

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ СОВРЕМЕННОГО ОБЩЕСТВА

КОРДОНЬЕ В., НЕМЧЕНКО В. П.,
КРИВУЛЯ Г. Ф., НЕМЧЕНКО С. В.

Сделан обзор и классификация существующих типов карт, показано место карт в информационных системах, приведена структура микропроцессорной карты типа переносное досье. Показана необходимость совершенствования применяемой элементной базы — микропроцессоров и других электронных устройств, оптимизации их структуры и создания специального программного обеспечения на базе языка Java.

Несколько слов о терминологии. В настоящее время в отечественной, так же как и в русской научной литературе, понятие Smart Card (в переводе с английского — “умная, интеллектуальная карта”) четко не определено и не имеет русского или украинского аналога. Термин “Кредитная карточка” в связи с его узостью не может претендовать на эту роль. Наиболее близким к английскому оригиналу, с нашей точки зрения, можно считать термин “Интеллектуальная карта” (ИК), который мы и будем здесь использовать наряду с английским термином Smart Card.

1. Классификация ИК по типу использования

Если взглянуть на историю создания и развития ИК, можно увидеть, что первоначально речь шла лишь о создании карточки для безналичных расчетов. И только в последнее время интеллектуальные карты освоили целый ряд новых для себя “професий”. Дадим краткую характеристику интеллектуальным картам с точки зрения области их применения [1].

ИК для кредитно-финансовых операций. При помощи этих карт осуществляется оплата в том или ином виде. Различают два класса карт:

1. *Карты предоплаты*, на которых находятся условные единицы, соответствующие некоторой реальной величине в зависимости от функции карты. Информация на карте может обновляться.

2. *Карты оплаты* на сегодняшний день представляют собой преимущественно карты с микропроцессором (банковские карты). В этом классе есть два типа — кредитные и дебитные карты. Кредитные карты позволяют осуществить покупку, которая является дебетом на счете, соответствующем карте с процентом, зафиксированным в кредитующей организации. Дебитная карта также осуществляет покупку, но изменение будет записано в дебет счета карты только через несколько дней, без дополнительных процентов.

ИК доступа. Такого класса карты имеют три категории доступа:

1. *Идентификация.* Карты используются для идентификации человека на предприятии (информация

отдела кадров предприятия), в телефонной сети (позволяют производить переадресацию оплаты за телефонные услуги) или в обществе (удостоверение личности). Этот тип карт часто комбинируется с другими типами.

2. *Информационная безопасность.* Карта используется для получения доступа к серверу, базе данных в сети.

3. *Физическая безопасность.* Карта используется в качестве пропуска на предприятиях.

Переносные досье. Карта содержит совокупность определенной информации о физическом состоянии и возможностях субъекта. Например, медицинская, студенческая, транспортная карты.

Остановимся подробнее на ИК, относящихся к типу переносного досье, которые в последнее время находят все более широкое применение. Карты такого типа называют еще микропроцессорными, поскольку основным логическим блоком в них является микропроцессор.

1. *Студенческая карта.* Рассмотрим конкретный пример — лицей Charle de Gaulle de Muret во Франции. Он открылся в 1989г., в его стенах учится 900 учеников. Это первый лицей Франции, который начал использовать многосервисные электронные карты. Эта карта поддерживает такие функции как предоставление специальных скидок в студенческих столовых, в кафетерии; предоставление услуг в спортивных залах и т.п. Кроме того, она позволяет вести централизованный учет оценок и посещения занятий, оказание услуг ксерокопирования, является читательским билетом в библиотеках и пропуском в общежитие, позволяет учащимся иметь доступ ко всем информационным ресурсам лицея.

2. *Медицинская карта.* Одним из ее видов является страховая карта. Она заменяет формуляры, уменьшая тем самым возможность возникновения ошибок при заполнении, а также позволяет значительно ускорить оплату страховки и возмещение ущерба. Другим видом медицинской карты является *переносное досье*. Оно содержит медицинское досье пациента, рецепты для аптек, результаты последней консультации у врача, особенности пациента (противопоказания, аллергии и т.п.) и результаты обследований.

Еще одним видом такой карты является *амбулаторная карта*. Она хранит предписания врача на проведение амбулаторного лечения, помогает переносить информацию между отдельными электронными медицинскими установками дома у пациента, в его поликлинике, а также между отдельными поликлиниками и другими медицинскими центрами. Использование таких карточек вызывает необходимость унификации различного медицинского электронного оборудования.

2. Информационные системы на основе Smart Cards

В настоящее время наиболее глобальной и известной является медицинская информационная система Франции, работающая на основе smart cards. В этой системе врач (или другое заинтересованное лицо) имеет свою карту, которая ему позволяет считывать данные, находящиеся на карте пациента, и записывать туда новую автоматически “подписанную” информацию [2].

Чтобы прочитать (записать) информацию с карты пациента, врач вставляет свою карту в считыватель

и вводит свой личный пароль, при этом карта пациента также должна находиться в считывателе. Считыватели должны быть подключены к информационной сети MINITEL (французская национальная информационная сеть – упрощенный аналог Internet), Internet или к компьютеру. После этого врач имеет доступ к данным, соответствующим его уровню доступа. Схематично функционирование такой системы представлено на рис. 1.

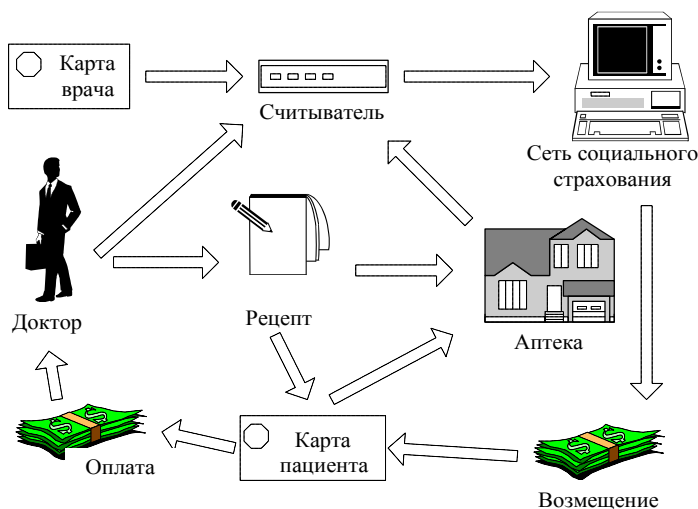


Рис. 1. Принцип функционирования медицинской информационной системы

Используемая в рассматриваемой системе микропроцессорная карта представляет собой пластиковый прямоугольник размера кредитной карточки (стандарт ISO 7816/1: 86x54x0,8 мм), в которую встроен микропроцессор, прикрытый металлическими контактами (стандарт ISO 7816/2), используемыми для ввода / вывода информации и электрического питания карты, а также ряд вспомогательных блоков и устройств, использование которых значительно повышает надежность и функциональную гибкость карты.

На рис. 2 показана структура высоконадежной микропроцессорной карты типа “переносное дощечное”, реализованной на базе микропроцессора ST6XYZ фирмы SGS-Thomson Microelectronics [3].

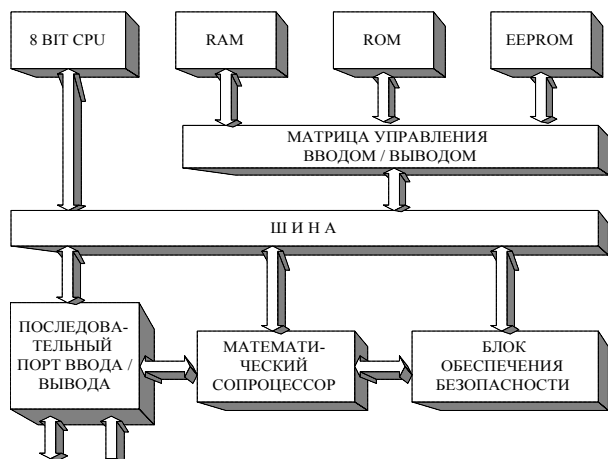


Рис. 2. Структура микропроцессорной карты

Кроме 8-разрядного микропроцессора, в карте используются следующие устройства:

- оперативная память RAM, которая служит рабочей памятью для процессора;
- постоянная память, состоящая из ROM или PROM, которая позволяет хранить операционную систему карты и постоянную информацию идентификации и безопасности;
- постоянная память типа EEPROM, которая позволяет однократно записывать данные;
- блок обеспечения безопасности, который обеспечивает конфиденциальность информации логическими методами;
- последовательный порт ввода / вывода, обеспечивающий обмен информацией с внешней средой;
- матрица управления доступом к памяти различного типа;
- шина, посредством которой происходит обмен информацией между всеми блоками карты.

При необходимости в карту встраивается математический сопроцессор, значительно повышающий быстродействие и гибкость системы.

3. Функциональная структура ИК и считывателя информации

Рассмотрим функциональную модель подсистемы “ИК – считыватель – пользователь”, которая входит в медицинскую информационную систему.

С точки зрения выполняемых функций в основе карты лежат собственно данные (например, в банковской карте – количество денег на счету).

Непосредственный доступ к этой информации имеют только функции работы с данными, которые физически также находятся на карте.

Они в свою очередь состоят из функций доступа к данным (считать, записать) и функций обработки данных. На “выходе” из карты находится ее интерфейс – именно с этим набором команд и имеет дело считыватель.

Обмен информацией между считывателем и картой осуществляется при помощи пользовательского интерфейса считывателя и интерфейса карты (стандарт ISO 7816/3).

Далее информация обрабатывается с помощью функции обработки информации считывателя и затем уже в окончательно преобразованном виде попадает в интерфейс пользователя (например, терминал специализированной машины).

Информация от пользователя на карту попадает, пройдя путь, аналогичный рассмотренному, но в обратном порядке.

На рис. 3 приведена показывающая взаимодействие структура ИК со считывателем информации. Такая структура характерна лишь для обычных ИК.

Для многофункциональных же карт между функциями доступа к данным и функциями обработки необходимо добавить распределитель потоков данных, своего рода интеллектуальный коммутатор.

В завершение приведем мнение авторов статьи [4] по вопросу перспектив развития и внедрения ИК в жизнь современного общества.

Представьте себе картину, пишут они, что вы в супермаркете расплачиваетесь за покупки деньгами, которые хранятся у вас на маленькой электронной карте. Чтобы пополнить запас денег, вы вставляете

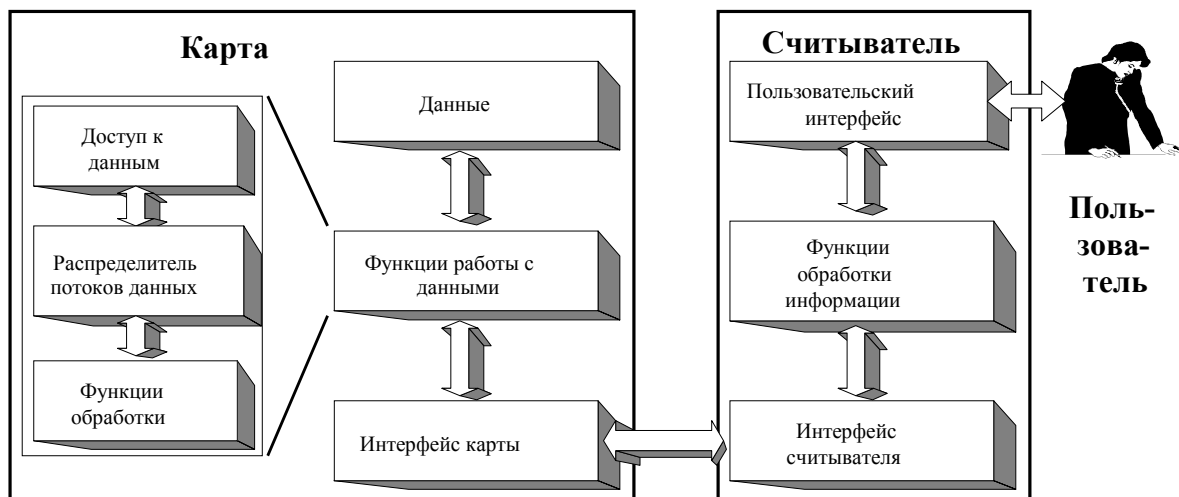


Рис. 3. Функциональная структура ИК и считывателя информации

вашу карту в Глобальную систему для мобильной связи (GSM), звоните и набираете номер вашего банковского счета. Затем в метро вы используете ту же карту, чтобы добраться домой, поскольку в ней содержится приобретенный вами месячный проездной билет.

Прибыв домой, вы включаете телевизор и ваша карта позволяет идентифицировать вас как подписчика на ваш любимый канал, когда вы вставляете ее в специальный считыватель.

Как видим, в ближайшей перспективе планируется создание универсальной многофункциональной интеллектуальной карты.

Литература: 1. *Cordonnier V.* The Future of Smart Cards Technology and Applications. IFIP 96 World conference On mobile communication. Canberra. September 1996. 21 p. 2. *Marie-Theruse Chapalain.* La carte a memoire sante. Gestions Hospitalieres, № 258, septembre, 1986, p. 478-480. 3. *Robyn A. Lindley.* Smart Card Innovation. Saim Pty Ltd, Australia, 1997. 4. *Peter Hofland, Lana Janowski.* Smarter Smartcards. BYTE. February, 1998, p. 7-10.

Поступила в редколлегию 28.04.98

Рецензент: д-р техн. наук, проф. Загарий Г.И.

Венсан Кордонье (Vincent Cordonnier), д-р наук, профессор, руководитель исследовательской группы Лилльского университета наук и технологий, Франция. Научные интересы: интеллектуальные карты (Smart Cards). Увлечение: путешествия. Адрес: 59655, Villeneuve d'Ascq Cedex. Тел. +33 3.20446046.

Немченко Владимир Петрович, канд. техн. наук, профессор, начальник отдела международного сотрудничества ХТУРЭ. Научные интересы: проектирование специализированных цифровых устройств, техническая диагностика. Увлечения и хобби: автомобилизм, рыбная ловля, иностранные языки. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. (0572) 40-91-07.

Кривуля Геннадий Федорович, д-р техн. наук, профессор, заведующий кафедрой АПВТ ХТУРЭ. Научные интересы: техническая диагностика, системы автоматизированного проектирования цифровых устройств. Увлечения и хобби: автомобилизм, туризм, рыбная ловля. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. (0572) 40-93-26.

Немченко Сергей Владимирович, магистр технических наук, инженер-исследователь кафедры АПВТ ХТУРЭ. Научные интересы: интеллектуальные карты (Smart Cards), техническая диагностика. Увлечения и хобби: автомобилизм, спорт, музыка, путешествия. Адрес: 310726, Украина, Харьков, пр. Ленина, 14, тел. (0572) 40-99-11.

УДК 681.325

АЛГОРИТМ ДИАГНОСТИРОВАНИЯ ТЕСТОПРИГОДНЫХ ЦИФРОВЫХ СТРУКТУР

ХАХАНОВ В.И., СКВОРЦОВА О.Б., МОНЖАРЕНКО И.В.

Предложен безусловный алгоритм диагностирования цифровых устройств, использующий заложенную на стадии проектирования тестопригодность, заключающуюся во внесении избыточности, которая позволяет сканировать существенные линии, служащие в качестве точек контроля.

Согласно [1] тестопригодность достигается путем применения методов проектирования цифровых объектов, которые позволяют уменьшить временные и материальные затраты на организацию и

проведение диагностического эксперимента. Цифровой объект является тестопригодным, если процедуры генерации тестов, оценки их качества и реализации тестового диагностирования могут быть выполнены при условии соблюдения в установленных пределах финансовых и временных затрат, а также значений показателей, характеризующих приспособленность схемы к контролю и поиску дефектов, реализации тестового диагностирования.

Методы проектирования тестопригодных схем можно дифференцировать на:

- 1) анализ структурно-функционального исполнения объекта, численная оценка управляемости и наблюдаемости как меры тестопригодности схемы, которая может использоваться на этапе проектирования;
- 2) способы структурного проектирования тестопригодных схем, в пределах самотестируемых, основанных на использовании свойств сканируемого пути, обеспечивающего доступ к внутренним точкам схемы, а также эффективные методы генерации тестов;