Смарт-карты во встроенных системах

Николай Кольский (Московская обл.)

В статье описываются современные системы безопасности на основе смарт-карт.

Интеграция человека в современные трудовые и общественные отношения является многоплановым процессом, каждая из граней которого строится с учётом существования на этом пути угроз физической и экономической безопасности отдельным личностям, компаниям, общественным институтам и государству в целом.

Сегодняшние системы безопасности не только разграничивают права доступа к информации и на территории, предотвращают кражи в системе торговли, в библиотеках, музеях и на границах государства, но и защищают банковскую и корпоративную информацию. В системах безопасности используются решения, автоматизирующие контрольные процедуры и повышающие степень их надёжности.

Ряд технологий безопасности опирается на процесс аутентификации, включающий предоставление и проверку доказательств того, что человек является именно тем, за кого он себя выдаёт. Аутентификация может проводиться на основе носимых материальных доказательств прав на доступ – «то, что у тебя есть с собой» (something-you-have, как правило, некий пропуск, удостоверение личности и т.п.), на основе знания пароля или кода – «то, что ты знаешь» (something-you-know), на основе биометрии – «то, что ты есть на самом деле» (something-you-are, дактилоскопия, особенности лица, голоса и т.п.).

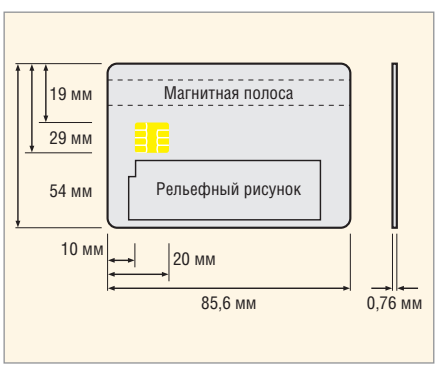


Рис. 1. Габариты смарт-карты, определяемые стандартом ISO/IEC 7816-2

Комбинация этих методов обеспечивает более надёжную аутентификацию. Использование интеллектуальных карт (smart card) является примером трёхфакторной аутентификации: в носимом объекте (something-you-have) хранится ключ или пароль (something-you-know), а также личные биометрические данные (something-you-are). Электронные технологии, встроенные в смарт-карты, и работающее с ними оборудование ускоряют и упрощают процедуры аутентификации и проведение следующих за ними действий (пропуск на территорию, проведение платежа и т.п.), обеспечивая при этом безопасность доступа.

Что такое смарт-карта

Изначально смарт-карта была пластиковым изделием со стандартизованными размерами (см. рис. 1). Современная смарт-карта такого форм-фактора может поддерживать несколько функций (например, быть банковской картой и картой доступа). В неё, как правило, встроен полупроводниковый кристалл (память и/или микропроцессор) и, возможно, антенная система. По возможностям записи данных смарт-карты могут допускать однократную запись или быть перезаписываемыми. Обычный объём памяти составляет 16...32 Кбит, есть устройства с памятью около сотни бит; смарт-карты с оптической памятью могут содержать мегабайты данных.

Микропроцессорные смарт-карты (microprocessor cards) содержат процессорную микросхему, что делает их миниатюрным специализированным компьютером, который имеет встроенную операционную систему (ОС) и способен сохранять и обновлять данные, производить вычисления, осуществлять контрольные функции и взаимодействовать с внешними устройствами. Среди существующих процессорных микросхем для смарт-карт есть 8-, 16- и 32-разрядные приборы, при этом объём памяти микропроцессорных смарт-карт может составлять от 300 байт до сотен килобайт.

Примером 32-разрядного микроконтроллера для смарт-карт является микросхема AE55C1 компании Renesas Technology. Смарт-карты с такой микросхемой могут поддерживать приложения, предъявляющие повышенные требования к информационной безопасности, для чего микроконтроллер сертифицируется на соответствие требованиям Common Criteria level EAL4+. По сравнению с возможностями своих 16-битных предшественников семейства AE-4, новый микроконтроллер имеет в восемь раз большую производительность. Построенный на основе ядра AE-5 с оригинальной 32-битной архитектурой, созданной Renesas Technology, микроконтроллер имеет тактовую частоту 20 МГц. В составе микроконтроллера AE55C1 имеется контроллер прямого доступа к памяти (DMA), а также сопроцессор, поддерживающий технологии шифрования. Следует отметить, что при всех нововведениях обеспечена совместимость с 16-битной архитектурой AE-4, поддерживающаяя плавную миграцию приложений на новый микроконтроллер.

Операционная система процессора смарт-карты должна решать ряд задач, в том числе, осуществлять дефрагментацию памяти, необходимую после многократных операций перезаписи, и сохранять файловую систему в случае сбоя в момент записи. Надёжные ОС для смарт-карт поддерживают «атомарность» изменений данных в памяти, и в случае сбоя данные в памяти сохранятся в том виде, в каком они были до начала процесса записи.

Возможность развития функциональности смарт-карты предоставляют современные операционные системы, которые поддерживает язык программирования Java. Подобные ОС уже зарекомендовали себя в качестве средства поддержки платформы VGP (Visa Global Platform) – отрасле-

вого стандарта для смарт-карт, обслуживающих нужды финансового сектора.

Смарт-карты являются вычислительными устройствами с ограниченными ресурсами. В таких системах используется сокращённый вариант языка Java, в котором оставлены только необходимые возможности: «короткие» типы данных: boolean, byte, short, одномерные массивы и такие объектно-ориентированные свойства Java, как наследование, виртуальные функции, перезагрузка методов, динамическое создание объектов, области «видимости».

В качестве примера современной ОС для смарт-карт можно привести TanGO французской компании ASK. Она предназначена для работы на микросхемах от Atmel и Philips Semiconductors, совместимых со стандартами ISO 7816-4 и 14443 A/B. Такие микросхемы применяются в смарт-картах, обеспечивающих перевозки, банковские операции и системы ограничения доступа. Объём памяти, занимаемый TanGO, составляет 0,5...16 Кб; ОС позволяет создавать новые директории и файлы.

Другой пример – семейство операционных систем под названием WebSphere Everyplace Chip Operating Systems, в которое входят продукты для смарт-карт на базе стандартов Java Card 2.2.1 и Global Platform 2.1.1 (семейство IBM Java Card Open Platform) и решения для многофункциональных карт MultiFunction Card, позволяющие создавать приложения на базе стандарта ISO 7816. Операционные системы WebSphere Everyplace Chip Operating Systems обеспечивают повышенный уровень безопасности за счёт использования алгоритма шифрования Eliptical Curve Cryptography (ECC) и RSA-шифрования с ключом длиной более 2048 бит. Преимуществом алгоритма ECC является то, что он способен обеспечить такой же уровень защиты, как и системы с открытым ключом, однако использует ключи меньшей длины, что повышает скорость вычислений и снижает требования к потребляемой мощности.

Примером микросхем для смарт-карт, использующих возможности операционных систем, является ST19WR66 компании ST Microelectronics. Объём ПЗУ микросхемы ST19WR66 составляет 224 Кб, что обеспечивает хранение в ней операционной системы и программы шифрования, отвечающей требованиям стандарта для смарт-карт ISO 14443B. Микросхема также имеет 66 Кб энергонезависимой памяти для хранения, например, биометрических данных или другой персональной информации. По утверждению специалистов STMicroelectronics, данные могут храниться в памяти микросхемы до 10 лет, что позволяет реализовать на её основе электронный паспорт. Новое изделие обеспечивает считывание данных как при непосредственном контакте со считывающим устройством (ридером), так и по радиоканалу.

Масочное ПЗУ микроконтроллера AE55C1 обеспечивает размещение общеупотребительных операционных систем, нескольких прикладных программ и набора данных. Оно имеет объём 240 Кб и позволяет на 20% повысить плотность хранения кода по сравнению с микросхемами предыдущего поколения компании Renesas Technology, ориентированными на рынок смарт-карт.

Контакт или радиоканал?

По принципу использования смарт-карты подразделяются на контактные, бесконтактные и комбинированные. Для работы контактной карты она должна быть вставлена в ридер, а в бесконтактные карты встроен миниатюрный радиопередатчик, обеспечивающий беспроводную передачу данных в ридер. Как правило, при проходе турникета бесконтактную карту можно не вынимать из сумочки или бумажника.

Смарт-карты комбинированного применения имеют и радиопередатчик, и контактные площадки. Существуют смарт-карты, в которых поддержка «контактного» и «беспроводного» режима обмена данными поддерживается либо одной, либо разными микросхемами.

Обеспечение возможности и контактного, и беспроводного обмена данными необходимо в том случае, когда работа с картой включает ответственные операции, требующие повышенных мер безопасности. Например, запись в проездную карту суммы, лежащей на счету, является более ответственной операцией, чем контроль прохода в зону.

Рынок смарт-карт сегодня регулируется рядом стандартов, число которых превысило десяток. Основополагающими документом являются ISO 7816, который описывает требования к конструкции и технологиям обмена данными для контактных смарт-карт, и документ ISO 14443 (A и B), определяющий требования к бесконтактным смарт-картам. Стандарты Java Card 2.1.1 и 2.2 регламентируют использование технологии Java.

Ридеры, работающие со смарт-картами, являются своеобразными шлюзами для ввода данных в различные информационные системы, поддерживающие систему платежей в розничной торговле или разграничивающие права доступа к корпоративным данным.

Считыватели смарт-карт широко используются в корпоративных информационных системах не только для обеспечения информационной безопасности на основе разграничения прав доступа, но и для поддержки «мобильного» режима работы пользователей. В качестве примера можно привести технологию авторизации пользователей в платформах корпоративных информационных систем на основе «тонких» клиентов Sun Ray компании Sun Microsystems. Все клиентские терминалы оснащены устройством считывания смарт-карт. Наличие такого устройства обеспечивает независимость пользователя от конкретного рабочего места, поскольку он может в любой момент прервать работу на одном терминале и возобновить её, перенеся свою идентификационную смарт-карту на другой.

Для смарт-карт и их аналогов, работающих с компьютерными системами, компания Omnikey, немецкий производитель ридеров, в партнёрстве с компанией Atmel создала семейство микросхем для OEM-производителей высокоскоростных считывателей: серия Smart® включает Smart®Key, предназначенную для клавиатурных USB-ридеров, серия Smart®Link – для автономных ридеров с портом USB, серия Smart®Bus – для ридеров в виде модулей PCMCIA, работающих в ноутбуках и КПК.

Смарт-карты как инструмент трёхфакторной аутентификации

Возможности процессоров для смарт-карт быстро расширяются, в том числе и за счёт расширения объёма встроенной памяти. Компания

Sharp использует в своих микросхемах для смарт-карт технологию флэш-памяти. Это позволяет увеличить объём памяти до 1 Мб, в то время как в традиционных смарт-картах объём памяти обычно составляет 16...32 Кб. Совместные усилия компаний Sharp и IBM позволили интегрировать в подобные процессоры ОС типа JCOP31 – новейшую версию операционной системы IBM для смарт-карт. Эта ОС поддерживает стандарт шифрования AES и метод шифрования ECC, обеспечивающий повышенный уровень защиты при использовании ключа малой длины.

Разработки компаний Sharp и IBM позволят поддерживать одной смарт-картой несколько функций, например, сделать её одновременно кредитной картой, служебной картой сотрудника и членской картой клуба. По мере необходимости в выпущенную карту можно добавлять новые функции. К их числу относится включение в смарт-карты данных биометрии и проведение биометрической идентификации на базе процессорных возможностей самой смарт-карты. Это повышает уровень безопасности, обеспечиваемый смарт-картами в различных приложениях.

Интеграция технологии распознавания человека по биометрическим признакам в смарт-карты включена в рекомендации и стандарты Международной организации гражданской авиации (International Civil Aviation Organization, ICAO), Международного комитета по стандартизации (ISO), в правительственные рекомендации ряда ведущих стран (США, ЕС, Япония). Это стимулирует создание компонентов, облегчающих включение систем распознавания отпечатков пальцев в состав ридеров и устройств, выполняющих функции смарт-карт. Ридеры, а иногда и смарт-карты поддерживают в том или ином объёме функции сравнения полученных дактилоскопических данных с данными, хранящимися в памяти смарт-карты. На этом сегменте рынка сегодня работают не только специализированные компании, но и лидеры рынка, представленные в различных сегментах. Производители широкого спектра продуктов предлагают интегрированные «сборочные» модули, включающие биометрические датчики, процессоры и ПО.

Так, развивая поддержку своего дактилоскопического сенсора FingerChip, компания Atmel предложила биометрический модуль AT77SM0101BCB02VKE на его основе. Сферами применения нового модуля являются системы ограничения доступа, торговые точки, системы учёта работы персонала и т.п. Новый модуль является законченной COTS-подсистемой для биометрии на основе анализа отпечатков пальцев и поставляется с предустановленным ПО для аутентификации (лицензия включена в поставку). Наличие стартового комплекта разработчика, операционная система на базе Linux и высокоуровневые биометрические макросы позволяют быстро создать интерфейс для обеспечения работы модуля в составе законченной системы.

Биометрический модуль AT77SM0101BCB02VKE создан на основе микроконтроллера AT91RM9200 (архитектура ARM9). Наличие у модуля интерфейсов Ethernet, SPI и RS-232 даёт разработчикам свободу манёвра при разработке конечного продукта. Использованный в конструкции модуля сенсор FingerChip имеет небольшие габариты (меньше подушечки пальца, в связи с чем полная дактилограмма реконструируется на основе данных сканирования) и устойчив к ударным нагрузкам, повышенной влажности и загрязнениям.

Гибкую отладочную платформу для разработки систем биометрической идентификации (Fingerprint Authentication Development Tool, или FADT) предлагает корпорация Texas Instruments (TI); FADT поддерживает разработку систем на основе датчиков компаний Atmel, AuthenTec и Fingerprint Cards.

Датчик FingerLoc AFS8600 компании AuthenTec на основе технологии TruePrint имеет активную рабочую область 9,75 × 9,75 мм и разрешение 250 dpi. Ёмкостной сканирующий сенсор FPC1031, производимый фирмой Fingerprint Cards, обладает разрешением 363 dpi при размерах 2,24 × 10,64 мм. Сенсор FingerChip (Atmel) имеет габариты 0,4 × 14 мм и обеспечивает разрешение 500 dpi.

Корпорация TI первой создала технологию поддержки сканирующих датчиков Atmel и Fingerprint Cards с помощью сигнальных процессоров (DSP). Широкий выбор производительных и недорогих DSP с малым энергопотреблением в сочетании с самыми миниатюрными датчиками упомянутых выше компаний расширяет возможности разработчиков биометрических систем в части повышения надёжности, компактности и автономности.

В качестве программной поддержки отладочной платформы FADT предлагаются программные пакеты фирмы Bioscrypt (верификация дактилоскопических шаблонов) и Fingerprints Cards (для формирования рисунка папиллярных линий). В недавно проведённых сравнительных испытаниях (2004 Third International Fingerprint Verification Competition) программное обеспечение Bioscrypt заняло первое место в категории открытых продуктов: потребовалось около 0,08 с для включения дактилоскопического шаблона в реестр и 1,48 с для сравнения по четырём базам данных. Кроме того, ПО Bioscrypt позволяет повысить точность распознавания за счёт расширенных возможностей работы с изображением папиллярного рисунка.

Продукция компаний Atmel и TI позволяет расширить спектр данных, хранимых в памяти смарт-карты, повышая уровень надёжности аутентификации её владельца. По оценкам Международной биометрической организации (International Biometric Group/IBG), объём рынка малых и средних систем биометрии составит в 2008 г. до 1,5 млрд. долл. США.

Будущее технологий на основе смарт-карт

В ближайшем будущем технологии смарт-карт могут быть внедрены в «электронные» паспорта (e-passports). Претендентами на использование в электронных паспортах США были электронные метки компаний Electronic Data Systems, Oberthur Card Systems, On Track Innovations и ASK. Во время испытаний, проведённых по заказу австралийского Министерства иностранных дел и торговли, были исследованы возможности 11 ридеров от 11 разных производителей, а в качестве меток – 25 изделий от шести поставщиков. К введению электронных паспортов готовятся в России.

Встраивание микросхем в документы может производиться двумя способами. Микросхема с антенной может изготавливаться в виде вставки (inlay), «вклеиваемой» в напечатан-

ный документ. Другой вариант предусматривает «печать» микросхемы с антенной на бумаге, вставляемой в конечный документ (в т.ч. паспорт). Так, французская компания ASK создала «бумажные» транспондеры Smart Paper ID для использования в паспортах, визах, водительских правах и других национальных документах автоматической идентификации. Новые транспондеры состоят из микросхемы на бумажной подложке с впечатанной серебряной антенной. Они созданы на основе стандарта ISO 14443A/B и работают на нелицензируемой частоте 13,56 МГц. Добавленные на бумажную основу электронные компоненты практически не увеличивают толщину подложки и неразличимы на ощупь.

Компания ASK уже использует транспондеры Smart Paper ID для производства проездных билетов, используемых на территории Европы. При этом Нидерланды стали первой в мире страной, чья система оплаты проезда в общественном транспорте будет полностью построена на подобных технологиях. Голландский проект построения электронных транспортных платежей (e-ticketing) реализует консорциум, образованный пятью крупнейшими операторами транспортных услуг, и охватывает железные дороги, метрополитен, автобусное и трамвайное сообщение, водный транспорт.

Наряду с внедрением в паспорта и проездные документы, технологии смарт-карт могут полностью захватить рынок поддержки платежей, проводимых не только владельцами «платиновых» и «золотых» документов, но и мелкими плательщиками.

Компания Atmel и израильская компания On Track Innovations, производящая смарт-карты, выполнили крупный заказ на микропроцессоры, разработанные для программы бесконтактных платежей MasterCard PayPass. Эта программа призвана заменить мелкие наличные расчеты безналичными. Поставленные в рамках заказа микросхемы поддерживают стандарты ISO 14443B и 7816. Помимо микроконтроллеров для поддержки защищённых платежей, компании поставили и другие компоненты, включающие операционную систему и программные приложения.

Более миллиона пластиковых идентификационных карточек поставила компания X-ident Technology горнолыжным курортам Франции. Эти карточки используются лыжниками и сноубордистами для доступа к подъёмникам. В конструкции карт применены микросхемы французской компании Inside Contactless, работающие в частотном диапазоне 13,56 МГц. Эти микросхемы снабжаются антеннами немецкой компании KSW-Microtec и превращаются в полуфабрикат RFID-системы, соответствующей требованиям стандарта ISO 15693-2.

Массовый характер применения идентификационных смарт-карт и стремление к максимальному их удешевлению трансформировали внешний вид смарт-карт. Сегодня они могут выглядеть как брелоки или браслеты или встраиваться в мобильные телефоны.

Так, Bank of America проводит испытания брелоков в качестве средства проведения бытовых платежей, в дополнение к кредитным и дебетовым картам банка. Тестируемые устройства, работающие на принципах технологии RFID, созданы компанией Oberthur Card Systems на основе пассивных высокочастотных микросборок, удовлетворяющих стандарту ISO 14443. Микросборки выпускаются корпорацией TI и сертифицированы компанией MasterCard на соответствие требованиям спецификации для карточек MasterCard PayPass на основе технологии RFID.

Одна из систем, предназначенных для предотвращения похищений или подмены младенцев в детской больнице, использует беспроводные электронные наручные и ножные идентификационные браслеты (см. рис. 2), а также считывающие устройства, контроллеры и ПО, автоматически закрывающее двери и подающее сигнал тревоги в случае несанкционированного местонахождения младенца. Система защищена от повреждений и даёт сигнал тревоги при попытке снятия электронного браслета с ребёнка.

Обслуживающий медперсонал, акушерки, матери и младенцы носят специальный электронный наручный или ножной браслет, хранящий индивидуальные данные их носителя и выступающий в роли своеобразного удостоверения личности. Данное устройство регулярно посылает сигналы, принимаемые считывателями в потолке отделения для грудных детей, приборами сигнализации на входах и выходах, а также контроллерами. Электронные идентификационные браслеты сообщают статус их носителя, его местонахождение, а также состояние батарей на считывателях. Программное обеспечение компании CIAC позволяет в режиме реального времени установить, где в данный момент находится носитель идентификационного браслета.

Рис. 2. Система, предназначенная для предотвращения похищений или подмены младенцев в детской больнице

Модули ввода/вывода контролируют установки видеонаблюдения, точки доступа и системы аварийного освещения. В случае возникновения угрозы похищения они включают сигнализацию и автоматически закрывают двери.

Расширение использования радиоканала для работы со смарт-картами стимулирует работы в области информационной безопасности при передаче данных. Наряду с использованием традиционных технологий шифрования данных, включая Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA) и стандарты США Federal Information Processing Standards (FIPS) для формирования уникального числа, которое можно использовать для целей аутентификации, ещё одним способом обеспечения информационной безопасности при беспроводном обмене идентификационными данными является использование технологии NFC (Near Field Communication, связь в ближнем поле).

Технология NFC обеспечивает быструю, удобную и защищённую передачу данных между устройствами на расстояниях до 10 см, т.е. на физическом уровне гарантируется невозможность установления незапланированного сеанса связи. Защита от несанкционированного доступа к данным может обеспечиваться и

на уровне сетевого протокола, и на более высоком уровне. Важной особенностью протокола NFC является поддержание режима пассивного соединения (passive mode of communication), который позволяет обеспечивать сеанс связи энергией, используя ресурсы лишь одного из устройств. Технология NFC может быть использована для передачи небольших объёмов данных, проведения платежей и конфигурирования доступа к беспроводным сетям Wi-Fi или Bluetooth.

Опеку над стандартами в области технологии NFC осуществляет организация NFC Forum (Ассоциация разработчиков и пользователей коммуникационных систем на основе технологий ближнего поля), основателями которой являются компании Nokia, Royal Philips Electronics и Sony. Требования к технологии NFC уже описаны в спецификациях ISO 18902, ECMA 340 и ETSI TS 102190. Принятые стандарты описывают процедуры считывания и записи данных в метку, организацию связи класса peer-to-peer, эмуляцию метки. Проведённые работы позволяют интегрировать NFC в системы на основе протоколов Philips MIFARE (ISO 14443-A) и Sony FeliCa. Это означает, что смарт-карты способны «видеть» NFC-устройства, а ридеры – работать с оборудованием, использующим технологию NFC.

Чтобы передать данные между NFC-устройствами, их надо сблизить на предельно короткое расстояние или привести в соприкосновение. Это инициирует работу беспроводного интерфейса и конфигурирование сети равноправных узлов (peer-to-peer network). Соединение устанавливается на частоте 13,56 МГц.

Корпорация Nokia продемонстрировала первый сотовый телефон с интерфейсом NFC на конференции Cartes & IT Security, прошедшей в конце 2004 г. в Париже. Конструкция подсистемы, реализующей возможности технологии NFC, включала NFC-микросхему от Philips Semiconductors и контроллер смарт-карты Philips SmartMX, соединённые интерфейсом Philips S2C.

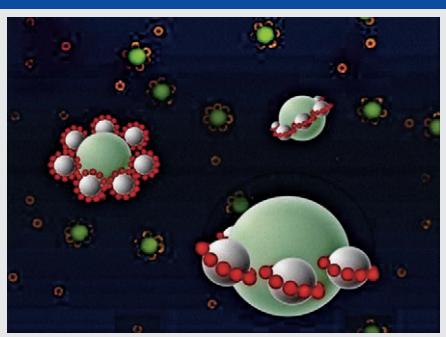
Лидеры рынка мобильных телефонов также готовы начать производство или выпустить прототипы сотовых телефонов с беспроводным интерфейсом на основе технологии NFC. При этом новый интерфейс предполагается использовать либо для обеспечения возможностей оплаты проезда, либо для совершения небольших платежей в розничной торговле или сфере услуг.

Новости мира News of the World Новости мира

Тончайшие плёнки – очередной апгрейд современной электроники

Несмотря на постоянную миниатюризацию современных интегральных микросхем – компания Intel рассказала о своих грядущих 32-нм продуктах, – бесконечно процесс уменьшения размеров элементов, особенно в случае кремниевой электроники, длиться не может. Это заставляет исследователей искать пути для уменьшения размеров транзисторов за счёт новых материалов, и очередных успехов в этой области добились сотрудники Массачусетсткого Университета (University of Massachusetts Amherst). Помимо миниатюризации интегральных микросхем – размеры транзисторов могут быть снижены в несколько раз по сравнению с кремниевыми, – их исследование позволяет увеличить и скоростные показатели ИС.

Команда учёных под руководством Джереми Леви изготовила «нанотранзистор» на основе двух керамических материалов: алюмината тантала и титаната стронция. Изначально оба этих соединения являются изоляторами, однако при соединении их друг с другом они становятся проводниками – положительные носители заряда способны протекать через подобную структуру. Впрочем, это ещё не всё – посредством атомно-силовой микроскопии, приложением напряжения, исследователи добивались формирования крошечного проводящего мостика между



двумя материалами, который впоследствии легко разрушался при протекании заряда противоположного знака.

Точно такие же материалы могут использоваться для создания транзисторов размером с отдельные атомы, а на их основе можно формировать интегральные микросхемы для вычислительных систем, устройств хранения информации и сенсоров самого различного назначения, в том числе и высокоточных детекторов.

Практически одновременно с сообщением о разработке новейших транзисторов сотрудниками University of Massachusetts Amherst поступила информация, что команде учёных из того же заведения вместе с сотрудниками Калифорнийского университета Беркли (University of California Berkeley) удалось разработать способ изготовления тончайших полупроводниковых плёнок, позволяющих резко повысить ёмкость современных устройств хранения информации.

Многие годы попыток создания подобных конструкций на основе полимеров не приводили к нужным результатам «благодаря» потере материалом своей структуры при растяжении на значительную площадь. Чтобы преодолеть эту трудность, исследователи использовали специальные гребенчатые материалы, работающие как направляющие для полупроводниковых плёнок. В этом случае уже вполне возможно получать структуру с необходимыми для исследователей свойствами, а главное, процесс их формирования весьма прост. На полупроводниковых плёнках учёные надеются создавать уникальные по своим характеристиками устройства хранения информации, в сотни раз более ёмкие, нежели популярные сегодня оптические DVD-носители.

wired.com

LG заявила о начале выпуска 15" OLED-панелей

Компания LG Display практически готова к запуску серийного изготовления 15-дюймовых OLED-панелей, – согласно официальному заявлению, старт намечен на июнь 2009 г. Среди технических характеристик отметим разрешение 1366 × 768 пикселов и ресурс работы панелей в 30 тыс. ч. Впрочем, главным вопросом остаётся стоимость дисплеев, и именно эта информация пока для широкой публики оказывается недоступной.

Networkworld