого было достаточно, чтобы Цутому, человек с самурайскими понятиями о чести, поклялся найти того, кто это сделал. Затем начался долгий поиск путей, которые должны были привести к хакеру, но этих путей было очень мало, и многие из них замыкались сами на себя, так и не приведя к чему-либо конкретному. Было видно, что действовал не просто профессионал высокого класса, а виртуоз.

Атака на компьютер Шимомуры была проведена необычайно искусно. Митнику приходилось работать вслепую, так как он управлял движением данных через несколько компьютеров и не знал, доходят ли пакеты до компьютера-плацдарма (кстати, плацдармом Кевин сделал компьютер крупнейшей в штатах телекоммуникационной компании NetCom, откуда он в дальнейшем похитил полную базу данных по клиентам). Дело в том, что когда система получает пакет (TCP/IP), она посылает на компьютер-отправитель сообщение, подтверждающее получение, и только после получения такого подтверждения передача информации продолжается. Митник, не видя эти сообщения (ведь они поступали не на его на компьютер), смог, тем не менее, разгадать номера последовательностей и приписать соответствующие номера последующим пакетам. Теоретическую возможность этого предсказал еще в 1989 году Стив Белловин из Bell Labs, однако атака Митника — первый известный случай применения данной техники на практике.

Скачав файлы Шимомуры (в частности, программы обеспечения компьютерной безопасности), Митник перекинул их на бездействующий эккаунт компании The Well, предоставляющей доступ к Интернет.

27 января системный оператор The Well обратил внимание на необычно большое количество данных на эккаунте, который обычно был почти пуст. Позже техники из The Well обнаружили еще десяток используемых хакером эккаунтов, большей частью "спящих", где он хранил украденную им информацию. Среди прочего были обнаружены файлы с паролями и кодами многих компаний, включая более 20 тыс. номеров кредитных карточек, украденных из NetCom Inc.

Позже Митник, развлекаясь, вытащил из NetCom полную информацию по более чем 50 тыс. клиентам, включая номера личных и служебных кредитных карточек, адреса и номера телефонов.

Шимомура установил на компьютере, на котором были найдены украденные файлы, круглосуточный мониторинг, позволяющий фиксировать любую активность, и с помощью агентов ФБР начал вычислять приблизительное место, откуда могло

произойти нападение. После долгих расчетов была определена зона в радиусом в два километра.

12 февраля 1995 года группа из специалистов-компьютерщиков и агентов ФБР вышла в примерный район поиска — Ралейх. Члены группы патрулировали район, пеленгуя все работающие в данный момент сотовые телефоны. Они вынуждены были сохранять радиомолчание, так как опасались, что Митник прослушивает переговоры по рации. В конце концов Митника засекли.

14 февраля в 1:30 ночи, когда Митник вышел в очередной раз на связь, в дверь его квартиры постучали... Через минуту в квартире начался обыск.

Информация о Кевине Митнике после ареста очень скудна. Известно, что он сменил к октябрю 1995 года три тюрьмы, причем условия содержания в них были ужасными, а на его протесты и просьбы никто не обращал внимания. В результате 18 июня он был госпитализирован с диагнозом "спазм пищевода", а спустя некоторое время вновь водворен в восьмиместную камеру. Ему было отказано в доступе к любым средствам связи, даже простому телефону.

Митнику выдвинули 23 обвинения, большей частью в мошенничестве с использованием незаконного доступа к компьютеру и нанесении ущерба на 80 млн долларов. Суммарный срок по всем обвинениям составляет более 450 лет тюрьмы, но благодаря усилиям адвоката 22 обвинения отпали — удалось доказать, что Митник не преследовал никаких корыстных целей. Кроме того, хакер придерживался правила не хранить на своей машине данные, которые могут его изобличить. Да и вообще зашифрованные файлы с компьютера Митника специалисты-криптографы и по сей день не смогли "расколоть". Осталось только одно обвинение, за которое Митник может быть осужден на 8 месяцев.

В настоящий момент Митник все еще находится в тюрьме. Обвинители тянут с доказательствами его вины, и есть большая вероятность, что дело "рассыпется".

Друзья Митника своими средствами добиваются его освобождения. Недавно, в середине сентября, они совершили успешную атаку на электронную версию популярного в США журнала Time. Полосы издания были подменены материалами на черном фоне, содержавшими, помимо критики официальных властей, личные оскорбления с "непереводимыми" перлами местного жаргона и подобающими случаю картинками, а также угрозу расправы в отношении тех журналистов, которые, как они полагают, поддерживали контакты с Митником и "сдали" его агентам ФБР. В перечне персональных мишеней оказался также Джон Маркофф, автор нашумевшего бестселлера "Takedown", в котором детально описаны охота на знаменитого хакера, скрывавшегося "в бегах" пять лет, и его поимка.

В конечном счете, злоключения Митника можно объяснить тем, что он вторгся туда, куда ему не следовало — в игру с военными, политиками и ФБР, а у этих ведомств, как известно, все колоды крапленые. И тем не менее, исход этой игры пока еще неясен.

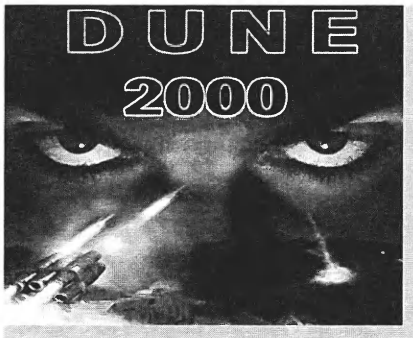
Информация о Кевине Митнике в Интернете:

http://www.gulker.com/ra/hack/ — Кевин Митник и Шимомура.

http://www.ora.com/oracom/crime/index.htm — борьба с компьютерными преступлениями.

http://www.takedown.com/ — Шимомура и Джон Маркофф.

http://www.well.com/user/jlittman — книга Джонотана Литмана "The Fugitive Game" о Кевине Митнике и других хакерах.



Осторожно, вирус!

Вряд ли сейчас найдется геймер, который не знает о существовании одного из самых популярных игровых жанров — RTS (Real-Time Strategy, стратегия реального времени).

В 1992 году уже достаточно известная в то время фирма Westwood Studios создала игру Dune 2 (предыдущая ее версия, Dune, не являлась RTS). Ее сценарий был написан на основе нашумевшего цикла книг Фрэнка Херберта "Дюна". Так родился новый жанр...

После успеха "Дюны 2" Westwood Studios выпустила известные RTS Command & Conquer с Covert Operations (дополнительными операциями) и Command & Conquer: Red Alert, но огромное количество фанатов Dune 2 завалили офис компании Westwood письмами с просьбой продолжить "Дюну"... И вот, в конце 1997 года началась разработка Dune 2000, и сейчас игра попадает к фанам, так долго ее ожидавшим, в том числе и российским.

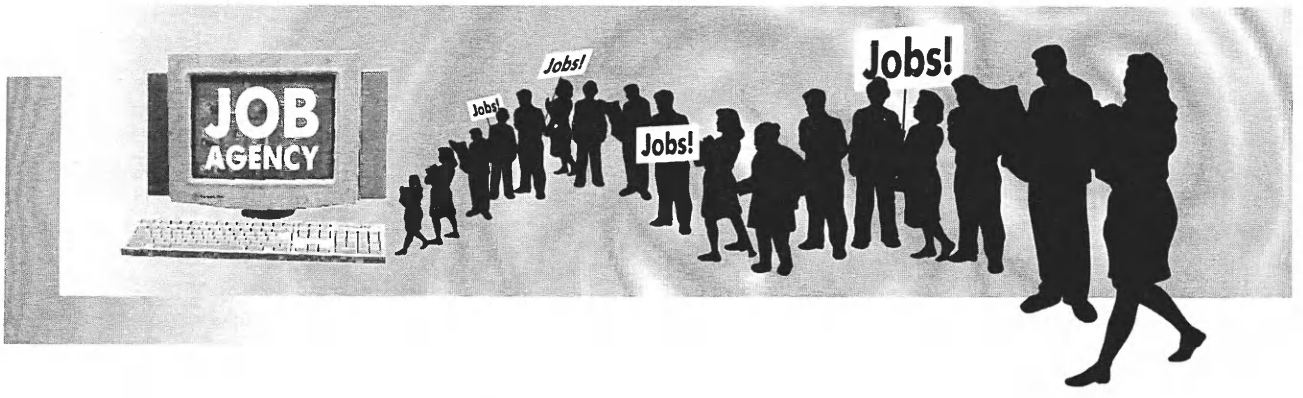
Ну, с Западом все понятно. Красивые коробочки, дорогие, но лицензионные диски с буклетами, гарантией и т.д. До нас же дошли "пиратские" копии, но не в совсем традиционном исполнении. Практически все продаваемые сейчас CD-ROM с Dune 2000 заражены вирусом Win95.CIH. Правда, зараженными оказались не основные файлы, а только обеспечивающие мультиплеер и поддержку DirectX.

Чтобы снять все вопросы, приведу список зараженных файлов, выданный AVP32

list of infected files:
x:\DXSETUP\DIRECTX\DDHELP.EXE
обнаружен вирус Win95.CIH
x:\DXSETUP\DIRECTX\DPLAYSVR.EXE
обнаружен вирус Win95.CIH
x:\DXSETUP\DIRECTX\DXINFO.EXE
обнаружен вирус Win95.CIH
x:\DXSETUP\DIRECTX\DXSETUP.EXE
обнаружен вирус Win95.CIH
x:\DXSETUP\DIRECTX\DXTOOL.EXE
обнаружен вирус Win95.CIH
x:\SETUP\REGSVR32.EXE
обнаружен вирус Win95.CIH

Будьте осторожны!!!

Кирилл Кириллов



Поиск работы в Интернет

Андрей Самсонов

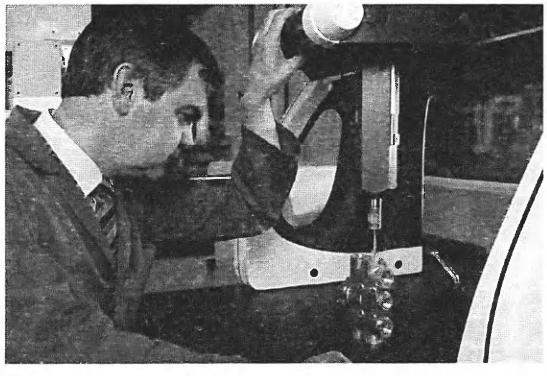
— Ну, а вы-то что здесь делаете?
— Кто, мы? Да мы тут работаем!
(из жизни)

Все люди делятся на мужчин и женщин, на автомобилистов и пешеходов, на первых и вторых, а также на тех, у кого есть работа и у кого ее нет. Последние, в свою очередь, подразделяются на две неравные части: меньшинство, которых такое положение устраивает, и большинство, которых это не устраивает и которые ищут. Умные люди говорят, что искать лучше всего по знакомству, и я, поскольку себя дураком не считаю, с ними совершенно согласен. Но если вы не можете воспользоваться этим, наиболее простым способом, придется набраться терпения и погрузиться в мир лаконично-строгих и заманчиво-обманчивых частных объявлений.

Это была присказка. А сама сказка о том, как найти что-то путное в Интернете. Рабочие вакансии встречаются в "паутине" несколько реже, чем предложения стать сексуальным партнером или купить десять милых щенков от случайной любви водолаза и таксы. Но такие вакансии существуют и, при желании, работу найти можно! Даже несмотря на то, что в обычной базе данных обычного агентства по найму раздел "Ищу работу" по количеству заявок в несколько раз больше раздела "Есть работа", унывать не стоит.

Предположим, что вы душой и телом преданы нашему замечательному городу и хотели бы жить и работать именно в нем. В этом случае можно спуститься от http://www.spb.ru/000/ через "бизнес и услуги" в "агентства по найму". Перед вами открывается список из 13 сайтов (счастливое число, не правда ли?). Предлагаю вам совершить прогулку по ним, не тратя вашего драгоценного on-line времени. Первым в списке стоит Nevalink Employment Agency, он же http://www.job.spb.ru. Вы попадаете на него и из питерского сайта через "объявления" и "работу". Таким образом, это некое перекрестье всех дорог. Сразу ожидаешь многого. И, как всегда бывает, когда многого ждешь, кажется, что чего-то недодали. Впрочем, выбор имеется. На первой странице в столбик выстроились:

— резюме;
— вакансии;
— объявления;
— разное.



Вакансии существуют (от фирмы "Гранд"): в Санкт-Петербурге, в Израиле и в США, вроде, как на выбор. Как можно догадаться, наибольшее число предложений относится к славному городу СПб. Среди них вакансии: обслуживающего персонала, экономистов и бухгалтеров, менеджеров и торговых представителей, руководителей и инженеров, бандитов и проституток (прошу прощения, неуместная шутка). Если серьезно, то предложений немало, только будьте внимательны, некоторые из них могут быть с большой "бородой".

Предложения от израильских товарищей более специфичны: приглашаются домработницы, массажи-

стки, танцовщицы, официантки и разнорабочие. Специалистов других профессий, видимо, не ждут на Земле Обетованной. Другое дело — Штаты. Эта страна, как и положено флагману науки и техники, ожидает исключительно инженеров-программистов и электронщиков. Отдельное спасибо за это компании ATS Inc.

Перехожу к разделу "Объявления", среди которых изобилуют предложения для серьезных программистов о работе как тут, так и там. Например, приглашаются программеры с опытом работы в Японию. Причем, "особо отличившихся на работе в Японии Агентство в дальнейшем рекомендует на работу в США". Как говорится, Штаты — они и в Африке Штаты.

Раздел "разное" включает в себя Human Resources On-Line — сайт www.hro.ru, о котором скажу особо чуть ниже. Russian International Job Agency, ссылка на который отошлет вас прямо на www.job.ru. Спешить туда не стоит, потому что там уже начинается безраздельное господство Москвы. Не знаю, как с безработными, но количество вакантных рабочих мест в Москве, как мне кажется, вполне сравнимо со всей остальной Россией.

И, наконец, последняя ссылка отправит вас прямо на Южный Урал. Там давно уже ждет вас "Поиск и предложение работы на Уфимском интернет-рынке". Впрочем, если вы не верите, что Уфимский интернет-рынок — самый, самый... то можете пропустить эту ссылку.

Вернемся, однако, к исходному списку из 13 питерских джоб-агентств. В большинстве из них предпочтение отдается спецам с экономическим уклоном. В базе данных агентства "Dero" из 33 вакансий 14 — сбыт и снабжение, 10 — экономика и финансы. Агентство "Арес Стафф" предлагает 1 вакансию в разделе "ПК и программное обеспечение" и 0 вакансий в разделе "наука" (какая уж тут наука, господа!).

"Келли Сервисес СИ-АЙ-ЭС" (на английском) предлагает вакансии в США. Впрочем, если вы уже решили "рвать когти", то есть, допустим, вам вдруг надоели те милые шалости, которыми "развлекают" страну Большие Дяди в Кремле, вас можно понять. Для поиска работы ТАМ предлагаю просто начать с www.yahoo.com. Если вы знаете, что вам нужно, и это нужное существует в Интернете, то вы с ним (с нужным) обязательно встретитесь.

В разделе "Консультанты по подбору персонала" появляются предложения от компании "Анкор". Требуются специалисты достаточно высокого класса, но все также ограничивается, главным образом, бизнесом.

Раздел "Поиск работы" отсылает в фирму "Аксон". Там вы не найдете большого количества предложений, но зато информацию можно скачать в виде zip-файла, что вообще-то довольно удобно (побольше заботьтесь о нас, уважаемые рекламодатели в Интернете).

В обсуждаемый список под именем "Стар Лайт" входит www.hro.ru, упомянутое выше. За забавно-незатейливым оформлением в виде "пузатых" кнопок скрывается серьезный банк данных почти по всему миру. Можно найти свой любимый город в России. Я, конечно, нашел Санкт-Петербург. Всего вакансий 73, но среди них, заметьте, есть целых 2 предложения для физиков и 3 — для химиков. Ученые, очнитесь от голодного забытья, вас ищут!

Последней в списке идет газета "Биржа труда". На нее стоит обратить внимание. По крайней мере, вы сможете углубиться в подшивку номеров за весь год, что поможет вам незаметно скоротать вечерок.

Это были, так сказать, официальные источники информации. Кроме них, как известно, в Сети существует масса досок объявлений. Пренебрегать ими не стоит — вдруг вам улыбнется судьба и среди мусора вы увидите свой счастливый лотерейный билетик. По личному опыту могу сказать, я увидел его по адресу http://win-www.medport.ru/bbslist/fidonews.html. Не пытайтесь откуда-нибудь выйти на этот адрес, я и сам не знаю, как, когда и с кем я туда пришел (кстати, там есть очень актуальная информация про "зеленых человечков"). Главное, что вышеуказанный адрес дает информацию по Питеру, в отличие, скажем, от рекламируемого www.ks-co.ru/~4all/, где вы видите много предложений, находите что-то подходящие и... в последний момент обращаете внимание, что речь идет о "дорогой нашей столице" (дорогой в смысле денег, конечно).

Итак, примерно понятно, в каких специалистах нуждается страна. А если все-таки вы "слуга науки верный"? Попробуйте, сходите на www.phds.org — сайт с вакансиями пост-доков. Кому это нужно, те меня поймут. Мы, правда, вначале договорились, что вам нравится наш замечательный город, но... Если совсем надоест глядеть на все это безобразие, то имейте ввиду.

Пора завершать экскурсию по "паутине". Ну что, убедил я вас, что нужно искать работу в Интернете? Если да, то вы слишком доверчивы! Не отказывайтесь от просмотра объявлений в газетах. Хотя некоторые из них не внушают доверия, попадаются и вполне пристойные. Помните, что компьютер, с точки зрения многих людей, пока роскошь, а не средство передвижения по Сети.

PS. Должен предупредить, что в последние дни перед выходом этого номера журнала количество вакансий на упомянутых мной адресах значительно сократилось. И все же — *желаю Удачи*!

Алексей Богдановский

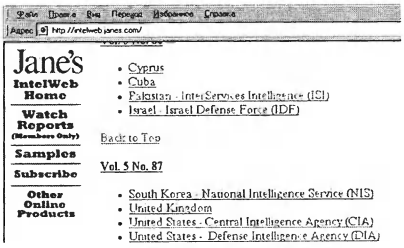
Спецслужбы в Интернет

Представьте себе, что перестали работать телевизоры и радиоприемники, отключились телефоны, не выходят газеты... Что бы мы тогда знали о мире? Почти ничего. Вот эта малость и составляет реальный мир. Все остальное — политика, войны, биржевые цены, спорт — ни что иное, как мир виртуальный. Он может быть сколь угодно похожим на реальный, но никогда не соответствует реальности полностью. Значит, достаточно чуть подкорректировать правила доступа к информации, и мы будем жить в совсем другой стране, на другой планете.

Вероятно, именно эти соображения заставили американцев в 70-е годы принять Закон о свободе информации, согласно которому граждане и общественные организации могут преследовать в судебном порядке государственные и коммерческие структуры, повинные в необоснованном засекречивании и сокрытии информации от общественности. Спецслужбы США, вынужденные заботиться о своем имидже, самостоятельно, не дожидаясь суда, стали активно рассекречивать архивы, срок давности по которым истек.

Но подлинный переворот в доступе к информации о деятельности спецслужб произошел с появлением Интернет. Если раньше рассекреченные архивы были доступны только ограниченному числу специалистов, то теперь оригиналы документов сканируют и выставляют на сервере в gif-формате на всеобщее обозрение. Если учесть, что большинство рассекреченных операций касаются советской разведки, то экскурсия по серверам американских спецслужб обещает быть довольно интересной.

Итак, дозваниваемся до провайдера и начинаем.



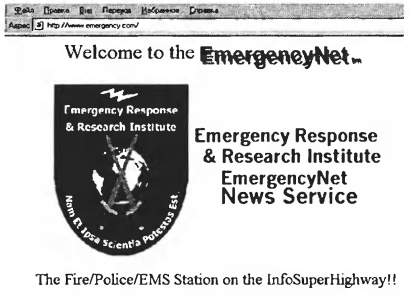
Сначала стоит сходить на негосударственный сайт http://www.intelweb/janes.com. Там есть очень недурной справочник по спецслужбам мира (в нем присутствует даже сверхсекретный израильский "Моссад" и кое-что о разведке Пакистана) и, главное, отлично рубрицированный каталог сетевых ресурсов по каждой из них. Правда, попытка ткнуть мышкой в линки часто выводит на столь тормозные пути, что вспоминается фраза Лени Голубкова: "Мы сидим, а денежки идут".

"Журнал электронной обороны" на http://www.jed.com содержит в бесплатном доступе интереснейшие статьи о средствах и методах технического шпионажа и противодействия ему, а также немало линков с производителями спецтехники. Он же выводит на несколько международных организаций. Это Центр исследования терроризма http://www.terrorism.com, содержащий подборки материалов о наиболее известных терактах, оружии, которое используют террористы, правилах противодействия угрозам, ссылки на электронные конференции. Безусловно, интересен и сайт Института исследований чрезвычайных ситуаций http://www.emergency.com. На нем вы найдете статьи и конференции по поддержанию и восстановлению бизнеса в чрезвычайных ситуациях самого разного рода — от землетрясения до гражданской войны.

Единственный в мире официальный сайт службы внешней разведки принадлежит ЦРУ: http://www.odci.gov/cia/. Подборка материалов на сервере очень велика, особенно, если учесть обильные ссылки. Наиболее интересны, конечно, представленные в свободном доступе "Бюллетень разведок" (выходит два раза в год) и ежегодник

"CIA World Factbook", ранее практически недоступные русскому читателю и содержащие информацию по разведкам всего мира. Раздел "Публикации" на сервере содержит программу поиска нужного документа по ключевому слову, что существенно облегчает работу.

Что касается рассекреченных проектов, то они в большинстве сво-



ем доступны через ссылки. Совсем недавно, кстати, появились документы по проекту "Синяя книга" ("BLUEBOOK"), касающиеся изучения аналитиками ЦРУ неопознанных летающих объектов в период 1948—1953 годов (электронная версия журнала Studies in Intelligence, vol. 1, 1997, p. 67, расположена в директории http://www.odci.gov/csi/).

Рекомендую также поискать документы по проекту "Stargate" (использование паранормальных способностей человека в интересах разведки и контрразведки, 1962—1985 гг.), рассекреченные пару месяцев назад. Начать лучше со статьи в журнале "Fate" за апрель 1996 года — http://www.fatemag.com.

Не отстает от цэрэушного и сайт ФБР http://www.fbi.gov. Ход расследований громких терактов, может быть, мало кому из россиян интересен, а вот статью про real hack дорогого земляка Володи Левина, безусловно, стоит почитать хотя бы в порядке самообразования.

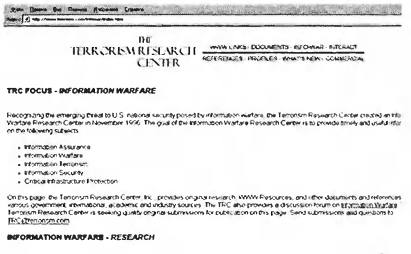
Но наибольший интерес в данный момент представляет сайт Национального агентства безопасности США (NSA) http://www.nsa.gov. Эта организация занимается примерно тем же, что и наше ФАПСИ, плюс спутниковая и радиоразведка. Материалы по текущим событиям отсутствуют, зато много архивов, в том числе виртуальная часть Музея криптографии.

Недавно на nsa.gov появилось несколько тысяч рассекреченных документов по проекту "VENONA" (http://www.nsa.gov:8080/docs/venona/). Этот проект осуществлялся совместными усилиями ЦРУ и NSA с 1943 по 1980 год и включал радиоперехват, анализ и дешифровку сообщений агентов ГРУ и КГБ СССР. Отсканированные оригиналы представлены в виде gif-файлов размером 700x900 пикселов (читаются с некоторым трудом, но разобраться можно) и дают исчерпывающее представление о деятельности русских разведчиков в стане врага, в том числе и о воровстве атомных секретов. Рискну привести сокращенный перевод пресс-релиза бывшего директора NSA Вильяма П. Кроуэла.

Проект "ВЕНОНА"

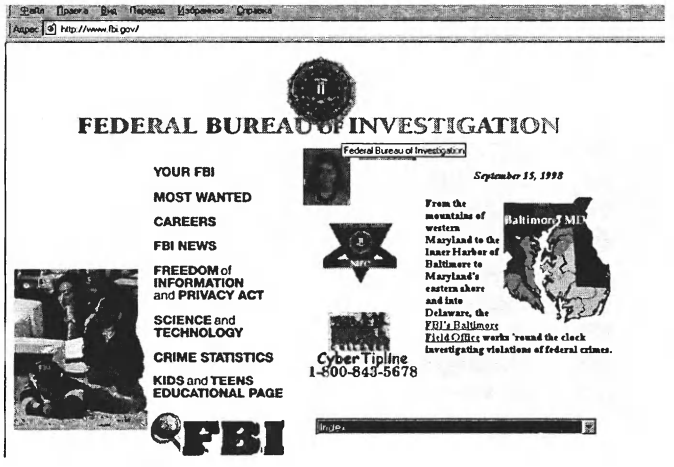
Первая попытка проследить трафик КГБ и ГРУ была сделана в феврале 1943 года: молодой даме, мисс Гени Грабел, поручили систематизировать, организовать и охарактеризовать несколько сотен зашифрованных советских дипломатических сообщений. В течение десяти следующих лет множество аналитиков упорно пробивали брешь в исключительно изощренных, дважды зашифрованных криптосистемах. По слову, по два они старательно извлекали информацию из наиболее сложных из когда-либо применявшихся криптосистем.

Первый и самый важный прорыв был осуществлен без использова-



ния какой-либо вычислительной техники, и этот задел позволил уверенно перехватывать сообщения последующие тридцать лет, поскольку коды почти не изменялись десятилетиями. Такая небрежность советской разведки объясняется крайней осторожностью ЦРУ в применении добытой информации — оно скорее позволило бы русским получить информацию об очередном испытании ядерной бомбы, чем показать, что американцы могут читать перехваченные радиосообщения.

Советская шифросистема предполагала двойное и даже, как выяснилось, тройное и четверное кодирование информации. На первом этапе (этот способ и поныне применяется в военной радиосвязи) каждая фраза, слово или буква кодировались числом, причем одинаковая кодовая единица могла шифроваться разными числами. Затем числа отстукивали телеграфом (отнюдь не привычной морзянкой), записывали на кассету (или перфоратором на киноленту) и выстреливали в эфир максимально коротким радиоимпульсом, дополнитель-



но обработанным через аналоговый скремблер.

После того, как удалось понять систему скремблирования, начались попытки прочитать слово или два в перехваченных документах. Криптоаналитики пытались найти в них ту информацию, которую другие спецслужбы специально подбрасывали советским шпионам. Каждая такая находка позволяла возобновить работу над другими сообщениями, если эта кодовая группа в них присутствовала. В таком случае тщательно исследовали соседние кодовые группы, проверяя, не является ли известная последовательность ключом к еще неизвестным. Когда информацию, полученную из дешифрованных сообщений, передавали в ФБР, и бюро проводило собственное расследование, поступала новая информация, служившая ключом к раскрытию других кодовых последовательностей. И тогда вновь начиналась обработка старых сообщений.

Затем к работе подключились лучшие лингвисты США: Арлингтон Холл, расшифровавший немецкие и японские коды времен II мировой войны (русские много заимствовали из криптосистем противника), ученые-слависты из Гарварда Мередиф Гарднер, Фердинанд Коудерт и многие другие. Они обратили внимание на "лингвистическую сетку" русского языка, определявшую структуру предложения и правила согласования времен — кодовые группы в радиограммах не переставлялись местами. Многое дали и редкие сообщения, передаваемые голосом — анализ психологического состояния говорящего позволял выделить наиболее важные фрагменты сообщения и сопоставить их с информацией, которая могла быть известна шпиону.

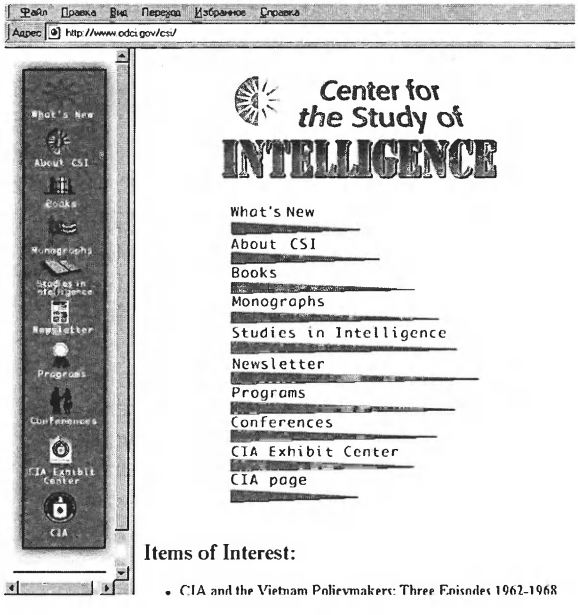
Таким образом, в период с 1948 по 1951 год удалось идентифицировать и арестовать главных агентов КГБ: Гарри Голда, Клауса Фукса, Дэвида Грингласа, Теодора Холла, Вильяма Перла, Розенбергов, Дональда Маклина, Кима Филби и Гарри Вайта. В 1952 году накопленный опыт позволил взломать шифры ГРУ и расшифровать множество сообщений армейской разведки.

Система кодирования сменилась лишь в конце семидесятых, и 1 октября 1980 года проект "ВЕНОНА" был закрыт.

Советы начинающему шпиономану

"...Дальнейшее совершенствование аппаратуры скрытой связи на основе технологии псевдослучайного переключения радиочастот пойдет одновременно с развитием средств контроля радиоэфира".

Из пресс-релиза ФАПСИ



Ныне, когда Министерство обороны США разрешило экспорт алгоритмов шифрования с открытым ключом и с 256-битной кодовой последовательностью, обеспечивающих криптостойкость чуть ли не в тысячу лет, над шифрованием конфиденциальных сообщений никто сильно не задумывается. Прогнал через программу, и готово!

Это непростительная беспечность. Неужели американцы выставят на продажу программы, при помощи которых смогут безнаказанно общаться по e-mail арабские террористы?!

Прежде всего, любая процедура шифрования начинается с генерации случайного числа. А компьютер, будь то БК 0010.01 или Pentium-II, генерирует не случайные, а псевдослучайные числа. И как эта псевдослучайность коррелирует с хардом и софтом вашего ПК — Гейтс его знает.

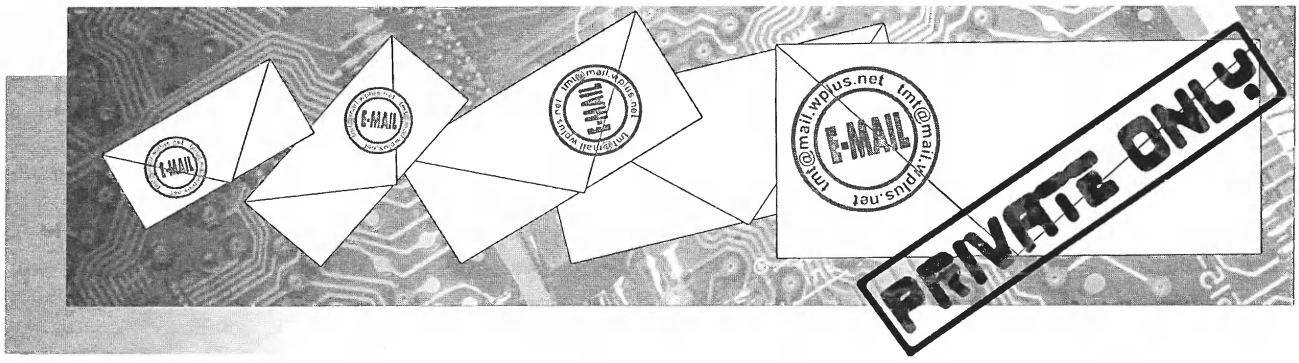
Потом, где гарантия, что программа не выбирает кодовую последовательность, исходя из содержания документа, уменьшая таким образом длину ключа до разумной величины, доступной быстрой дешифровке? Кто знает, как поизвращался над исходным алгоритмом разработчик?

Поэтому до сих пор не потеряли актуальности "дубовые" методы шифрования, предполагающие обмен закрытым ключом. Например, у вас и вашего друга есть по экземпляру русско-китайского разговорника 1937 года издания. Вот и обменивайтесь на здоровье шестизначными числами, где вторая и четвертая цифры обозначают номер страницы, шестая и третья — номер строки, первая — начальное слово из фразы, пятая — конечное слово из фразы. С таким же успехом можно использовать номера стихов из Библии.

Используйте ассоциативную терминологию, понятную только в контексте переписки. В любом случае, никакой суд не сочтет интерпретацию терминов за доказательство.

Наконец, не повторяйте ту информацию, которая уже известна адресату. Чем короче сообщение, тем труднее его расшифровать. Знаменитый фестский диск, что хранится в музее Гераклейона на Крите (на нем меньше трехсот символов), не расшифрован до сих пор...

Успехов!



Алексей Смирнов

Электронная почта и перехват информации

Козла бойся спереди, коня сзади, а человека — со всех сторон

Любопытство, как известно, не порок, а лишь признак прагматичной заинтересованности, а в наш век информационных технологий — вполне реальный способ "ковать деньги". О том, что "люди гибнут за металл", мы знаем давно. Но не все еще осознали, что денежный эквивалент — уже давно не золото, а информация.

На какой информации можно "делать деньги?". Ответ, если вдуматься, предельно прост: "На любой, лишь бы ее было много". Да, именно так, уважаемый читатель. Представьте себе на мгновение, что вы круглосуточно регистрируете и классифицируете по степени значимости все то, что пишется на всем земном шаре. Уверяю вас, очень скоро вы стали бы самым богатым человеком на планете.

Превращением информации в деньги люди занимаются уже многие века. Уверен, что на вопрос о том, кто является литературным прототипом агента-перехватчика информации, большинство ответит: Джеймс Бонд, знаменитый агент 007. Но это не так. Методом перехвата телеграфных сообщений воспользовался за столетие до него небезызвестный граф Монте-Кристо. Правда, это был оптический телеграф, передававший сообщения от станции к станции в пределах видимости (подробнее см. врезку "Деньги — информация — деньги").

Кто что охраняет, тот то и имеет

Чтобы иметь информацию, нужно контролировать информационные потоки. А самый насыщенный информационный трафик, как известно, в Интернет, причем он возрастает на порядок в течение года. Система передачи сообщений по электронной почте затмевает все существующие ныне альтернативные способы обмена данными в силу высокой скорости и низкой стоимости — даже малая компания тратит в 100—200 раз меньшие суммы, нежели пользуясь обычной бумажной почтой.

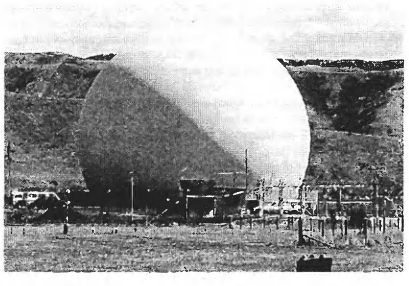
Как передать конфиденциальную информацию по электронной почте? Самый надежный способ — криптография (см. "Как защитить информацию от чужих глаз", "Магия ПК" N6). Подобные способы шифрования данных есть в составе распространенных почтовых программ (Eudora, Pegas, Outlook, Netscape-Mail). Однако за пределы США экспортируются только криптопакеты с длиной ключа-пароля не более 40—56 бит, в то время как на территории США (как, впрочем, Канады и подавляющего числа промышленно развитых стран Европы и Азии) уже в ходу почтовые клиенты с длиной слова-пароля в 128 и даже 256 бит. Конечно, умному пользователю не составит особого труда достать и эти запрещенные к экспорту пакеты. А любой доставший их с нескрываемой гордостью будет посматривать на несчастных "40-битников": уж его-то информация защищена куда как прочно.

К сожалению, невежество большинства пользователей состоит в том, что они не задаются продолжением вопроса: "От кого она защищена?". Практическая уязвимость каждого пользователя сети Интернет обусловлена прежде всего отсутствием единого международного закона в отношении охраны частной электронной переписки. Такого закона и не может быть в обозримом будущем, поскольку правила игры регламентируются национальными законодательствами, а любое государство всегда стремится не только охранять свои внутренние (политические, экономические, военные) интересы, но и выведывать секреты других стран, то есть в той или иной степени ведет мониторинг почтовых каналов.

Первая страна, развернувшая сеть контроля за системой электронных сообщений (электронная почта, цифровая телефонная связь, факсимильная передача), — США. Начав с контроля над обычными телефонными каналами и радиоэфиром, ее станции перехвата вскоре перешли к слежке за международными каналами — как наземными, так и космическими. Системой электронного сетевого шпионажа заведует отнюдь не ЦРУ, а NSA of USA (National Security Agency), рожденная в далеком 1952 году по инициативе "отца" холодной войны Гарри Трумена и более 15 лет имевшая статус "неизвестной организации" за пределами США.

Именно NSA владеет и распоряжается в интересах США охватывающей весь земной шар системой ЭШЕЛОН для перехвата электронных сообщений. Информация черпается из наземных кабельных сетей, микроволновых и радиорелейных каналов передачи данных, эфирного вещания и спутниковых коммуникационных систем. Станции перехвата цифровых каналов расположены в США (западное и восточное побережье), Исландии, Англии, Австралии и Новой Зеландии, чтобы равномерно покрыть все пространство под геостационарными спутниками связи Intelsat, "подвешенными" над экваториальной частью Земли. Все станции оборудованы не только ультрасовременной аппаратурой для приема радиосигналов, но и компьютерными центрами для просеивания данных. Эти центры объединены в единую компьютерную сеть с помощью специальных высокоскоростных коммуникационных магистралей. Производительность компьютеров в узлах слежения близка к "суперкомпьютерной" не только в части скорости просеивания информации, но и по объему RAID-систем для ее накопления ввиду постоянного роста трафика (пропускная способность шлюза Intelsat-5s составляла 12000 каналов, Intelsat-7s более 90000, трансконтинентальных кабелей связи — более 100000, а к 2001 году перевалит за 980000 каналов).

Слежка ведется как за отдельными адресами в режиме избирательного круглосуточного контроля трафика (посольства, государственные органы, военные ведомства и их спецканалы связи, международные корпорации, политические и общественные организации), так и в виде просеивания всего сетевого трафика путем поиска по ключевым словам или фразам из специального контекстного словаря Echelon Dictionary Listing (физические лица, общественные организации, исследовательские и образовательные институты и пр.).



В периоды эскалации региональной напряженности, либо при подготовке к заключению выгодных контрактов (в частности, при продаже военного оборудования), система ЭШЕЛОН работает в режиме пиковой загрузки, и каждый компьютерный узел локальных станций слежения становится узлом распределенной системы параллельных вычислений. Экономическая эффективность системы ЭШЕЛОН подтверждается многомиллиардными контрактами на поставку вооружений в страны Ближнего востока и Юго-Восточной Азии, и свежий пример тому — сделки, доставшиеся концернам Локхид и Боинг (вместо французских компаний). С помощью ЭШЕЛОН удалось "вычислить" не только объемы предполагаемых контрактов, но и размеры взяток должностным лицам в правительстве, отвечавшим за заключение контракта.

Перлюстрация частных почтовых сообщений занимает существенное место в системе мониторинга "на благонадежность". Слежка ведется как за гражданами США, так и за иностранными корреспондентами с помощью системы ELINT (Electronic Intelligence Gathering) и разветвленной сетевой магистрали DOMINT, недоступной для "простых смертных". Многолетняя "обкатанность" ЭШЕЛОНа, по данным из независимых источников, позволила завести электронные досье на каждого жителя США, а также политических и профсоюзных функционеров, лидеров общественных организаций, финансистов, ученых и активных деятелей во всех остальных странах.

Сейчас система перлюстрации почтовой переписки частных лиц переживает новый бум в связи с повальной практикой предоставления "бесплатных" почтовых ящиков на серверах известных зарубежных компаний. Как правило, такие компании берут на себя обязательство сохранять в тайне содержимое почты корреспондента, за исключением случаев, установленных законом данной страны. Очевидно, что такие службы в определенной степени облегчают работу NSA, выступая, в лучшем случае, в роли пассивных концентраторов почтовых магистралей.

В каждой избушке свои поскрипушки

С недавнего времени и нашу российскую компьютерную общественность стали беспокоить слухи о том, что ФСБ намеревается взять под контроль ВСЮ информацию, проходящую через Интернет. Особую активность в этом плане развивает подразделение по борьбе с компьютерными преступлениями, созданное в январе 1996 года в рамках управления по борьбе с экономическими преступлениями. Задуманный проект называется "Система технических средств по обеспечению функций Оперативно-Розыскных Мероприятий на сетях (службах) документальной (цифровой) электросвязи", а сокращенно — СОРМ.

Приведем несколько выдержек (с минимальной литературной правкой) из циркулирующего на российских сетевых узлах документа от 20 августа 1998 года, который утверж-

ден на совещании в Госкомсвязи РФ с участием ФСБ и АДЭ.

Задача проекта формулируется следующим образом: "Обеспечение режима сохранения государственной тайны при использовании глобальных телекоммуникационных систем с применением для этого новых программно-технических средств обеспечения защиты информации, циркулирующей в корпоративных и других сетях, подключающихся к Интернет". Видимо, понимать эту формулировку следует так: наша задача — не только вылавливать тех, кто пытается пересылать за кордон государственные тайны, но и оградить российские предприятия от внешней угрозы.

"В состав системы войдут аппаратно-программные средства, обеспечивающие реализацию требований к СОРМ, и канал связи (линии связи и каналообразующая аппаратура), обеспечивающий организацию связи между СДЭС (сетью документальной электросвязи) и пультом информационного контроля.

По команде с пульта управления СОРМ должна обеспечивать съем статистической информации, а также съем информации (входящей и исходящей), принадлежащей конкретным пользователям, причем независимо от того, какие способы защиты информации используются в СДЭС. Кроме того, комплекс аппаратно-программных средств должен обеспечивать прерывание предоставления услуги абонентам и пользователям СДЭС по команде с ПУ СОРМ".

Заметим сразу, что охрана государственных тайн — дело несомненно нужное и важное. Любое государство, претендующее на политический вес, будет по мере возможности бюджета создавать подобного рода системы. Но вводить данную систему нужно грамотно, экономя средства, с учетом имеющейся материальной базы. Поскольку ни средств, ни собственной материальной базы уже попросту нет, проект потребует огромных затрат. А традиционные для России волокита и долгострой выльются в еще большие затраты, помноженные на абсолютную неэффективность.

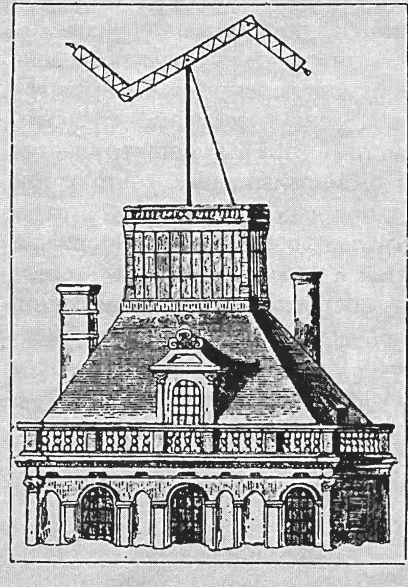
Технически реализовать контроль всей информации очень трудно. Для этого нужно не только перехватить и прочитать все сообщения, но и проверить их на наличие скрытого кода. Ведь мало кто сподобится передавать чертежи, скажем, новейшей ракеты класса "земля-воздух" в незашифрованном виде. Это означает, что сообщения будут про-

Деньги — информация — деньги

Если дедушкой электронной почты является обычный телеграф, то прадедушкой можно с полным основанием считать так называемый оптический телеграф. Его изобрел француз Клавдий Шапп в 1794 году.

В детстве Шапп учился в Анжерской семинарии, а его братья — в пансионе, расположенном неподалеку. Мальчик, разлученный с братьями, очень скучал, и решил переписываться с ними, подавая условные сигналы из своего окна с помощью системы из двух линеек, которые могли вращаться вокруг концов третьей линейки. Число комбинаций из возможных взаимных поворотов трех линеек превышало число букв алфавита, и некоторые наиболее часто употребляемые фразы передавались одним сигналом.

Став взрослым, Шапп предложил свое изобретение правительству и вскоре был назначен главным инженером телеграфа. Первая линия была проведена из Парижа в Лилль. Вышки с семафорами ставились на расстоянии прямой видимости друг от друга, и на них постоянно дежурили телеграфисты. В ночное время для сигнализации использовались фонари, укрепленные на концах семафорных крыльев.



Работал такой телеграф по тем временам довольно быстро — на передачу известия через 100—120 станций (около 1500 км) уходил час. Однако обычным явлением были ошибки при чтении и дальнейшей передаче сигналов. Секретные телеграммы передавались особым шифром, поскольку любой, знакомый с телеграфной азбукой, мог читать текст сообщений, а шифрование еще больше увеличивало возможность ошибок.

Наконец, передача правительственной и биржевой информации требовала от телеграфистов полного бескорыстия, а это качество встречается не у всех людей. Так, одна из известных европейских банкирских династий достигла своего благосостояния благодаря подкупу служащего французского телеграфа. За определенную мзду он исказил сообщение об исходе битвы под Ватерлоо. Ложное известие о победе Наполеона, дойдя до Лондона, вызвало панику на бирже, благодаря которой агенты банкира за бесценок скупили акции, на следующий же день вернувшие свою стоимость.

Александр Альбов

ходить через фильтры ФСБ с весьма ощутимой временной задержкой.

Можно, конечно, следить за данными, передаваемыми только определенными абонентами Интернет, имеющими непосредственное отношение к секретной информации. Но тогда останется возможность пересылать эти данные с других, "незасвеченных" адресов, и проблема останется нерешенной.

В конечном счете, прикинув сметные затраты, можно попросту ограничить число провайдеров, либо вообще передать предоставление Интернет-услуг "наиболее достойным" со всеми вытекающими для простых пользователей последствиями.

Однако именно такие затеи, гиблые по существу и вредные для подавляющей массы населения, — настоящий "клондайк" для так называемых "галочников", которые не только оправдаются в будущем за потраченные деньги и персональные оклады, но и сумеют аргументированно поставить "на уши" полстраны, чтобы поймать одного шпиона "ко Христову дню".

Гласность о двух концах

Как же так, — возмутятся самые демократичные читатели, — американцев подслушивают их государственные ОРГАНЫ и они, американцы, не возмущаются? Не может быть!

Во-первых, возмущаются, хотя и вполголоса, а во-вторых, как большинство прагматичных людей, воспринимают это не сердцем, а умом. Дело в том, что система тотального информационного контроля КОРМИТ Америку, и кормит весьма аппетитно, поскольку собираемая информация используется для протежирования американского бизнеса, а это вполне ощутимо отражается на уровне жизни любого возмущающегося.

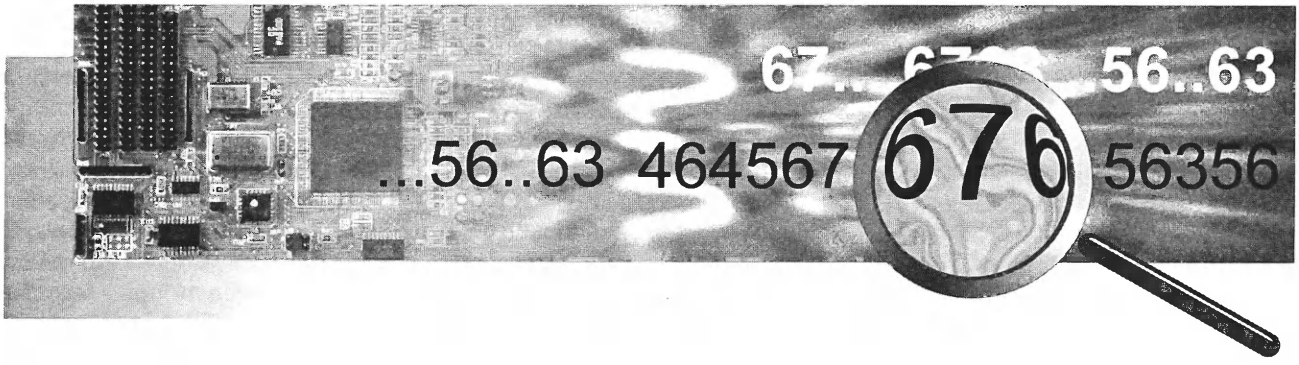
Хотите проверить? Нет проблем: зарегистрируйтесь в любой дискуссионной группе Интернет, обозначив себя как ярого поборника гласности, и на ваш адрес хлынет поток сообщений о СОРМ. Отберите десяток американских адресатов и попросите прислать также известные им данные о системах Shadow, Echelon, радиоэлектронного перехвата в эфире и мониторинга компьютерных сетей, тематике работ класса С4... — гробовое молчание будет вам ответом, и не только потому, что подобного рода секреты там умеют хранить, но и потому, что каждый из возмущающихся знает — его телефонная линия или сеть всегда под колпаком у дяди Сэма.

* * *

Так можно ли защитить свой электронный почтовый ящик? Средства защиты, предоставляемые почтовыми клиентами в виде SSL (Secret Socket Layer), либо 40-, 56- или 128-битного крипторгафирования, явно недостаточны для того, чтобы гарантировать почту от взлома специалистами NSA. Возможностей суперкомпьютерного парка NSA хватит, чтобы в разумное время справиться с криптопакетами, использующими ключевые слова до 1000 бит. В то же время, сейчас в ходу криптопакеты tripple-DES с длиной ключевого слова 168 и 256 бит. Их использование с некоторыми дополнительными ухищрениями может озадачить даже прожженных экспертов NSA. Ведь только после одиночного прохода 168-битного tripple-DES им необходимо угадать одну "счастливую" комбинацию из 37414441915671114706014331717536845303191873100185 6. Поиск комбинаций в режиме "тупого" перебора при производительности компьютера 1 миллион ключей в секунду займет не менее 10^{14} лет. А после двукратного "разбавления мусором" зашифрованного в первом проходе файла и его повторного шифрования с применением нового пароля приведенное выше число придется возвести в квадрат.

Наглядным подтверждением тому, что пользователь-индивидуал может свести на нет усилия громадной машины государственного контроля даже такой страны, как США, является дело Кевина Митника — авторитета в мире хакеров. Следствие продолжается уже почти три года, но экспертам так и не удалось "разбомбить" систему криптозащиты "запароленных" файлов на его домашней персоналке.

Любой пользователь электронной почты должен знать, что содержимое его переписки будет просматриваться, и во все возрастающей мере. Залогом тому служат пятилетние совместные исследования США и Европейского союза по стандартизации коммуникационных обменов в цифровых сетях Интернет, что подразумевает возможность перехвата и "трассировки" клиента в режиме on-line. Так что, при всей нелюбви подавляющей части пользователей e-mail к играм в джеймсов бондов, привыкать к употреблению криптопакетов придется точно так же, как к средствам для безопасного секса.



Виктор Ананьев

Электронная тайнопись

Стеганография (по-гречески "тайнопись") имеет многовековую историю и по возрасту существенно старше криптографии. Любители детективного жанра смогут привести массу увлекательных и поучительных исторических примеров ее применения: от татуировок, скрытых под волосяным покровом гонцов, до писем, написанных физиологическими растворами. Мы же остановимся на современном и сравнительно новом направлении этой сферы человеческой деятельности — компьютерной стеганографии.

Как известно, цель криптографии (шифрования) состоит в сокрытии содержания секретных сообщений. Стеганография идет принципиально дальше. Ее задача — скрыть от непосвященных сам факт существования сообщений. Такие скрытые сообщения могут включаться в различные внешне безобидные данные, вместе с ними храниться и передаваться без всяких подозрений со стороны. Если разработчики криптографических алгоритмов исходят из предположения, что потенциальный противник будет делать что угодно для дешифровки сообщения, то разработчик стеганографического алгоритма озабочен тем, как не дать противнику обнаружить существование тайного сообщения.

Хотя стеганография и криптография принципиально отличаются по целям, их не стоит рассматривать как альтернативу друг другу. Это, скорее, две стороны одной медали. И не только потому, что по-настоящему эффективно лишь их совместное использование, но и потому, что в их основе лежит общая методическая и инструментальная база.

Компьютерная стеганография исходит из следующих базовых принципов.

Защита строится на предположении, что противник имеет полное представление о проекте стеганографической системы и деталях ее реализации. Единственной неизвестной противнику информацией является ключ (некоторая достаточно короткая кодовая комбинация). И если сообщение скрыто с помощью такого ключа, то необходимо, чтобы лишь держатель ключа мог установить факт наличия сообщения и прочитать его (принцип Кергоффа).

Если все же противник как-либо узнает о присутствии скрытого сообщения, это не должно позволить доказать данный факт третьему лицу и, тем более, обнаружить другие подобные сообщения до тех пор, пока ключ не раскрыт.

Потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Чем больше шума, тем лучше

Теоретически диапазон возможных методов стеганографии соизмерим с широтой человеческого воображения. Поэтому ограничимся лишь теми подходами к проблеме, которые уже получили распространение.

Начнем с того, что львиная доля компьютерной информации "шумит". "Шумит" все то, что хранится, передается и обрабатывается. Далее кавычки убираем, так как это законный технический термин, указывающий на наличие ошибок в данных, помех в каналах связи и прочих случайных сигналов и знаков.

Минимальной единицей хранения информации в компьютере является, как известно, бит. Любое значение — это совокупность битов. А если это значение содержит, например, ваш текущий оклад в ведомости на зарплату с точностью почему-то до 3 знака после запятой, то как раз эти "лишние" биты и есть шум. Аналогичный шум мы найдем практически в любом массиве результа-

тов измерений, графическом или звуковом файле.

Алгоритмы стеганографии как раз и основаны на идее замены шумовых компонентов цифровой связи шифрованными "псевдослучайно" секретными сообщениями.

Такие компоненты, предназначенные для упрятывания секретных сообщений, называют контейнерами. Данные контейнера должны быть достаточно шумными, чтобы небольшое изменение в их беспорядочности не могло быть заметным. Биты контейнера, хотя и являются шумом с точки зрения точности измерений, могут иметь некоторые специальные статистические характеристики. Предполагается, что кодирование тайного сообщения должно воспроизводить характеристики шума контейнера. Цель труднодостижимая, но реальная.

Одна из возможностей состоит в генерации большого числа альтернативных контейнеров, чтобы выбрать наиболее подходящий для хранения тайного кода. Такой подход именуют селектирующей стеганографией. Основная проблема, связанная с этим подходом: он позволяет спрятать малое количество данных при больших затратах.

Другой подход — моделирование характеристик шума контейнера. Подражательная функция должна быть построена так, чтобы не только кодировать секретное сообщение, но и придерживаться модели первоначального шума. В предельном случае целое сообщение конструируется в соответствии с моделью шума. Такой подход называют конструирующей стеганографией, и он также имеет много недостатков. Его трудно совместить с сильным алгоритмом шифрования, да и моделирование шума или компонентов ошибок в данных — занятие не из легких. Формирование модели требует значительных усилий, творческой работы над каждым каналом связи или контейнером.

Поскольку попытки подражания первоначальному шуму либо ведут к сомнительной безопасности или к слишком малому диапазону рабочих частот для большинства применений, наиболее привлекательной остается следующая базовая процедура.

Выбирается класс достаточно шумных контейнеров и идентифицируются биты шума. Затем приблизительно определяется, какую порцию шумовых битов контейнера можно заменить псевдослучайными данными без значительного изменения его статистических характеристик. Например, если контейнер представляет собой цифровую фотографию, нас должны интересовать младшие биты серой шкалы или RGB-значений при цветном изображении, либо коэффициенты Фурье в JPEG-формате изображений. Изменяя в среднем, допустим, только 100-й пиксель изображения, в один мегабайт несжатого изображения можно спрятать примерно один килобайт тайных данных.

Для дополнительной безопасности и придания тайному сообщению вида случайных данных оно должно быть зашифровано сильным криптоалгоритмом. Замена псевдослучайными битами некоторых наиболее шумных битов контейнера только немного увеличит уровень шума сообщения. Включение открытого текста в контейнер может заметно изменить его статистические характеристики. Более того, последовательность скрывающих битов должна выбираться псевдослучайным способом как функция секретного ключа. Иначе противник, имеющий алгоритм, без труда вскроет контейнер.

Но и шифрование с ключом не освобождает от проблем. Если скрывающие биты в подозреваемом сообщении имеют некоторые статистические отклонения от других аналогичных сообщений, то противник получит все основания для вывода, что оно содержит скрытые данные. Тогда путем дополнительного зашумления он может исказить сообщение, этим фактически его уничтожив.

Типы контейнеров

Контейнеры могут быть двух типов. Они представляют собой или поток непрерывных данных, подобно цифровой телефонной связи, или файл, подобный растровому изображению. О потоковом контейнере заранее нельзя сказать, когда он начнется и когда закончится. В достаточно длинном контейнере можно скрывать несколько сообщений. Более того, объективно нет возможности узнать заранее, какими будут последующие шумовые биты, и необходимо включать скрывающие сообщение биты в поток в реальном масштабе времени. Скрывающие выбираются с помощью специального генератора, который задает расстояние между последовательными битами в потоке. Такой способ называют произвольно-интервальным методом. В непрерывном потоке данных самая большая трудность для получателя — определить, когда начинается скрытое сообщение. В простом случае, если поток данных имеет конечную длину и часто вновь открывается, тайное сообщение может начинаться при открытии сеанса. А для отправителя основная проблема — отсутствие уверенности, что поток контейнера будет достаточным для размещения сообщения.

Файлы фиксированной длины в качестве контейнеров свободны от недостатков потоковых контейнеров. Отправитель знает заранее размер файла и его содержание. Скрывающие биты могут быть равномерно выбраны с подходящей псевдослучайной функцией. Поскольку контейнер известен заранее, есть время оценить его эффективность применительно к выбранному алгоритму сокрытия информации.

Некоторые программные продукты

К настоящему времени получили распространение десятки программ, реализующих методы стеганографии. Рассмотрим несколько примеров.

StegoDos — одна из свободно распространяемых и широко обсуждаемых программ стеганографии анонимного автора (псевдоним Черный Волк). Представляет собой ряд исполнимых модулей для MS DOS. Работает только с 256-цветными изображениями формата 320x200,

которые предварительно должны быть отображены на экране программой просмотра, не входящей в StegoDos. Затем с помощью резидентной программы делается копия видеобуфера компьютера. Полученный образ используется в качестве контейнера, в который помещается закодированное сообщение пользователя. Декодирование производится аналогично — контейнер отображается на экран и вызывается программа извлечения сообщения, которое затем помещается в выходной файл.

WNS (англ. Белый шумовой шторм, автор Arsen Arachelian) — одна из универсальных программ стеганографии для DOS. Автор рекомендует шифровать сообщение перед вложением в контейнер. WNS включает и подпрограмму шифрования, чтобы "рандомизировать" скрывающие биты в контейнере. Программа разработана с использованием результатов спектрального анализа, выгодно отличается качеством сопроводительной документации, что сглаживает некоторое ее отставание в теоретическом отношении. Основной недостаток метода шифрования в WNS — потеря большого количества бит, которые могли бы использоваться в качестве скрывающих. Отсюда — завышенные требования к размерам контейнеров.

S-Tools for Windows v. 3.00 (автор Andy Brown) — один из наиболее развитых универсальных инструментальных комплексов стеганографии. Включает несколько программ, которые обрабатывают изображения GIF и BMP, звуковые WAV-файлы и даже скрывают информацию в "неиспользуемых" областях на гибких дискетах. В дополнение к поддержке 24-битных изображений включает поддержку подпрограмм шифрования (IDEA, MPJ2, DES, 3DES и NSEA) с многочисленными опциями, содержит хороший интерфейс с подсказками и четкую интерактивную документацию. К сожалению, программа лицензирована и по действующему законодательству США не подлежит экспорту.

Этому же автору принадлежит интересная реализация GZIP-архиватора. На 100 Кб несжатого текста ему удалось добиться включения 1 Кб скрытого текста. Специалисты, знакомые с эффективностью (плот-

Семнадцать килобайт весны

(из будней разведчика)

ВИНДОС — ЮЗЕРУ

Модем не установлен. Сведения отсутствуют. Устройство работает нормально.

Хакерлиц понял, что Центр в течение некоторого периода не сможет поддерживать связь. Видимо, на Родине велись приготовления к тестированию, и Центр опасался постоянных сбоев в работе Системы. Однако из шифровки следовало: руководители Главного Взломного Управления не забыли разведчика и давали ему понять, что в любой момент Хакерлиц должен быть готов к новому заданию.

ЮЗЕР — ВИНДОСУ

Для данного устройства не требуются или не были загружены файлы драйвера.

Хакерлиц сообщал Центру, что противник в лице альтконтролфюрера MS Ламмера, шефа 6-го управления Софтвера, явно ведет двойную игру, стремясь натравить его, оберэнтерфюрера ПО, на союзников. Конечно же, в случае удачного результата тайных контактов союзники смогут эвакуировать Ламмера из Сети ведения боевых действий и даже, может быть, спасти от делетины. На это и рассчитывает Ламмер, направляя на секретные переговоры Хакерлица.

ВИНДОС — ЮЗЕРУ

Конфликты не обнаружены.

...Хакерлиц спал. Он знал, что проснется ровно через 19 минут 26 секунд реального времени и перезагрузит Систему. А пока разведчик спал, и снились ему добрые трехмерные сны с акселератором.

БИОС — ЮЗЕРУ

Полное форматирование. Вывести отчет о результатах.

Хакерлиц понял, что это — провал. Видимо Ламмер, его сотрудник по видимой и противник по тайной, никому в OS не известной жизни, получил секретную информацию о том, кто же такой на самом деле оберэнтерфюрер Хакерлиц.

ЮЗЕР — ВИНДОСУ

Перезагрузить в режиме эмуляции MS-DOS.

Только один раз в году Хакерлиц позволял себе немного расслабиться. На Родине должны были знать, что сегодня ночью разведчик на связь с Центром не выйдет.

ВИНДОС — ЮЗЕРУ

Форматирование успешно завершено.

Центр сообщал Хакерлицу, что Родина вручила ему, Ивану Васильевичу Петрову, самую высокую награду — Герой Операционной Системы. А в ближайшее время Центр направит Хакерлица на новый невидимый фронт — свежую версию операционной среды.

...Хакерлиц удовлетворенно вздохнул и с тихой ностальгией загрузил "Пентиум".

Павел Лаптинов

ностью упаковки) этого архиватора, оценили его весьма высоко.

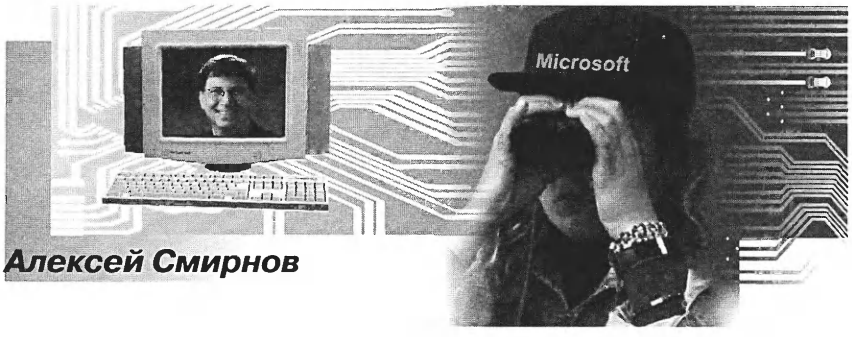
Covert_TCP 1.0 (автор Craig H. Rowland) предназначен для скрытой передачи файлов по каналам ОС Linux. Эта программа управляет TCP/IP заголовком и передает с каждым файлом один скрытый байт на главную ЭВМ адресата. Программа может работать как станция и как пользователь. При значительном трафике возможности передачи скрытых данных весьма велики, тем более, что экспорт данных производится и со служебными пакетами.

HideSeek v5.0 — программа для ДОС, предназначена для обработки gif-файлов. Для рандомизации (но не шифрования) используется алгоритм IDEA. Работает при различной разрешающей способности дисплея, но может быть довольно медленной для большого gif-файла и/или файла скрываемых данных. Программа свободно распространяется и вполне удобна для знакомства с практическим использованием стеганографии.

Выводы и прогнозы

Несмотря на молодость компьютерной стеганографии, уже сегодня любой тип данных может быть скрыт и перемещен невидимо в местах, где производится хранение или передача больших объемов "шумных" данных. Наиболее подходящими для сокрытия тайных сообщений являются цифровые аудио- и видеофайлы.

Создавая определенные удобства для сохранения тайны переписки, стеганография создает условия для возникновения неконтролируемых информационных каналов. В частности, это вызов органам контрразведки, которая неизбежно должна отреагировать новым прорывом в технологиях информационной безопасности. Стеганография — привлекательное средство для деятельности хакеров, она позволяет распространять вирусы. Данный список можно продолжить. Но очевиден тот факт, что прогресс в области стеганографии может кардинально изменить существующие подходы к проблеме информационной безопасности.



Алексей Смирнов

Под колпаком у Microsoft

"Билл, если хочешь спать спокойно, убери свидетелей и спили мушку у кольта, сынок... Так, на всякий случай".

Каждый разработчик программного обеспечения мечтает о том, чтобы его продукция раскупалась как можно лучше. Как этого добиться? Повышать качество и снижать цены. Это нормальный регулятор рыночных отношений, но работает он только при наличии конкуренции. А если повышать и снижать не очень-то хочется? Как вытеснить конкурентов "на обочину"? Очень просто — для этого служат такие испытанные средства, как экономический шпионаж за конкурентами и разрушение программной совместимости для их продукции.

Классический пример того, как это делается, демонстрирует ведущая корпорация мира — Microsoft.

Все началось с внешне безобидной ремарки, занесенной в зашифрованном виде в диспетчер запуска WIN.COM в далеком теперь уже 1990 году при представлении первой beta-версии Windows-3.1:

WARNING: This Microsoft product has been tested and certified for use only with the MS-DOS and PC-DOS operating systems. Your use of this product with another operating systems may void valuable warranty protection provided by Microsoft on this product.

ВНИМАНИЕ: Данный продукт Microsoft протестирован и сертифицирован для использования только с операционными системами MS-DOS и PC-DOS. В случае его применения с другими операционными системами пользователь может лишиться гарантийного обслуживания Microsoft.

Причина кроется в противостоянии MS-DOS (приобретенной тогда еще мало кому извстной Microsoft всего за 100000$) с конкурентной операционной средой DR-DOS (разработанной Digital Research Corp., затем проданной Nowell и перепроданной Caldera Corp.) на просторах европейского компьютерного рынка, где DR-DOS в то время доминировала стараниями ведущего европейского концерна Vobis (Западная Германия). Предупреждение возникало на экране в том случае, если диспетчер запускавшейся Windows-3.1 (WIN.COM) обнаруживал на ПК пользователя DR-DOS.

Это и подрубило на корню честолюбивые планы Novell, первого конкурента Microsoft: диспетчер загрузки через некоторое время производил запланированный обвал Windows-3.1 (расправиться так же с PC-DOS могущественной IBM в то время Microsoft не могла себе позволить). После многолетних безуспешных попыток докопаться до причины непонятных обвалов специалистам удалось вычислить и расшиф-

ровать как саму запись, так и алгоритм "обвала замедленного действия", и даже найти подтверждение этому в электронной переписке группы разработчиков Windows-3.1 со своим руководителем Дэвидом Коулом:

"The most sensible thing from the development standpoint is to continue to build dependencies on MS-DOS into Windows."

"Наиболее разумная статегия развития состоит в жесткой привязке Windows к MS-DOS".

"...Aaron had some pretty wild ideas after three or so beers-earleh has some too... put competitors on a treadmill... should surely crash at some point shortly later..."

"После трех кружек пива Аарону пришла в голову блестящая идея, как этим парням устроить МЯСОРУБКУ... просто обваливать операционку спустя лишь некоторое время..."

"We should surely crash the system... but the less people know about exactly what gets done, the better."

"Нужно просто обваливать операционную среду,... но чем меньше людей об этом будет знать, тем лучше".

После того, как значительная часть пользователей была напугана непонятными обвалами, компания "запретила" (программным путем) выдачу данного сообщения в окончательной версии операционной среды, появившейся под новый 1991 год, правда, то ли по недоразумению, то ли по недомыслию, запись осталась внутри того же командного файла.

Точнее, фраза была преобразована в форму слегка завуалированной угрозы. Вот что можно прочитать в файле README.WRI русскоязычной версии WINDOWS-3.11 (англоязычный фрагмент абсолютно идентичен).

"Microsoft Windows для рабочих групп и MS-DOS работают вместе как единое целое. Они разрабатывались вместе и прошли тщательное совместное тестирование на множестве разных компьютеров и конфигураций оборудования. Запуск Windows для для рабочих групп с операционной системой, отличной от MS-DOS, может привести к неожиданным результатам или плохой производительности, и не рекомендуется корпорацией Microsoft".

С переходом от Windows-3.xx к Windows-95 открытая "рельсовая война" сменилась более продуманной тактикой негласного сбора информации о программных приложениях конкурентов, имеющихся на жестком диске "дисциплинированных" пользователей, которые регистрировали установку как новой операционной среды, так и последующих модификаций (так называемый upgrade ПО). Для этой цели в состав Windows'95 были введены четыре файла: WELLCOME.EXE, REGWIZ.EXE, PRODINV.DLL, SIGNUP.EXE (в директории c:/windows/system). Забегая вперед, скажем, что первой "триады" вообще не нужно для нормальной работы ОС. Их можно попросту "грохнуть" без каких-либо последствий, поскольку их назначение, помимо установления законности upgrade, — тайный сбор информации о том, какое ПО конкурентов установлено на машине пользователя.

Так, внутри файла PRODINV.DLL в зашифрованном виде содержался перечень из 128 (а затем и больше) конкурирующих программных приложений, на предмет наличия которых на жестком диске пользователя и производился НЕГЛАСТНЫЙ НАДЗОР. Вот лишь небольшая часть этого списка:

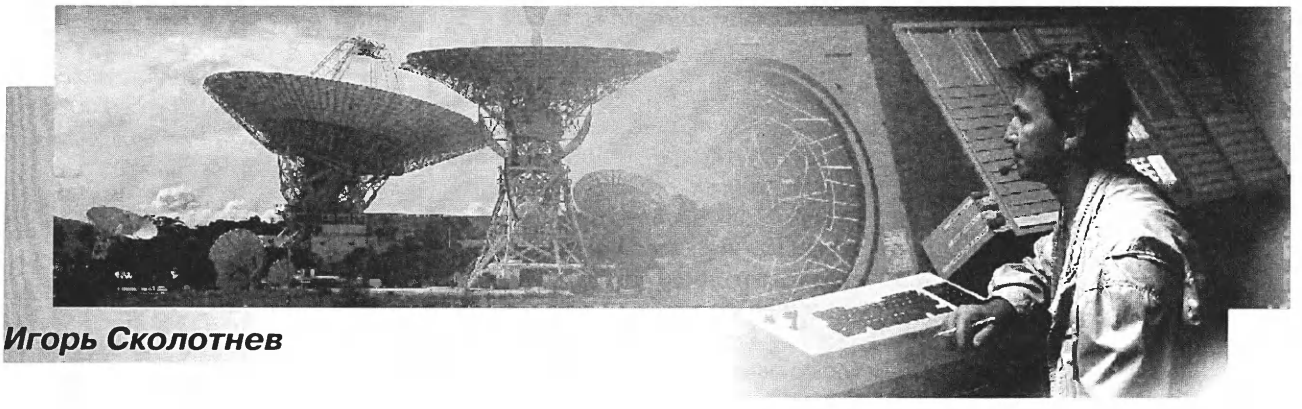
Aldus PageMaker for Windows, Aldus Persuasion, America On-line, AmiPro for Windows, Borland Dbase, Borland C++ for Windows, Turbo Pascal for Windows, Borland Delphi, Borland Paradox for DOS, Corel Draw for Windows, Lotus 123 for Windows, Lotus Notes, Lotus123 for DOS, Personal Oracle 7, Quattro Pro for Windows, Quick C for Windows, Quicken for Windows, WordPerfect for DOS, WordPerfect for Windows, PowerBuilder Enterprise 4 for NT, NCSA Mosaic for Windows...

Файл PRODINV.DLL действительно содержит признаки подготовки данных для проведения легального upgrade, но не только, в чем можно убедиться, открыв его обычным экранным редактором Word (напечатав полностью имя файла в соответствующей позиции, поскольку формально он "убран" из файлового окошка просмотра даже при установке режима "All files"). В теле файла перечислены тематические категории действий программы, среди которых можно увидеть Registry Search, INI File Search, Big Search, Hard Disk Search. Это и есть перечень инструкций по поиску ПО конкурентов.

Чтобы скрыть факт перлюстрации диска пользователя, список в PRODINV.DLL зашифрован вместе с перечнем ключевых имен искомых файлов и их ориентировочных размеров в байтах (на случай установки их в не рекомендованные разработчиками директории). Как только обнаруживалось присутствие продукции конкурентов, соответствующие "донесения" заносились в базу данных, сформированную ТОЛЬКО в RAM-памяти ПК, а затем передавались посредством модемного канала в сетевые узлы MSN (Microsoft NetWork), после чего тихо и незаметно исчезали при выходе из приложения. Данный сценарий удалось раскрыть спустя некоторое время с помощью специальных программ — "резидентных блокираторов" (TSR), которые прерывали работу REGWIZ.EXE (Registration Wizard) и проверяли содержимое RAM.

Конечно, формально регистрацию можно провести и по обычной почте с использованием бумажных купонов, поставляемых вместе с лицензионным ПО, но компания приветствовала именно "электронную" регистрацию как наиболее УДОБНУЮ для обеих сторон, которая, к тому же, поощрялась соответствующими бонусами...

Я далек от рассуждений на тему о морали в бизнесе, хотелось только показать ту его сторону, которая имеет оттенок заурядного штампа — промышленный шпионаж в сфере IT-технологий. Никто не говорит, что остальные компании не прибегают к приемам "подковерной борьбы", но Microsoft, пожалуй, преуспела в этом куда более других.



Игорь Сколотнев

Безопасность информации при радиосвязи

Проблема "беззащитности" информации при ее передаче средствами радиосвязи, наверное, хорошо всем известна из просмотра многочисленных шпионских фильмов. При этом, как хорошо показано в тех же фильмах, возможны три варианта воздействия на информацию: ее перехват, подмена и уничтожение.

Но, как ни удивительно, большинство людей даже и не задумывается о том, что все эти "шпионские страсти" полностью справедливы и применимы практически для всех систем радиосвязи, начиная с простейшего домашнего бесшнурового радиотелефона. И если уничтожение информации ("забивание" радиосигнала мощной помехой) становится заметно сразу, попытки "подсовывания" информации обычно также легко выявить по различным косвенным признакам или просто ее проверкой, то о действиях по перехвату информации обычно удается узнать уже только по результатам ее использования "противником".

Очевидно, что наиболее надежным способом защиты информации от перехвата при таких методах передачи является ее кодирование. Использование различных условностей при разговорах по радиотелефонам оставим читателям и писателям детективных романов, а здесь остановимся только на технической стороне дела.

Бытовые радиотелефоны

Применительно к каналам голосовой связи всевозможные методы шифрования получили общее название — скремблирование. Следует сразу отметить, что различные системы "кодирования", упоминаемые в описаниях многих бытовых радиотелефонов, не имеют ничего общего с защитой передаваемой звуковой информации. Все эти системы предусматривают только проведение обмена специальными кодовыми последовательностями между базовым блоком радиотелефона и трубкой, и предназначены они лишь для предотвращения случайного подключения трубок к базовым блокам других радиотелефонов, работающих поблизости. А системы защиты голосовых каналов радиотелефонов (среди встречающихся у нас моделей) есть только в относительно старых аналоговых немецких телефонах "Sinus-52" и новых цифровых телефонах стандарта DECT, выпускаемых сейчас в мире уже целым рядом фирм.

Сотовые системы

Не лучше обстоят дела с защитой и в сотовых системах. Из трех стандартов сотовой связи, используемых питерскими компаниями-операторами (NMT-450 у "Дельта Телеком", NAMPS у FORA communicatoins и GSM — у "Северо-Западного GSM") только в последнем голосовой сигнал передается в цифровой форме и дополнительно шифруется. Радиопереговоры абонентов двух других сотовых компаний могут совершенно элементарно прослушиваться с помощью любого обычного приемника, имеющего соответствующий диапазон частот. Причем, если в США весной этого года был принят закон об уголовной ответственности (вплоть до тюремного заключения!) за прослушивание сигналов в диапазонах частот, используемых для сотовой связи, то в России ничего подобного пока нет. Одним словом — слушай в свое удовольствие (что, впрочем, и делают в нашем городе уже несколько подпольных "центров радиоперехвата").

Однако соотношение между "защищенными" и "незащищенными" абонентами уже на следующий год может измениться в лучшую сторону. Дело в том, что в 1998 году сразу две

новые компании (выигравшие соответствующий конкурс) получили право на развертывание в северо-западном регионе сетей сотовой связи в новом стандарте DCS. Основные технические решения, используемые в этом стандарте (за исключением диапазона рабочих частот и численных значений некоторых других параметров) полностью заимствованы из стандарта GSM, за что его иногда называют стандартом GSM-1800. Переговоры абонентов этих двух сотовых систем также будут передаваться в цифровой зашифрованной форме и, следовательно, будут достаточно хорошо защищены от радиоперехвата.

Другие виды радиосвязи

Очень похожая ситуация имеет место и в системах транкинговой связи. Из действующих сейчас у нас систем пока лишь в стандарте EDACS (в Петербурге его использует пока только сеть компании "РадиоТел") предусмотрена защита голосовой информации. Сходное решение заложено и в перспективном стандарте TETRA, но пока это дело завтрашнего дня.

Говорить же о конфиденциальности связи в других распространенных радиостанциях, например, диапазонов "Си-Би" и "Low Band", вообще не приходится — там все полностью открыто. Совершенно беззащитны перед радиоперехватом и все существующие в нашей стране пейджинговые системы общего пользования.

Передача данных

Естественно, все сказанное о защищенности голосовых каналов (и хорошее, и плохое) полностью распространяется и на случаи передачи по этим радиоканалам любых данных, например, с помощью модемов и факсов. Причем, если современные протоколы взаимодействия модемов иногда и могут создать какие-либо проблемы при восстановлении перехваченной информации, то копии факс-сообщений получаются просто элементарно!

А если шифроваться?

Ну что же, если нет встроенных средств засекречивания переговоров, то можно подключить внешнее устройство шифрования и наслаждаться возможностью ведения "секретных" разговоров. Современные персональные компьютеры вполне позволяют обойтись даже без использования дорогостоящих специальных скремблеров. Ведь самый обыкновенный модем на скорости 33600 бит/с, подключенный к компьютеру, на котором запущена, например, свободно распространяемая через Интернет программа "PGPphone", вполне обеспечивает довольно неплохое скремблирование звуковых сигналов. Однако как раз эти действия (в отличие от упомянутого ранее подслушивания) в нашей стране попадают в разряд незаконных! Это вызвано тем, что еще в 1995 году Указом Президента № 334 использование средств криптографии, не имеющих лицензии ФАПСИ, в России запрещено. Правда, подобная "однобокость" ситуации до сих пор компенсируется чисто российским курьезом: форма наказания за нарушение данного указа до сих пор так и не установлена. То есть нарушать указ нельзя, но если такое случится, то что потом будут делать с виновным (то ли казнят, то ли просто скажут: "Ай-яй-яй!") — пока неизвестно.

Что же делать?

Думаю, с "безопасностью" радиосвязи уже все ясно. Но это еще не все проблемы. Ведь если учесть, что на практике подавляющее большинство радиопереговоров так или иначе идет с абонентами... обычной телефонной сети, то подслушивать их можно даже и без специального приемника — просто подключившись к проводам на лестничной площадке. Ну, а для серьезных случаев существует еще и специальная аппаратура...

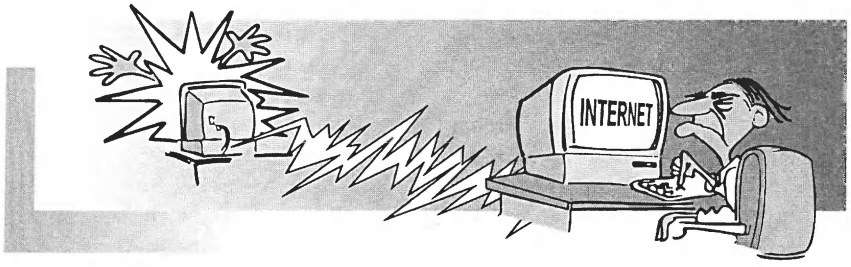
Одним словом, если вам нужно сохранить конфиденциальность передаваемой информации, то лучше всего делать это по старинке — на ухо своему собеседнику и оглядываясь, чтобы рядом никого не было.

Интернет может быть безопасным местом, во всяком случае, не более опасным, чем ваш офис. Для этого требуются только знания и осмотрительность.

Среда Интернет становится все более привлекательной для бизнеса. Типичный путь российского бизнесмена во всемирную паутину таков. Сначала — подключение к Интернет-узлу провайдера одного своего компьютера по коммутируемому телефонному каналу: присмотреться, что такое Интернет, набраться опыта нетсерфинга и полезной информации (что называется, мир посмотреть). Следующий шаг —создание своей Web-страницы (home page) на сервере провайдера: что называется, себя показать (свою фирму). Ну, а затем пробуждается желание идти к вершинам: сделать свою Интернет-витрину чуткой к желанию клиента и управляемой им. И, наконец, розовая мечта — виртуальный магазин с электронной формой продаж (или, на худой конец, заказов).

Самая первая и насущная в этом ряду проблема — установка по выбору посетителя страницы подходящей русской кодировки (из возможных, вообще-то, 5, а практически 2—3).

Если на предыдущем этапе наш бизнесмен познакомился в той или иной степени с HTML (возможно, лишь на уровне восприятия этой аббревиатуры при оплате счета за работу Web-мастера по созданию home page), то теперь из глубин стандарта HTML выдвигается понятие формы (FORM). И тут же выясняется, что формы должны быть обеспечены программами — так называемыми шлюзами, удовлетворяющими протоколу CGI (Common Gateway Interface), в названии которого фигурирует слово "шлюз" (Gateway). Для создания же этих самых программ-шлюзов предназначен замечательный язык программирования интерпретирующего типа PERL (впрочем, наряду с другими языками, указанными ниже). И наконец, наш просвещенный (продвинутый) бизнесмен выясняет (хорошо, если не опытным путем), что использовать CGI-про-



Шлюзы безопасного бизнеса в Интернет

Валерий Беленков

граммы — вовсе не безопасное дело.

Теперь введены и обозначены взаимосвязи всех терминов из заглавия. Цель данной статьи — обрисовать проблему безопасности при использовании CGI-программ и указать Интернет-источники, которые и сами могут помочь, и послужат отправной точкой для поиска необходимой информации.

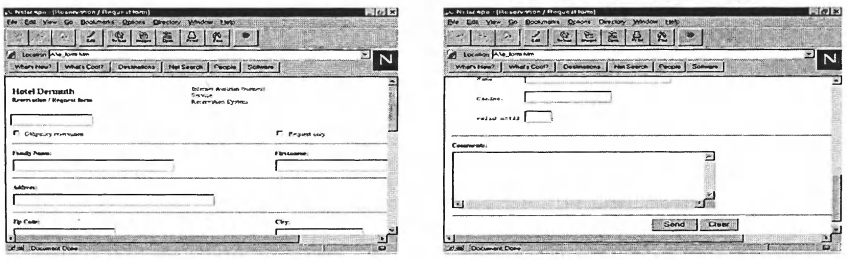
Формы и скрипты

Язык гипертекстовых документов HTML дает возможность вставлять в текст на Web-странице обрамленное именованное и озаглавленное прямоугольное окошко требуемой длины и ширины, вроде графы в форматированном документе (например, бланке заказа), куда удаленный посетитель вашей страницы может занести некоторое значение — либо на выбор из прокручиваемого в окошке списка, либо свободно порождаемое, например, свою фамилию. И это значение, после того как вы щелкнете на клавише SUBMIT (или SEND), тут же передается на ваш сервер или даже прямиком на офисный компьютер. Отличие от e-mail, вызываемой тэгом адресной ссылки с параметром mailto, состоит в том, что в этом случае сообщение строго регламентировано — здесь полная аналогия со спецификацией полей записей базы данных. Такое окошко называется формой и задается при создании HTML-документа тэгом FORM. Комбинацией окошек-форм создается электронный вариант гостевой карточки посетителя, бланка заказа и т.д., вроде карты предварительного заказа номера в отеле, представленной ниже в окне программы-клиента.

На русском языке описание тэга FORM можно найти, например, в http://www.ksu.ru/base/helpuser/form.ru.htm. Информация, занесенная посетителем Web-страницы в формы, адресуется CGI-программе, размещенной на сервере (вашем или вашего провайдера, или вообще провайдера такого рода услуг). Понятие CGI более широко, чем понятие стандарта программ, обслуживающих формы. CGI — это общий стандарт для взаимодействия внешних приложений (программ) с информационными Web-серверами. С помощью CGI-программ можно, взаимодействуя с такими прикладными системами, как система управления базой данных, электронные таблицы, деловая графика и пр., выдавать на экран пользователя динамическую информацию и информацию по его выбору, обеспечивая интерактивные формы работы. В Интернет много источников с информацией о CGI, начиная от публикаций самого стандарта (например, http://www.ksu.ru/base/helpuser/helpcgi/ru.htm или http://www.web.ru/CGI/cgi.html).

Программы-шлюзы пишутся на языках программирования, таких как C/C++, Fortran, PERL, TCL, Unix shell, Visual Basic, AppleScript.

Как и всякие языки программирования, они могут быть охарактеризованы либо как компилирующие, либо как интерпретирующие языки. Тексты, написанные на C/C++ или Fortran, должны быть предварительно оттранслированы и обработаны редактором связей, чтобы получить исполняемый код программы. Именно этот код и размещается обычно в директории /cgi-bin сервера для вызова и исполнения. Scripting-языки PERL, TCL или Unix shell являются языками интерпретирующего типа, и написанный на них код программ (скрипт) является исполняемым (вернее, интерпретируется непосредственно в процессе обращения к программе). Большинство авторов предпочитает писать скрипты, а не транслируемые программы, так как первые легче в отладке и модификации. Заметим, что термин "скрипт" применяется для обозначения всех программ, вызываемых сервером



Заголовок Web-страницы и заполняемые поля формы (слева) и заполняемые форматные поля, поле свободного текстового заполнения (Comments:), клавиши отсылки сообщения (Send) и очистки полей (Clear).

через CGI. Стоит упомянуть и такой облегчающий жизнь программиста инструмент, как библиотеки подпрограмм. Для языка PERL, ориентированного на сетевую работу, разработаны библиотеки cgi-lib.pl Стива Бреннера (http://www.bio.cam.ac.uk/cgi-lib/) и CGI.pm Линкольна Стейна (http://www-genome.wi.mit.edu/ftp/pub/software/WWW/cgi_docs.html).

Вопрос, на чем писать программы-шлюзы, также необходимо рассмотреть с точки зрения обеспечения безопасности.

Где таятся угрозы безопасности в Интернет

Начнем с известного тезиса: угроза безопасности диалектически проистекает из самой природы всемирной сети, предназначенной для всеобщего неограниченного общения. Вы пришли в Сеть, чтобы распространить нечто, являющееся вашей собственностью, на весь мир. И проблема для вас заключается в том, чтобы не потерять контроль над вашей собственностью, чтобы "весь мир", который может быть и шаловливым, и просто завистливо-враждебным, не произвел с вашей собственностью того, чего вы не предвидели и не предусмотрели. Протокол TCP/IP, на котором базируется Интернет, не создавался с заботой о безопасности, следовательно об этом надо подумать обоим — и конечному пользователю, и администратору Web-узла.

Проблема безопасности в Интернет объемна и многогранна. Она затрагивает буквально все аспекты вашего существования в Сети. Для нее не безразличны ни операционная платформа вашего Web-узла (Unix — не лучший выбор), ни выбор программы Web-сервера, ни его конфигурирование, ни язык программирования используемых скриптов, ни размещение их в директории, ни... Наиболее полно все эти вопросы рассмотрены в публикации Линкольна Стейна (http://www-genome.wi.mit.edu/WWW/faqs/wwwsf1.html).

Основным же источником риска являются скрипты. Подчеркнем, не скрипты вообще, а написанные с ошибками, причем далеко не всегда явными. Будучи размещенными на узле, к которому подключен ваш компьютер, эти программы запускаются и работают с данными, посылаемыми из произвольной точки всемирной сети. Ведь Некто из этого безграничного пространства набрел на ваш Web-адрес (а вы сделали все для того, чтобы это происходило как можно чаще) и прочел ее, т.е. получил копию вашего HTML-файла на свой компьютер. И если ваш файл содержит активные элементы, например, уже знакомые нам формы, и если обрабатывающий их скрипт построен безалаберно, (в частности, не контролирует получаемые данные), то этот Некто может исхитриться и включить в отсылаемые данные исполняемые команды, которые сервер послушно выполнит.

В качестве иллюстрации подобного пути злонамеренного вмешательства Пол Филипс в "Safe CGI Programming" (http://www.go2net.com/people/paulp/cgi-security/safe-cgi.txt) описывает ситуацию с модификацией невидимого (hidden) адреса в mailing-форме, позволившей злоумышленнику получить список паролей сервера. Это открыло ему безграничный (привилегированный по отношению к администратору) доступ на сервер. Последствия, очевидно, могут быть самыми катастрофическими, причем как для сервера, так и для пользователя, инициировавшего установку скрипта (впрочем, как и для других конечных пользователей, подключенных к данному узлу).

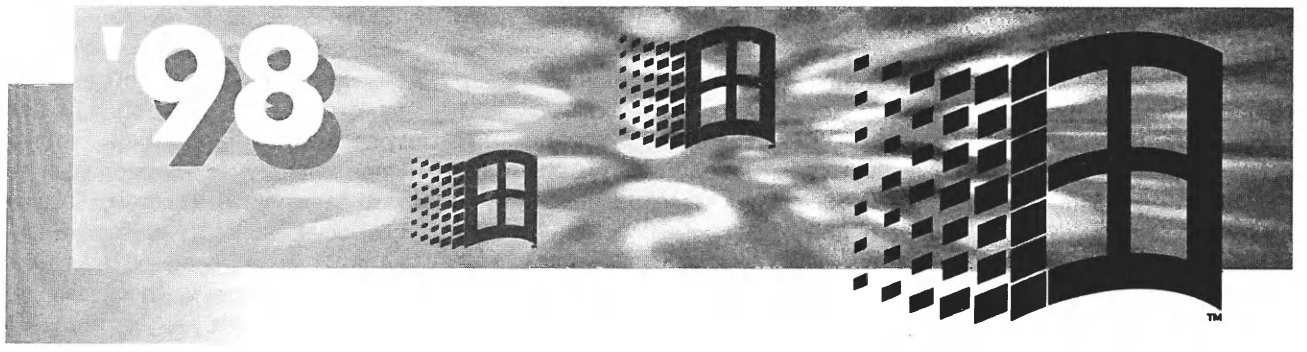
Меры безопасности пользователя

Постараемся подойти к безопасности с позиций неискушенного в программировании и не слишком еще опытного конечного пользователя, желающего придать своему Web-узлу (возможно, виртуальному) или даже только Web-странице элементы комфорта для посетителей, привлекательности и незаурядности. На этом пути от простой on-line брошюры к более интеллектуальному интерфейсу CGI остается по-прежнему относительно простым и легким решением. Интернет может быть безопасным местом, во всяком случае, не более опасным, чем ваш офис. Что от вас потребуется, так это знания и осмотрительность. И если вы встретите опасливое отношение администратора вашей сети к принесенной CGI-программе для обеспечения сервером необходимых вам функций, то к его словам "я должен посмотреть и изучить..." надо отнестись с пониманием.

Одна из рекомендаций Линкольна Стейна — никогда не доверяйте даже известным программам. Если вы не знаете языка программирования, на котором написана программа, и не можете сами проверить, что и как она делает, дайте ее тем, кто может это сделать. Не поручайте разработку ваших сетевых программ неопытным программистам. Следите за информацией об обнаруженных проколах в известных программах и библиотеках. Часто возникает вопрос, влияет ли на безопасность язык программирования, на котором написан скрипт. Хотя в первом приближении программа, написанная на компилирующем языке типа C/C++ в своей исполнимой exe-форме, выглядит более загадочной и недоступной для вмешательства, программирование на PERL, содержащем множество встроенных функций, ликвидирующих бреши безопасности, может быть не менее безопасно и более удобно (даже для отладки).

Оптимистическое заключение

Само по себе использование Common Gateway Interface не является исходно порочным в отношении образования брешей в системе безопасности. Однако использование его требует квалифицированного подхода. Интернет полон многочисленных рекомендаций на эту тему, и ими обязательно следует пользоваться. Приведенные здесь адреса —хорошая стартовая точка.



Кому нужна Windows'98?

Кирилл Кириллов

Несмотря на то, что вся рекламная кампания, приуроченная к выходу Windows'98 обошлась Microsoft "всего лишь в 10 миллионов долларов" (а не в 200 млн, как для Windows'95) новая операционная система "пошла в народ". По словам обозревателей, это событие не сопровождалось особой помпой, и все же около 30 тысяч американцев в полночь выстроились у дверей крупнейших универмагов, желая получить новую ОС.

Поставить ее на свои компьютеры возжелало большое количество самых разнообразных пользователей, от школьников до директоров больших корпораций. Такая готовность приобретать новую операционную систему несомненно не могла не порадовать Microsoft и, особенно, ее рулевого и главного идеолога Билла Гейтса. Но БГ повел себя довольно странно, особенно для тех, кто знаком с обычными методами его работы. Скромно потупив глаза, он сообщил (желающие могли наблюдать это интервью в прямом эфире на Web-узле по адресу http://www.microsoft.com/Windows98/keynote.asp), что корпоративным пользователям беспокоиться нечего, поскольку Microsoft считает Windows'98 своей первой (!?) операционной системой, ориентированной прежде всего на домашнего пользователя. В пору задаться вопросом, а для какого пользователя предназначалась Windows'95? Ведь готовили ее как пригодную для решения самых сложных задач, причем рекламировали на все 200 миллионов, с подсветкой небоскреба Empire State Building в цвета Microsoft и песнями Rolling Stones. А по сути она и для персональной системы вышла на редкость "сырой" и недоработанной.

И действительно, графические возможности "девяносто восьмых" больше подходят для компьютерных игр, нежели для серьезных коммерческих применений. Общий, если так можно выразиться, настрой ОС можно охарактеризовать как развлекательный. Помимо игр, в Windows'98 оптимизирована работа мультимедийных приложений, не говоря уже о работе с Интернет, которая для многих также носит не всегда рабочий характер. Кроме того, в Windows'98 практически отсутствуют средства сетевого администрирования, необходимые для работы корпоративных информационных систем. Вот почему компания Microsoft постаралась остудить пыл многих бизнес-пользователей и большую часть компьютерной прессы, заявив, что им, то есть бизнес-пользователям, лучше установить Windows NT 4.0. Для крупных корпоративных пользователей это, конечно, единственное решение, если речь идет только о продуктах Microsoft. Но для небольшого офиса с четырьмя-пятью компьютерами установка NT сродни стрельбе из пушки по воробьям, тем более, что без грамотного системного администратора в данном случае не обойтись.

Как и ее предшественница, Windows'98 может работать с локальной сетью. Причем делает это гораздо лучше и надежнее, в основном благодаря более "чуткому" отношению к установленным на компьютер устройствам. Тем более, что с момента выхода Windows'95 появилось множество таких сетевых адаптеров, о которых три года назад никто даже и не думал. Устранены и мелкие неприятности, характерные для "девяносто пятых". Например, значительно ускорено оповещение о входе/выходе компьютера из сети, нет долгих простоев перед выключением компьютера. Каждый отдельно взятый ПК стал нормально видеть "Всю сеть", и сакраментальная фраза "Сеть недоступна", кажется, отошла в прошлое. В общем, перечислять можно еще достаточно долго.

Единственная неприятность — плохая совместимость с Windows'98 старых, 16-битных сетевых адаптеров и сетевого программного обеспечения более ранних версий. Из самых известных пакетов сетевого ПО, с которыми Windows'98 работа-

ет заведомо некорректно, можно отметить Vines16, все версии ниже 7.1, и Netware Client for Microsoft Networks, версии ниже 3.11. Разработчики настоятельно не рекомендуют использовать версии Client 32 ниже 2.2. и Lantastic 32 ниже 7.0. Совсем не поддерживаются все версии Client 32 for DOS/Win31, Lantastic 16, а также драйверы VLM/NetX (ipx.com) и TCP 16-разрядные стеки. Такое отношение разработчиков к морально устаревшим устройствам и программам наверняка не понравится многим пользователям, поскольку модернизация означает дополнительные расходы. Но, с другой стороны, заставляет поддерживать вычислительную базу предприятия на современном техническом уровне. Если и рассматривать Windows'98 как сетевую операционную систему, то только в том случае, если необходимо найти замену Windows'95.

Разработчики Windows'98 постарались также откреститься от "позором заклейменного" DOS-овского прошлого. Если в Windows'95 осуществлялась поддержка этих программ через Share (Share.exe), то теперь они работают на общих основаниях. К тому же в новой операционной системе и многих продуктах Microsoft последнего выпуска не сохранена совместимость со старыми, особенно DOS-версиями многих программных продуктов (Word, WordPad и т.д.).

Не секрет, что Windows NT параноидальна. Любое подозрительное или незнакомое действие расценивается ею как попытка нарушить систему защиты и попортить самое ценное, информацию, а потому пресекается самым жестоким образом. Поэтому даже такие "противоправные" действия, как, например, запуск компьютерных игр — дело весьма неблагодарное. А что греха таить, многие сотрудники любят "побаловаться" с компьютером в свободное время.

Таким образом, если вам нужна надежность, ваш выбор — Windows NT, но если в работе требуется определенная гибкость, без Windows'98 не обойтись (хотя в мире существует большое количество операционных систем, успешно совмещающих и то, и другое, но разве за Microsoft угонишься?). А те, кто будет приобретать "десктопы" и, особенно, "ноутбуки", которым NT вообще ни к чему, автоматически перейдут на Windows'98, поскольку эта операционная система поставляется в базовом комплекте такими фирмами, как IBM и COMPAQ.

В Windows'98 значительно доработаны и усилены механизмы защиты. Теперь система может сама и без перезагрузки избавляться от большинства процессов, мешающих (с ее точки зрения) нормальной работе. "Отлавливаются" даже программы, которые, будучи запущенными под Windows'95 и OSR2, не вызывали моментальных сбоев, а

Опять девяносто пять!

Точнее даже "девяносто пять"/"девяносто восемь". Не дают покоя продукты Microsoft народным умельцам. Не так давно семейство макровирусов обрушилось на Word и Access. Особых потерь никто не понес, но приятного было мало. А сейчас — новая напасть. В некоторых европейских странах замечен полиморфный резидентный файлово-загрузочный вирус для Windows'95, получивший название Win95.Inca.

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код различными путями, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Расшифровщики полиморфных вирусов самомодифицирующиеся. Цель такого шифрования проста. Имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже во время исполнения. При этом возможны варианты: он может расшифровать всего себя сразу, либо выполнить такую расшифровку "по ходу дела", а может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Объектом атаки этого вируса стали EXE-файлы в формате PE (Portable executable), применяемые в операционных системах Windows 95/98, и загрузочные сектора гибких дисков. Вирус Win95.Inca паразитирует на EXE, но не препятствует их работе. Но он является так называемым вирусом-червем для архивов ARJ, LHA, LZH, PAK, RAR и ZIP, а также для программы mIRC32. Термин вирус-червь означает, что программы подобного рода "прогрызают" расположенные на физическом носителе файлы, изменяя небольшие участки в записи данных или кодов на своем пути. После того, как над архивным файлом поработал такой "червячок", разархивировать его будет, скорее всего, невозможно.

Если на компьютере был запущен на выполнение инфицированный EXE-файл, вирус получает управление, и специальная часть расшифровывает его основной код, хранящийся в виде таблицы индексов или смещений байтов тела вирусной программы. Поэтому размер самой программы весьма невелик. При запуске специальная часть осуществляет подстановку байтов основной программы на место их индексов или смещений. После того, как программа готова, она атакует функции в KERNEL32.DLL и создает на диске C:\ файл с названием W95INCA.COM. Это, по сути, и есть основная вирусная программа. Затем созданный

потихоньку "съедали" ресурсы системы, вызывая ее остановку через несколько часов работы. Обидно, конечно, если запущенный в фоновом режиме "кривой" проигрыватель аудиофайлов вызывает сбой в системе и уничтожает работу последнего получаса по набору и редактированию какого-нибудь документа.

Похоже, нам не удастся обойтись без Windows'98. Многие разработчики программного обеспечения вовсю занимаются адаптацией старых и написанием новых программ под новую ОС. Самые известные из них — следующая версия "оффиса", MSOffice 2000 (пока только бета, в которой большинство компонентов либо не работает, либо работает неправильно) и Internet Explorer 5.0 (альфа-версия). Если кого интересует более конкретная информация по MSOffice 2000, можно посетить http://www.zdnet.ru, там "расписано", что в нем есть и что работает на сегодняшний день. Что касается IE 5.0., то получился он не хуже четвертого. Лучше ли, по альфа-версии с полной уверенностью сказать трудно.

Некоторую настороженность вызывает тот факт, что всего через неделю после того, как официально был спущен на воду корабль Windows'98 (любимое выражение БГ), к передаче на бета-тестирование был готов комплект модернизации Service Pack 1 для Windows'98. Microsoft рассматривает SP1 как комплект расширения возможностей ОС в сторону мультимедиа, содержащий те возможности, которые еще не были окончательно готовы к моменту выпуска Windows'98. В частности, в него вошел ряд новых графических интерфейсов, поддержка новой электронной программы передач WebTV и дополнительных плат телевизионных тюнеров для компьютера.

Все же этот факт заставляет насторожиться. Если перефразировать к теме известную поговорку, звучать она будет так: "Service Pack без ошибок не бывает". В то же время, официальные представители корпорации отрицали, что исправляемых в этом комплекте модернизации ошибок много и что среди них есть крупные.

Справедливости ради надо отметить, что за несколько месяцев работы с Windows'98 ни одной серьезной ошибки обнаружено не было. Похоже, Microsoft в конце концов, сделала то, что обещала, и Windows'98 воплотила в себе некогда широко разрекламированные, но оказавшиеся призрачными, достоинства Windows'95.

Примечание редакции

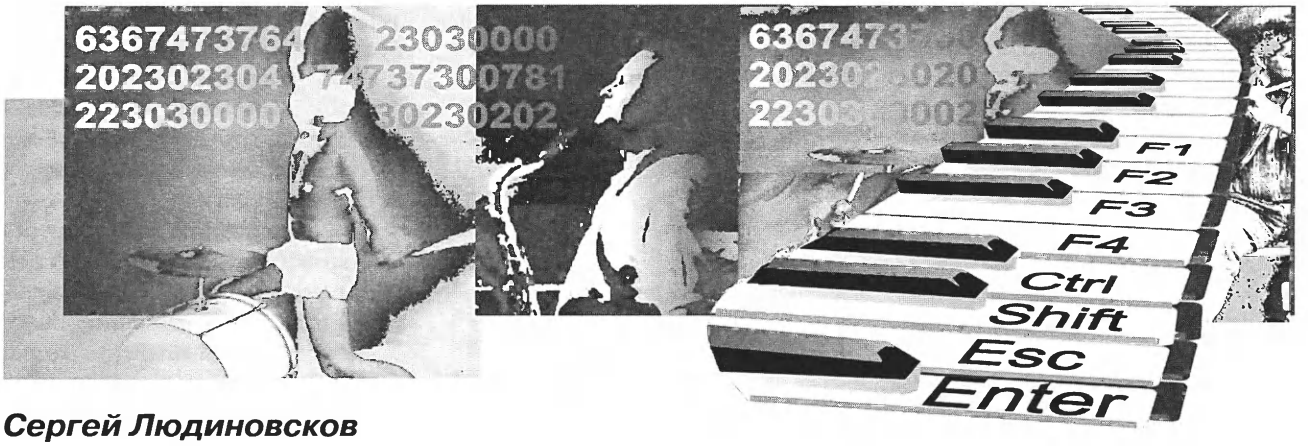
Мнения на этот счет высказываются самые разнообразные. Так, на сайте компании Matrox опубликована сверхкороткая рецензия на Windows'98: "Install. Uninstall".

файл закрывается, запускается вирусом на исполнение, а после выполнения программой необходимых действий удаляется. Далее вирус передает управление инфицированному PE-файлу — вирусоносителю. Запущенный на выполнение файл C:\W95INCA.COM определяет директорию, в которой содержится Windows (WINDIR), и пытается создать в каталоге \WINDOWS\SYSTEM файл с именем FONO98.VXD. Если попытка оказывается удачной, то в файле SYSTEM.INI вирус "прописывает" ссылку на этот файл, и после перезагрузки системы и новом старте Windows вирусный VxD-драйвер FONO98.VXD загружается системой в память и начинает распространять свои копии по другим PE-EXE-файлам. Это дает возможность классифицировать Win95.Inca как "медленный полиморфик".

Далее вирус "перехватывает" IFSMgr FileSystemApiHook и Int 13h (дисковые операции), устанавливая на них собственные обработчики событий, и берет на себя контроль над открытием файлов. При открытии файлов соответствующих типов (EXE и SCR) вирус проверяет их внутренний формат и, если они являются Portable executable, заражает их, создав дополнительную кодовую секцию со случайным именем в заголовке PE-файла и записывая в ее область свой полиморфный код. При открытии архивных файлов с расширениями LHA, LZH, PAK, ZIP, ARJ или RAR вирус дописывает к ним свой 16-разрядный полиморфный код (червь) в формате COM-файла и модифицирует заголовки архивных файлов таким образом, что сам вирус-червь оказывается помещенным в архив. При запуске файла MIRC32.EXE (программа для "разговора" в Интернет) файлы mIRC-червя и самого вируса пересылаются на компьютеры всех участников "разговора".

При работе с зараженным флоппи-диском вирусный обработчик дисковых операций Int 13h контролирует чтение загрузочного сектора флоппи-диска A: или B: и по возможности заражает его, заместив оригинальный загрузчик своим, полиморфным, при это записывая на диск еще и свои копии. При загрузке системы с инфицированного флоппи-диска вирусный загрузчик получит управление и перепишет из секторов диска в память весь свой код. А дальше процесс пойдет по уже знакомому сценарию.

Вероятность заразиться этим вирусом для наших пользователей, к сожалению, достаточно велика — покупка нелицензионного, непроверенного программного обеспечения, общение через mIRC, да мало ли еще что. Последствия работы вируса весьма неприятны: нарушение целостности и частичная или полная потеря данных. Для "отлова" вируса уже существует несколько программ, в основном это продукция фирмы "Диалог Наука". Судя по "заявлениям для прессы", сделанным этой компанией, при использовании ревизора диска ADinf появление вируса Win95.Inca на компьютере будет немедленно обнаружено. Если же таких программ под рукой нет, а с данными на вашем компьютере происходит что то неладное, просто загляните в каталог \WINDOWS\SYSTEM. Если там есть файл с именем FONO98.VXD, значит, в нем определенно "живет" Win95.Inca.



Сергей Людиновсков

Компьютер — композиторам

Когда начинаешь задумываться о судьбах цивилизации, почему-то на ум сразу приходит то парадоксальное обстоятельство, что любое, даже самое очевидное ее достижение с огромным трудом завоевывает (именно ЗАВОЕВЫВАЕТ) свое место под солнцем. Не стали исключением и персональные компьютеры — все-таки медленно они приживаются в нашей повседневной жизни. И дело здесь совсем не в объективных трудностях технического прогресса и даже в не очевидных несовершенствах общества, а в том, что подавляющее большинство людей даже в развитых, преуспевающих странах внутренне к этому не готово. К сожалению (здесь нет и намека на иронию), компьютер является безжалостным "судьей", когда дело касается личностного разгильдяйства, непоследовательности, умения уживаться с ложью в большом и малом. Впрочем, я далек от желания обсуждать столь глобальные и сложные проблемы и хотел бы затронуть более узкую тему — использование современных информационных технологий в творческом процессе.

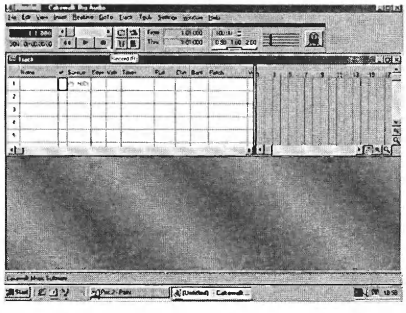
Очень часто даже взрослым солидным людям приходится напоминать, что все, чем пользуется человечество, первоначально было создано некими авторами. Совершенно очевидно, что необходимо создать элементарные условия для их творчества, и в этом, между прочим, заинтересовано все без исключения общество. На самом же деле, тем более в наше непростое время, тем более в нашей непростой стране, все сделано и делается в этом плане с точностью до наоборот. Возьмем, к примеру, музыкальное творчество. Ситуация в нашем городе (Петербург —культурная столица?!) крайне тяжелая. Мало того, что композитор в творческих муках должен родить музыкальное произведение, он должен к тому же иметь и немалое гражданское мужество, чтобы запустить его в тираж, и, кстати, немалые деньги! А в это время теле- и радиоэфир, прилавки музыкальных магазинов и ларьков заполняет низкокачественная, безликая и унылая продукция. Подавляющее большинство наших авторов, которые имеют действительно интересный в художественном, да и в коммерческом плане музыкальный материал, больше, как правило, не имеют ничего: ни признания, ни денег, ни связей, а у многих, увы, отсутствует даже чувство собственного достоинства.

Предельно четко вырисовывается замкнутый круг: нет денег на тиражирование — нет тиражирования — нет денег. А это обидно, тем более, что самый примитивный расчет дает следующие результаты: всего лишь одна песня (0,1) нашего отечественного композитора, попади она в альбом (20000000 экземпляров) какой-нибудь западной звезды типа Хулио Иглесиаса, может дать только авторский гонорар (8%), который перевалит за 1000000 долларов. Понятно, что это верхняя планка, но тем не менее. Откровенно говоря, наши композиторы о таких доходах пока и не мечтают, а зря... На родной совковый шоу-бизнес, который работает по принципу "чем хуже — тем лучше", надежд никаких. Печально, но такова суровая реальность.

И все-таки виден свет в конце туннеля. В настоящее время у композиторов (и не только у них) появилась реальная возможность реализовать свои даже грандиозные творческие проекты при помощи новейших информационных технологий. Персональный компьютер даже достаточно скромной модели позволяет получить высококачественный конечный продукт — фонограмму. Необходимо отметить крайне важную деталь: теперь возможности для плодотворного творчества есть даже у людей, не имеющих музы-

кального образования и не умеющих играть на музыкальных инструментах. На первый план выходит чувство композиции. Современные программы — музыкальные редакторы — предоставляют широкие возможности по написанию разнообразной музыки, будь то незатейливая песенка или полновесное симфоническое произведение. При этом, если композитор разорится на CD-рекордер, он сможет "шлепать" компакт-диски прямо у себя дома и периодически носить их в ближайший киоск, чтобы выставить свои произведения на реализацию. А если организовать в Интернет виртуальный магазин по продаже интеллектуальной собственности, то "запоют" (читай, останутся без "кормушки") всяческие бессовестно-бездарные деятели от музыкального шоу-бизнеса.

Еще один кардинально важный момент, особенно в жанре популярной музыки: если автор хочет, чтобы песня быстро "пошла в народ", ее необходимо "протолкнуть" через телевидение, а для этого необходим



приемлемый видеоряд. Наши родные клипмейкеры заламывают такие не нашинские цены, что даже у раскрученных звезд часто наворачиваются слезы, что уж говорить о начинающих композиторах! При этом качество видеоряда в творческом отношении крайне низкое, даже существенные элементы видеоряда иногда просто-напросто не попадают в такт музыкальной композиции. Видимо, наличие элементарного слуха не является для некоторых видеотворцов обязательным условием. К тому же, как правило, все "соучастники" — аранжировщики, студийные музыканты, вокалисты и, в особенности, клипмейкеры — решают свои "проблемы" самовыражения, к сожалению, в ущерб стилистической целостности произведения. Так что, если композитор хочет, чтобы его детище выглядело достойно, опять же нужно брать "быка за рога" —садиться за компьютер и осваивать программы видеомонтажа и компьютерной графики.

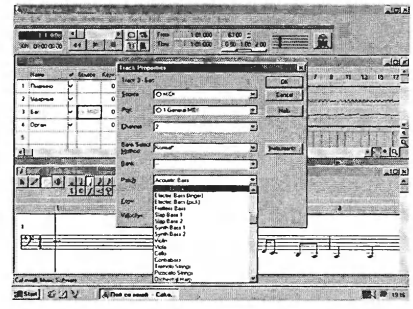
Теперь от риторического запала перейду непосредственно к рутинной работе и постараюсь показать, как начинающие композиторы могут решать свои творческие проблемы собственными силами. Но для начала позволю себе высказать несколько слов общего характера, адресованных в первую очередь композиторам. Уважаемые коллеги, помните, что если автор жаждет популярности, он должен научиться создавать в первую очередь популярную музыку. Если мелодия быстро забывается, то и об авторе тоже недолго будут помнить. Так что, прежде, чем браться за это, вообще говоря, непростое дело, хорошенько подумайте, готовы ли вы целеустремленно, терпеливо, шаг за шагом идти к заветной цели. Лично я глубоко убежден, что если в голове автора рождаются красивые мелодии, то для того, чтобы их услышали, не жалко никаких усилий.

Итак, начнем. Будем исходить из того, что у вас уже имеется персональный компьютер не хуже Pentium-100, звуковая карта и MIDI-клавиатура.

Cakewalk Pro Audio 6.1 — легкая прогулка

Одним из самых популярных музыкальных редакторов в мире сейчас является Cakewalk Pro Audio 6.1. Те, кто только сейчас начинает использовать современные компьютерные технологии в своем музыкальном творчестве, без труда могут сделать несложную аранжировку в этой среде.

Надеюсь, что загружать программы в Windows вы уже научились. После запуска Cakewalk Pro Audio 6.1 появляется главное окно программы. Оно имеет в основном стандартный вид Windows-приложения. Сразу бросается в глаза ряд характерных кнопок. Аккуратно подведите к ним указатель мышки, чтобы появились подсказки.



Record (R) — запись. Это как раз та желанная кнопка, на которую так хочется нажать. Но обождите чуть-чуть, сначала надо хорошенько рассмотреть другие кнопки, а также научиться устанавливать звучание различных инструментов.

Идем дальше.

Play (Spacebar) — воспроизведение.

Rewind (W) — быстрый возврат в начало.

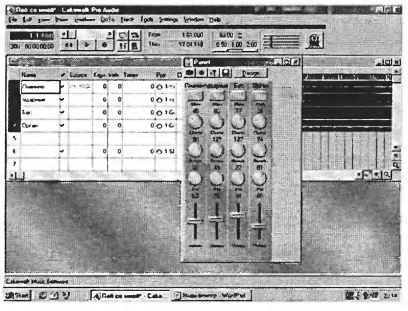
Над этими кнопками расположена линейка прокрутки. Поскольку терминология в области компьютерной музыки пока еще до конца не установилась, будем для простоты употреблять понятие "фонограмма". При помощи линейки прокрутки можно перемещаться по фонограмме, а точнее — по ее графическому образу. По существу процесс создания фонограммы в Cakewalk Pro Audio 6.1 осуществляется во многом путем различных графических манипуляций. Не буду обременять читателей перечислением всех возможностей Cakewalk Pro Audio 6.1, это займет слишком много места и времени.

Под вышеназванными кнопками вы увидите некую таблицу. На пересечении 1-й строки и столбца Source установите курсор мышки и дважды щелкните левой кнопкой, чтобы открылось диалоговое окно Track Properties —установки параметров дорожки. Нажмите кнопку в поле

Patch, и перед вами откроется весь набор инструментов, который имеется на вашей карте. Выбирайте любой — и играйте на здоровье.

После того, как вам это слегка надоест, вы можете воспользоваться заветной кнопкой Record (R) — запись. Надо сказать, что Cakewalk Pro Audio 6.1 является как бы многоканальным цифровым "магнитофоном". Попробуйте записать, к примеру, партию фортепиано на 1-ю дорожку. На 2-ю запишите партию ударных и так далее. Чтобы все это вместе прозвучало, необходимо присвоить дорожкам различные номера каналов от 1 до 16. Обратите внимание: 10-й канал закреплен за ударными.

Вы можете также, находясь на определенной дорожке (красная рамка), вызвать программу-нотатор — Staff. Для этого необходимо в меню нажать на кнопку View, установить курсор на New и нажать на Staff. После того, как вы налюбуетесь нотной записью своего произведения, можете добавить к нему последние штрихи — установить уровни громкости по всем дорожкам и добавить



аудиоэффекты. В Cakewalk Pro Audio 6.1 это делается довольно просто при помощи микшера. Пометьте мышкой все дорожки, устанавливая курсор на номера дорожек и делая щелчок левой кнопкой. После этого необходимо в меню нажать на кнопку View, установить курсор на New и нажать на Panel — появится панель микшера — далее крутите ручки.

Когда вы добьетесь нужного результата, нажмите на кнопку "фотоаппарат", чтобы зафиксировать полученные значения. Ну вот, как видите, наша с вами "прогулка" оказалась, как я и обещал, совсем не тяжелой. Воистину сказано — лиха беда начало. Не забудьте сохранить полученный сим непосильным трудом файл. И, как говорится, творческих успехов!

В заключение хочется пожелать нашим композиторам мужества, целеустремленности и хоть чуть-чуть удачи. Как ни крути, а время работает на нас, уважаемые сочинители великих произведений!

Продолжение следует

Словарь компьютерного фольклора

Продолжение. Начало см. "Магия ПК" № 3 – 9.

P

Разрезать диск — разбить физический диск на несколько логических.

Реаниматор — хакер, способный оживить безнадежно усопшую машину, несмотря на все ее сопротивление.

Репа — RIP-протокол. Из классики: "Посадил дед RIPку, тянет-потянет, а вытянуть — no carrier".

Реплюй — ответ на сообщение в почте (reply).

Рулевой — программа-оболочка DOS Navigator. Синонимы: Нафигатор, Пофигатор.

C

Самовар — программа, написанная по принципу Shareware.

Сантехника — продукция фирмы Sun Microsystems. Из зарубежной классики: "Nothing new under the Sun".

Сапер — сопроцессор (математический, музыкальный). Синоним: копик.

Сапог — тот, кто работает на VAX'е. Сарай — весьма ресурсоемкое программное обеспечение.

Сваха — SVGA-карта.

Светофор — внешний модем с огоньками.

Светофорная сборка — красная сборка, желтые плитки, зеленый BIOS.

Свечи — переключатели (switches).

Святые Робинзоны — фирма Santa Cruz Operation.

Сексельпильный — фанат Excel'а.

Синие таблички — программа Norton Commander. Один ламер сказал: "Включил я комп, загрузился Нортон, смотрю, у меня на одной панели C:\ и на второй C:\, так я с одного C:\ все стер. Нафига мне два C:\!?".

Сисемблер — программа на Си со вставками на ассемблере.

Сисоп — системный оператор станции. Поговорки: "Сисоп спит, почта идет", "Не будите спящего Сисопа". Из классики: "Что, сисоп, сидишь невесел, что ты Windows свой повесил?"

Скалить — выполнять команду SCALE.

Склевать — обработать командой SKEW (в 3DStudio & Graph-Editors).

Скос — UNIX фирмы SCO. Синоним: скошенный юникс.

Скрим Трахер — музыкальный редактор Scream Tracker. Синонимы: Воплеследопыт, Орущий буксир.

Скулить — работать с SQL-процессами.

Смерть вам! — модем Smart One.

Совок-с — музыкальная псевдоприставка COVOX.

Совт — советский софт.

Сосулька — Soft-Ice (дебаггер).

Стеклить — инсталлировать Windows. Говорят: "Тамбовский волк пусть стеклит тебе Windows!"

Стервер — сетевой сервер. Поговорка: "Все дороги ведут на Стервер".

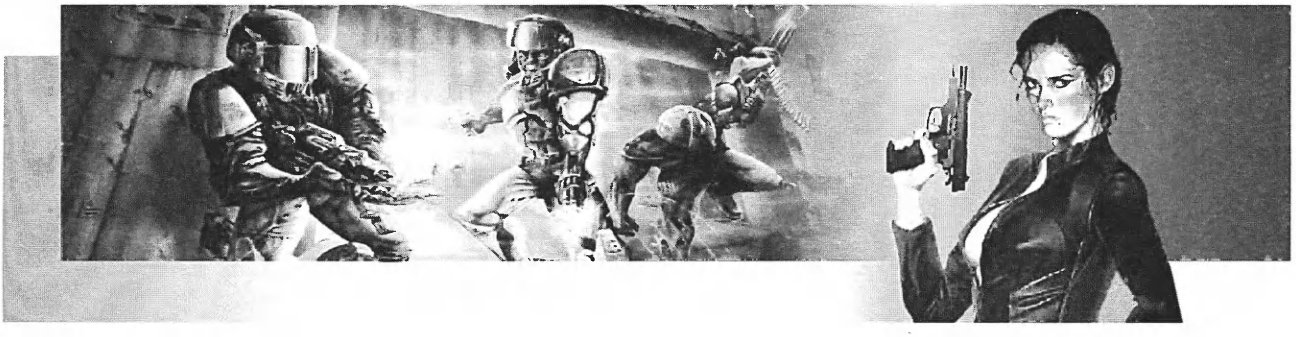
Стремный файл — файл на стриммере.

Ступор — место зависа в программе.

Стучать форточками — работать в Windows.

Сутенеры — связисты, телефонисты.

Сухопутный проц — процессор, не поддерживающий операции с плавающей точкой.

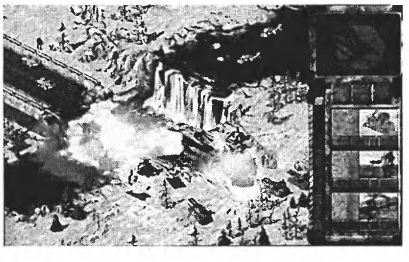


Тибериумное солнышко

Для поклонников стратегических игр в реальном времени (real time strategy) настают "горячие" времена. В октябре 1998 выходит C&C 2: Tiberium Sun.

Эту игру все ожидают с нетерпением. Стратеги и тактики компьютерных баталий уже устали от безликих игр, вышедших в последние несколько лет (Starcraft, Red Alert), которые, по сути, всего лишь улучшенные версии старых "хитов". С выходом Tiberium Sun ситуация должна измениться. Список новшеств очень внушителен.

Захватывающая графика, включающая 3D-объекты, реальные световые эффекты. Разнообразные пейзажи леса, города, пустыни выполнены с потрясающей детализацией. Максимальное разрешение, которое будет поддерживать Tiberium Sun, — 1024x768.



Меняющаяся погода и случайные атмосферные явления могут повредить боевые единицы, конструкции, орудийные башни и т.д. В случае ионного шторма отключится все HI-техническое оборудование. Эти шторма могут также нейтрализовать ховеры — летательные аппараты — и лазерное оружие как ваше, так и противника. В этой игре прогноз погоды становится стратегическим фактором.

Ландшафт игры стал динамическим (когда что-либо взрывается, то остается воронка). Лед может проломиться под тяжестью техники, поврежденные распорки моста рухнут в любую минуту, лес сгорит вместе с войсками.

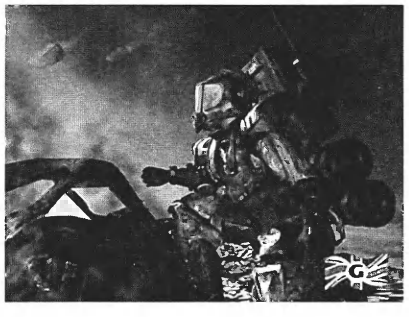
Новый, синий тибериум очень энергетичен и взрывоопасен при высокой концентрации на ограниченной площади. Он может уничтожить не только солдат, но даже харвестеры — комбайны, предназначенные для уборки этого минерала.

Боевой опыт полководца растет в ходе кампании, что делает его войска более эффективными в бою.

Коммандос теперь стали наемниками. Они будут работать на вас, если вы имеете деньги, оружие или медикаменты, в зависимости от условий. Нищим спецвойска служить не будут.

Игра, как и все ее предшественники от Westwood Studios (Command & Conquer с "крутым" дополнением Covert Operations и C&C: Red Alert с несколькими новшествами, которые не только стали популярны, но и оказали существенное влияние на другие игровые проекты в жанре RTS), имеет нелинейную структуру миссий, которая гарантирует относительную новизну каждой последующей кампании.

Multiplayer поддерживает 4 игрока по Интернет и 8 по локальной сети, а также создание кланов и войну против кланов из нескольких рас, управляемых компьютером. Пока объявлены 3 расы: GDI (Global Defender Initiative), NOD и The Forgotten ("забытые" — интересно, кто мог забыть о таком воинственном народе?), но ходит слушок о четвертой. Именно эта загадочная раса и направила тибериум на Землю!

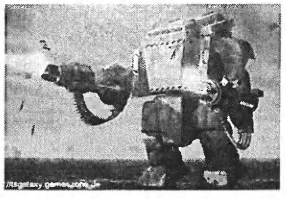


А теперь, если сказанное выше вас не заинтересовало, приведу несколько конкретных примеров того, с чем можно встретиться под сол-

нышком, затуманенным испарениями тибериума.

— На орбите будет находиться огромное космическое судно Kodiak, воюющее на стороне GDI.

— Боевые единицы могут вмерзать в лед при понижении температуры. База может "поплыть" при неожиданном наводнении.



— Новые юниты, "прыгающие" солдаты с реактивными ранцами могут стать настоящим сюрпризом для врага.

— Иногда вы будете получать бронепоезда. Их можно использовать для вторжения на вражескую базу, но нельзя строить.

— Некоторые коммандос могут захватывать транспортные средства.

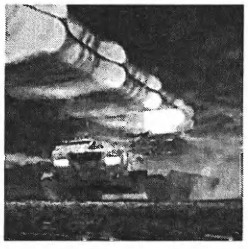
— Главный компьютер одной из рас (предположительно NOD) может заслать игрокам дезинформацию.

— Техника, идущая высокогорными тропами, может скатиться в пропасть.

— Некоторые юниты могут окапываться, чтобы увеличить свой защитный потенциал.

— Солдаты набирают боевой опыт по ходу игры. Ветераны будут более подвижными и сильными, чем "салаги", но, к сожалению, их нельзя будет взять с собой в следующую миссию.

Скриншоты на множестве сайтов в Интернет поражают детальностью и красочностью, как и список новшеств, надеюсь, далеко неполный. Правда, нет толковой информации по движку игры, но хиты от Westwood Studios всегда отличались самым "продвинутым" движком из всех похожих творений. Скорее всего, и на этот раз "Вествудовцы" в грязь лицом не ударят — гордость не позволит.



Т

Тапер — тот, в чью машину вставлен стриммер, используемый другими.

Твердая Рука — StrongARM (совместное пр-во DEC и Advanced Risc Machines Ltd).

Телиться — подсоединяться по Telnet.

Тербятник — модем, имеющий протокол terbo.

Т-мыло — почтовая программа T-MAIL. Принцип T-Mail: "Хватит и половины пакета".

Топтать — архивировать.

Тормозит — очень медленно работает (или соображает). Поговорка: "Тормоз — не девайс, а состояние души".

Тощая — Motherboard для корпусов типа Slim.

Трезубец — Trident.

Трехдюймовка, трехлинейка — дискета 3.5"

Тройка, трешка — IBM PC AT 386.

Труба — канал передачи данных. Говорят: "труба 64 кбод".

Трупосборщик — Turbo Assembler.

У

Убить — стереть что-либо.

Угол — винчестер Conner Peripherials.

Укнутый — запакованный архиватором UC.

Ультрадавка — архиватор UC II.

Уних — операционная система UNIX. Поговорки: "Уних у них, а у нас демос", "Не всякому человеку даже Уних к лицу". Из документации: "UNIX is user friendly. It's just selective about who its friends are...".

Усер бряк — прерывание программы, выполненное пользователем (user brake).

Утоптанный — архивированный.

Утюжить — сканировать ручным сканером.

Утя — утилита. 1. Полезная программа. 2. Общее название старых программ, которые жалко выкинуть.

Ухопроцессор — Echoprocessor.

Ушастый — накопитель на 8" дискетах.

Ф

Фаза Луны — обычное объяснение для неожиданно заработавшей машины или программы, которая вдруг ожила и принялась делать то, что от нее требуется.

Федора — почтовая программа Front Door. Синонимы: Фронда, фроня.

Феня — неожиданное действие программы, вызывающее удивление у составившего ее программиста. Возникает обычно во время генерального тестирования программы или демонстрации ее заказчику. Как правило, зачисляется в разряд недокументированных возможностей.

Филе — файл (file). Поговорка: "Филе к делу не пришьешь".

Флейм — ругань в эхоконференциях. Поговорка: "Не плюй в MAIL — вылетит, не поймаешь".

Флоппинет — обмен данными между пользователями посредством дискет. Поговорка: "Флоп модему не товарищ".

Фокусник — программист, пишущий на FoxPro.

Фонарь — светодиод.

Форточки для сараев — Windows for WorkHalls.

Форточки колхозные — MS Windows for WorkGroup. Синоним: Групповуха под Винды.

Фреза — программа-упаковщик (freeze).

Фрекать — скачать файл со станции командой file request. Синоним: хрюкнуть.

Фря — операционная система FreeBSD.

Издание зарегистрировано Северо-Западным региональным управлениемкомитета РФ по печати (С.-Петербург). Регистрационное свидетельство П-2745 от 28.10.97.
Учредитель: ООО "Техно-ПРЕСС". Адрес редакции: 198097, СПб, пр.Стачек, 47, тел.(812) 184-9868, 219-9772. Гл.редактор А. Альбов.
Подписано в печать 02.10.98. Тираж 7 000 экз. Цена свободная. Отпечатано в типографии "Турусел".

качество гарантируется ПЕТЕРЛИНК-холдингом

ОТЛИЧНЫЙ ИНТЕРНЕТ ПО НИЗКИМ ЦЕНАМ

RCom COMPANY

В ВАШУ ИНТЕРНЕТ-КОЛЛЕКЦИЮ

В.О., 14-я линия, д.39, к.215, тел./факс: 218-18-35, e-mail: info@rcom.ru, URL: http://www.rcom.ru