Разумные карты
начинают наступление по всему фронту

М. Гольцова

Как известно, разумные карты впервые появились в Соединенных Штатах. Испытания первых стандартных пластиковых карт с встроенной ИС, содержащей микропроцессор и устройство памяти, американская фирма MasterCard International, первопроходец в производстве электронных платежных средств, провела еще в марте 1985 года. Однако до последнего времени разработки в этой области в основном были сосредоточены в Западной Европе, в частности во Франции. Сегодня интерес к разумным картам стремительно растет во всем мире, в том числе и в США. Чем же это объясняется?

Области применения разумных карт чрезвычайно разнообразны. Первоначально они использовались главным образом при проведении банковских операций (кредитных и дебитных) и оплате телефонных переговоров. Сегодня уже трудно найти сферу, где для тех или иных целей не использовались бы разумные карты. С их помощью расплачиваются за различные услуги, оплачивают дорожные сборы, они широко применяются как средство контроля доступа, идентификации личности и т.п. Разумные карты как средство ведения истории болезни пациента начинают осваивать и сферу здравоохранения. При этом они снабжаются дополнительным кодом, известным только врачу. По прогнозам, объем операций, выполняемых с помощью разумных карт, к 2005 году увеличится втрое и составит 30 млрд. транзакций, из которых 25 млрд. будут связаны с оплатой услуг телефонных операторов и сети Internet.

Сколько стоит разумная карта? Ответить на этот вопрос столь же трудно, как и на вопрос о стоимости автомобиля, если не уточнить, о каком автомобиле идет речь: о подержанном “фольксвагене” или новом “роллс-ройсе”. В зависимости от выполняемых функций и объема закупок стоимость разумных карт колеблется от 1 до 20 долларов.

По данным фирмы Dataquest, в 1995 году в мире было продано 544 млн. разумных карт. Ожидается, что к 2001 году объем их потребления возрастет до 3,4 млрд. шт., а производства – до 2 млрд. Львиная доля карт на основе ИС (90%) в 1995 году была продана в странах Европы и только 2% — в Северной Америке. К 2001 году европейские страны будут приобретать 30—40% поставляемых на мировой рынок карт, азиатские — 25—30% и США — 20—30%. Более высокий спрос на разумные карты в Западной Европе в значительной степени объясняется относительно дорогими услугами связи в этом регионе. Замена обычных карт разумными позволяет получать разрешение на пользование услугами связи в автономном режиме и тем самым снизить их стоимость. В США, напротив, достаточно разветвленная сеть телекоммуникаций обеспечивает надежное подтверждение права доступа в реальном времени. Поэтому разумные карты не получили здесь широкого распространения, хотя американский деловой мир внимательно следил за их развитием.

В последнее время интерес к разумным картам в США значительно возрос. Этому способствовал целый ряд факторов. Во-первых, по мере отработки технологии стоимость разумных карт снижалась. Во-вторых, благодаря высокой степени защиты данных повысилась их надежность. В-третьих, активно идущие процессы слияния электронных технологий и объединения усилий многих отраслей с целью совершенствования предоставляемых услуг расширяют возможности использования разумных карт как средства получения доступа к этим услугам. И наконец, опыт успешного применения разумных карт в Западной Европе в значительной мере повлиял на формирование в США мнения о том, что они могут эффективно решить многие проблемы обработки информации в различных сферах американского бизнеса.

Одним из следствий этого стало создание организации Smart Card Forum, цель которой — ознакомление общественности с достоинствами разумных карт, их технологией, инновациями, а также оценка возможностей и перспектив их применения. В организацию вошли представители правительственных, финансовых и промышленных групп. В числе участников организации корпорации Visa International, MasterCard International, Bellcore, American Express, Mobil Oil, Gemplus, Schlumberger, Siemens, банки Citibank, Hoag & Eliot, Chase, The American Banker и др.

Сегодня известны два типа разумных карт. Первый представляет собой простую карту с памятью емкостью до 8 Кбайт, в которой зашиты средства защиты данных. Второй тип – это “интеллектуальная” карта с микропроцессорным ядром, ячейками энергонезависимой памяти и небольшим набором специальных аппаратных и программных средств для выполнения определенных функций, в том числе защиты данных. В картах первого типа наряду с персональным идентификационным номером, как правило, содержится только информация об итоговой сумме, оставшейся после платежей. С помощью такой карты ее владелец расплачивается за небольшие покупки путем списания потраченных сумм. После полного списания суммы карту либо выбрасывают, либо продолжают использовать, загрузив в нее новую сумму. Относительно простые разумные карты применяются для относительно простых операций, например для оплаты телефонных разговоров. Такая карта содержит 60 или 120 ячеек памяти, в каждой из которых хранится сумма для оплаты одного телефонного разговора. После сеанса связи ячейка очищается. Карты этого типа могут использоваться и как дебитные при сборе дорожных и транзитных платежей, регистрации документов грузовых перевозок, например отчетности станций взвешивания, транспортных накладных и т.п.

По мнению экспертов Smart Card Forum, истинно “разумной” можно считать лишь карту второго типа. Благодаря микропроцессору она не толь-

ко хранит, но и контролирует доступ к хранимой в ней информации, а также "принимает решения" в соответствии с конкретными нуждами пользователя. Разумная карта имеет собственные коды безопасности. Как и в карты для банковских автоматов, в нее могут быть записаны персональные идентификационные номера, соответствующие коду доступа.

Встроенные в ИС карт обоих типов вычислительные средства обеспечивают защиту хранимой информации от разрушения или несанкционированного доступа. Изъять интегральную схему или заменить содержащуюся там программу невозможно, не повредив ее. Применение карты не требует ручного ввода кода доступа в терминал считывания, поэтому код нельзя подглядеть. Благодаря всем этим мерам потери от мошенничества и краж в банковской сфере Франции при внедрении разумных карт сократились с 0,6 до 0,3%.

По сравнению с магнитными картами, в которых информация записана на внешних магнитных полосках и легко копируется, разумные карты гораздо надежнее. Поэтому они весьма перспективны для получения безопасного доступа к открытым интерактивным системам с помощью таких средств, как переменные шифровальные ключи, скрытые единичные символы и электронные цифровые подписи. Помимо микропроцессорного или запоминающего модуля, разумные карты могут содержать магнитную полоску и штриховой код, причем для считывания данных пригодно традиционное оборудование.

Как и 10—12 лет назад, в разумных картах по-прежнему используются восьмиразрядные CISC-микропроцессоры (типа 8051 или 6805), хотя современная микропроцессорная технология приближается к уровню 64-разрядных устройств. Чтобы преодолеть этот разрыв, с 1993 года по предложению ведущего изготовителя разумных карт – французской фирмы Gemplus в рамках европейской программы ESPRIT реализуется проект создания архитектуры схем для разумных карт и портативных интеллектуальных устройств — Cascade (Chip Architecture for Smart Cards and Portable Intellegent Devices). По оценке участников проекта, к 2000 году продажи микропроцессоров для разумных карт на мировом рынке увеличатся до 300 млн. долл. по сравнению со 150 млн. в 1996-м.

В разумных картах, создаваемых по этому проекту, используются 32-разрядные схемы британской фирмы ARM, специализирующейся в области RISC-микропроцессоров для портативных систем. Процессор последнего поколения ARM7 выполнен на базе ядра, содержащего всего 36 тыс. транзисторов (против 1,2 млн. в схеме микропроцессора i486 фирмы Intel). Схема изготовлена по 0,8-мкм технологии с двухуровневой металлизацией и занимает всего 6 мм^2. Производительность схемы – $28 \cdot 10^6$ команд/с на тактовой частоте 33 МГц. Это, конечно, ниже быстродействия высокопроизводительных микропроцессоров типа Supersparc фирмы Sun, Alpha фирмы DEC или R4000 фирмы MIPS. Но при сравнении по такому показателю, как отношение быстродействия к потребляемой мощности, ARM7 в 5—10 раз превосходит лучшие современные CISC- и RISC-микропроцессоры. О популярности схем фирмы ARM свидетельствует и тот факт, что компания Apple для своего персонального цифрового помощника Newton выбрала ее 32-разрядный RISC-микропроцессор, отличающийся высоким быстродействием, малыми габаритами и потребляемой мощностью.

Применение 32-разрядного микропроцессора фирмы ARM значительно увеличит скорость выполнения сложных расчетов при работе с алгоритмами шифрования. В отличие от устаревших восьмиразрядных CISC-микропроцессоров для процессоров фирмы созданы компиляторы языка высокого уровня (например "Си"), что также способствует увеличению производительности схемы карты. Ячейки памяти на кристалле схемы выполнены по технологии энергонезависимых ЗУ и обеспечивают возможность перезаписи информации. Относительно малое время задержки обработки прерывания и достаточно высокая тактовая частота упрощают реализацию архитектуры с поточной обработкой данных. Данные, хранимые в разумной карте, защищены динамическим кодированием транзакции/операции. Высокое быстродействие микропроцессора позволяет реализовать программы "открытых" криптографических систем, соответствующих требованиям современных средств пользовательского интерфейса.

В настоящее время для защиты данных к операционной системе просто добавляется соответствующая программа, что недостаточно эффективно. Присоединение устройств обработки данных к процессорному ядру в схеме разумной карты существенно повышает степень защиты. Работы по совершенствованию операционной системы и методов защиты данных в рамках проекта Cascade ведут университеты в Лилле (Франция) и Ловайне (Бельгия). Для увеличения объема информации, хранимой выполненными на кристалле ячейками памяти, разработчики используют алгоритмы сжатия данных. Кроме того, в операционную систему включены алгоритмы шифрования открытым ключом, обеспечивающие доступ к системе групп санкционированных пользователей.

Усовершенствованная разумная карта, разрабатываемая по программе Cascade, будет поддерживать такие биометрические функции, как распознавание голоса или отпечатка пальца. Это обеспечит качественно новый уровень защиты от мошенничества, что в свою очередь расширит рынки сбыта разумных карт. Сейчас карты с биометрической защитой используются только в сложных системах охраны важных объектов, поскольку для реализации такой защиты необходимы дорогостоящие высокопроизводительные вычислительные средства. Невысок и уровень защиты таких систем, так как сравнение данных осуществляет терминал, на индикаторе которого, помимо результатов сравнения, воспроизводятся и персональные данные владельца карты. Для повышения степени защиты сравнивать данные должна сама разумная карта. Участники проекта Cascade пытаются реализовать биометрические средства защиты данных в относительно дешевых картах, предназначенных для широкого применения. Биометрические блоки, расположенные на кристалле, будут непосредственно сопрягаться со считывающим терминалом, оснащенным микрофоном или датчиком распознавания отпечатков пальцев.

Биометрические средства защиты разрабатывают две британские фирмы: Neural Computer Sciences, которая предоставит нейронные сети для обработки биометрической информации, получаемой с помощью преобразователя и процесса декодирования; и Domain Dynamics, сосредоточившая усилия на создании инновационной технологии обработки сигналов, пригодной для применения в биометриче-

ских средствах. При разработке последней алгоритмов распознавания сигналов с ограниченной полосой частот, например речи, ставится задача не распознавания содержания сообщения, а отличия одного голосового сигнала от другого. Предлагаемые алгоритмы столь "устойчивы", что могут идентифицировать пользователя даже при некотором искажении голоса из-за простуды или сильного фонового шума. К тому же они требуют гораздо меньшего объема нормативно-справочной информации и вычислительной мощности, чем применяемые ныне.

Важное значение для широкого распространения разумных карт имеют устройства считывания их данных. Сейчас в мире существуют разнообразные системы считывания данных разумных карт: от мощных кассовых терминалов до компактных блоков карманного типа и устройств, подключаемых к персональным компьютерам. Во многом это происходит из-за того, что два ведущих изготовителя разумных карт — Visa и MasterCard — продвигают несовместимые архитектуры систем программного обеспечения. К тому же некоторые крупные корпорации предлагают собственные запатентованные типы разумных карт. Вот почему в ближайшие годы основным требованием к считывающим терминалам будет способность взаимодействовать с разнообразными программными продуктами.

Примером терминала, который способен работать с картами различного типа, является система для магнитных карт австралийской фирмы Intellect. С помощью легко присоединяемого модуля она быстро преобразуется в устройство считывания разумных карт. Именно эта система применяется в процессе экспериментальных работ с повторно загружаемыми картами Visa, проводимых с конца 1997 года в Канаде.

На другом конце спектра находятся считывающие устройства Value-Cheker, созданные фирмой Oki Advanced Products – американским отделением корпорации Oki. Машины этой серии представляют собой компактные считывающие устройства, облегчающие пользователю проверку хранимой в карте суммы и выполнение ряда других операций с помощью персонального компьютера. Участникам конференции Cardtech/Securetech (технологии карт и средств защиты), состоявшейся в США в середине 1997 года, фирма подарила считывающие устройства размером с брелок (габариты — 28,8x70,6x11,7 мм, масса — чуть более 28 г). Устройство работает от двух литиевых батарей и оснащено семисегментной индикаторной панелью на светодиодах, которая воспроизводит хранимую в памяти карты сумму. Другая модель фирмы – CP – по размерам сопоставима с картой (90x61 мм, масса — 31 г), а еще одна (толщиной всего 4 мм) служит футляром для карты устройства считывания. Во второй половине года фирма планировала выпустить прибор типа Value-Cheker Plus, который обеспечит считывание данных разумных карт с помощью ПК. Относительно большие габариты позволяют оснастить его клавиатурой (по типу калькулятора) и соединителем для подключения к компьютеру. Пароль вводится считывающим устройством, что исключает возможность искажения или кражи данных из ПК.

Поскольку банки заинтересованы в проведении различных финансовых операций через Internet, специалисты считают весьма перспективными считывающие устройства, ориентированные на домашние ПК и позволяющие выполнять через Internet операции купли-продажи. Во многом это стало возможным благодаря применению средств кодирования вместо простого пароля, что существенно повысило степень защиты данных.

Чтобы подготовиться к новым требованиям рынка, фирма Fisher International Systems (США) начала поставлять модуль Smarty ("остряк-самоучка"), преобразующий магнитный накопитель ПК на гибких дисках (диаметром 8,9 см) в устройство считывания разумных карт. Подключив модуль, пользователь сможет выполнять на ПК большинство операций, осуществляемых банковским автоматом. Связь модуля с магнитной головкой накопителя обеспечивает преобразователь и несколько интегральных схем. Данные считываются с помощью программных средств ПК, поэтому совместимый с накопителем прибор не нуждается в схемах памяти для хранения программ. По сути, такое считывающее устройство — это трубопровод, соединяющий разумную карту с персональным компьютером.

Появление подобных устройств очень своевременно. Одно из подтверждений тому – намерение корпорации Schlumberger в ближайшем будущем выпустить портфель средств кодирования для электронной торговли через Internet и Intranet. Средства выполнены на основе новой ИС для разумных карт фирмы Motorola, позволяющей кодировать/декодировать данные за доли секунды. Устройство считывания/записи данных отвечает новым требованиям к персональным компьютерам/разумным картам, разработанным при участии фирм Microsoft, Schlumberger, Hewlett-Packard и др.

Предсказываемый сегодня большинством аналитиков стремительный рост рынка разумных карт на самом деле возможен лишь в том случае, если крупные корпорации вложат деньги в разработку и производство считывающих и других устройств, необходимых для пользования картами. По мнению ряда специалистов, стимулировать этот процесс может принятие стандартов, поддерживаемых крупнейшими электронными фирмами. Однако немалое число промышленных обозревателей считает, что единый стандарт на разумные карты не будет выработан никогда: слишком уж разнообразны области применения карт и культурные традиции стран, где они применяются.

Весомый вклад в расширение рынка разумных карт внесла Японская ассоциация по разработке новых сред (NMDA), объявившая о том, что входящие в нее фирмы выбрали стандарт Международной организации по стандартизации и МЭК ISO/IEC 10536 для карт с бесконтактным считыванием. Согласно программе NMDA, поддерживаемой такими гигантами, как Dai Nippon Printing, Hitachi, Mitsubishi и Fuji Research Institute, планируется разработать карту, данные которой могут быть считаны при зазоре в 2 мм. Основные разработчики карты — Hitachi и Dai Nippon Printing. Первая предоставит ИС-ядра, а вторая — катушку приема/передачи и ПЗУ для хранения программы. NMDA уже предлагает участвующим в проекте изготовителям аппаратуры считывания и записи образцы новой карты размером 54x86x0,76 мм. На карте размещен восьмиразрядный микроконтроллер и ЭСРПЗУ емкостью 8 Кбайт, поддерживающее до 100 тыс. операций считывания/записи. Обеспечиваемая схемой скорость передачи данных — 9,6 Кбит/с на частоте 4,9157 МГц. Она работает в стандартах шифрования данных DES с 64-разрядным шифром и RSA с 256-разрядным шифром.

Одновременно совместными усилиями фирм Motorola и Sony разработаны ИС для карт как бесконтактного (на расстоянии до 4 мм), так и контактного считывания. В однокристальной схеме объединены ВЧ-аналоговые устройства фирмы Sony, генерирующие сигнал на частоте 13,56 МГц, и микропроцессорное ядро фирмы Motorola, изготовленное по 0,8-мкм технологии. Схема размещается на кристалле площадью 20—25 мм^2. Первоначально для хранения данных в платах будут использоваться ЭСРПЗУ, ПЗУ и ОЗУ, но в дальнейшем планируется перейти к сегнетоэлектрическим ЗУ и флэш-памяти. Недавно Sony предложила на рассмотрение Международной организации по стандартизации используемую в карте ВЧ-технологию.

Интерес Motorola к созданию совместной системы объясняется тем, что Sony активно выступает на рынке автоматизированных бесконтактных средств сбора платы за проезд. Разработанная ею система используется в подземке и на автобусах Гонконга, куда уже поставлено несколько миллионов карт. Бесконтактные системы считывания с высокой пропускной способностью активно разрабатываются в Барселоне, Мадриде, Лондоне, Париже, Берлине, Токио, Сеуле и Гонконге.

По-видимому, разумные карты на базе новой схемы появятся на рынке весной 1998 года. Цена их составит от 0,5 до 5 долл. в зависимости от числа поддерживаемых приложений.

http://www.aitworld.com/techvalley/smrtfaq.html
http://www.mastercard.com/newways/smartcards.html
Electronic Engineering Times, 1997, N956, N970

Новости

Проигрыватель дисков DVD книжного формата Samsung Electronics

Samsung Electronics сообщила о завершении разработки самого маленького – размером с книгу – проигрывателя цифровых видедисков DVD "P-Theatre". Его толщина – 5,5 см, длина – 20 см, ширина – 16 см и вес – 900 г. Проигрыватель можно подсоединить к обычному или проекционному телевизору с большим экраном, а также к персональному компьютеру в качестве внешнего устройства DVD-ROM. Коммерческая версия "P-Theatre" будет разработана во второй половине 1998 года.

По сообщению фирмы

Тенденции на рынке изделий бытовой электроники

Согласно "Обзору домашней бытовой электронной техники за 1996 год: телекоммуникационные системы дома", подготовленному фирмой International Data Corp. (IDC), более 70% из 2539 опрошенных американских семей знакомы с услугами информационных сетей. Это на 9% больше, чем в предыдущем году. 42% опрошенных считают, что в будущее информационного обслуживания и домашних средств досуга тесно связано с персональными компьютерами. Приблизительно 54% респондентов заинтересованы в приобретении видеотелефона, воспроизводящего полноподвижное изображение абонента на другом конце провода, а 57% семей хотели бы иметь усовершенствованный телефон с видеодисплеем, предоставляющим доступ к средствам информационного обслуживания.

Согласно отчету, 12% опрошенных семей имеют факсимильное устройство (на 3% больше, чем в 1995 году). Видеомагнитофонами пользуются 87% опрошенных, видеокамерами — 28%. Владельцами ПК оказались 37% опрошенных, что на 2% больше, чем в предыдущем году. Более 30% семей имели один или несколько сотовых телефонов, тогда как число владельцев автоответчиков уменьшилось с 69 до 67%. В целом объем услуг, оказанных телефонной сетью/средствами передачи сообщений, в 1996 году увеличился по сравнению с 1995-м с 7 до 11%. 20% респондентов высказали желание приобрести автоответчик, но только 5% из них заинтересованы в передаче речевых сообщений. Около 19% опрошенных семей пользуются двумя и более телефонными каналами (+2% по сравнению с 1995 годом). В числе причин установки дополнительного телефонного номера чаще всего называли необходимость в отдельном телефоне для ведения деловых переговоров (30%) и для детей (23%). Дополнительную телефонную линию для связи с компьютерными системами и передачи данных использовали 15% респондентов против 11% в предыдущем году.

http://www.mwjournal.com/mwj/html/aug97/08m17.htm

Дайджест

Цифровой фотоаппарат-карлик

Японские электронные компании регулярно изобретают самые миниатюрные в мире бытовые приборы. Так, в японскую торговую сеть недавно поступил самый маленький цифровой фотоаппарат, представленный компанией Matsushita. Хотя Coolshot II весит всего 142 г., он вмещает до 90 цифровых снимков.

«Коммерсант daily», 3 декабря 1997 г.

Дайджест

От конфликта сходимости к цифровому ослаблению напряжения

На очередной конференции изготовителей ТВ-аппаратуры и транслирующих компаний (весна 1997 года) группа Digital TV, образованная фирмами Intel, Microsoft и Compaq, предложила принять продвигаемый ею прогрессивный метод развертки, более пригодный для воспроизведения ТВ-изображения на экранах дисплеев ПК. Предложение Digital TV привело участников конференции в ярость, поскольку инфраструктура американской промышленности телевизионного оборудования исторически базируется на методе чересстрочной развертки, хотя никаких ограничений на технику передачи цифрового изображения в США нет.

В конце лета Intel заявила о том, что попытается найти средства, которые позволят ПК принимать сигнал в любом из 18 форматов передачи изображения для цифрового телевидения. Эти средства могут быть какими угодно — от специальной программной продукции до плат тюнеров. Если усилия Intel увенчаются успехом, для поставщиков плат и ИС откроются новые перспективы на рынке. По оценкам фирмы, стоимость программных средств для ПК составит не более 3 долл., а плат тюнеров, способных принимать изображение в различных стандартах, — 200—300 долл. Сейчас на рынке вычислительной техники действуют сотни поставщиков расширительных плат, которые могут выпускать такие тюнеры.

Electronic Business Today, Sept. 1997; http://www.ebtmag.com/issue9709/0997bts.htm

Дайджест