ПРОГРАММНО-АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПЕРСОНАЛЬНОГО МЕДИЦИНСКОГО ЭЛЕКТРОННОГО ПАСПОРТА

В. В. Петров, А. А. Крючин, И. В. Горбов

Институт проблем регистрации информации НАН Украины

A portable carrier based on the flash-media is proposed for personal medical information storage. The personal medical data carrier with USB-interface is developed and created. There is developed the carrier firmware that allows write the medical data and prevents its changes or deletion. The proposed carrier supports multilevel data access in concordance with status of user (doctors with various specialty or patient).

Информатизация медицинской отрасли на сегодняшний день является одной из приоритетных задач современной Украины. Медицинские организации многих стран уже используют медицинские информационные системы (МИС) для автоматизации процессов документооборота. Принципы построения таких МИС не отличаются от построения большинства баз данных, где медицинская информация пациента представляет собой файл (или его часть), хранящийся на главном сервере системы. Таким образом, данные всех пациентов хранятся в одном месте, а их защита реализована только на программном уровне, т.е. на физическом уровне носителя остается возможность эти данные изменить или удалить.

Медицинский электронный паспорт (МЭП) гражданина Украины – это программно-аппаратный комплекс, обеспечивающий сохранение и обработку персональной медицинской информации каждого пациента. Особенностью такой системы является то, что данные должны быть максимально защищены не только от несанкционированного доступа, но и от редактирования и удаления. При этом доступ должен ограничиваться правами и предоставляться определенному кругу специалистов и самому владельцу паспорта.

Основной составляющей такого комплекса может быть персональный носитель, удовлетворяющий следующим основным требованиям: запись информации осуществляется без возможности ее исправления или удаления, доступ к данным имеет несколько уровней и зависит от того, кто пользуется носителем (пациент, врач или другие лица). При этом персональный носитель МЭП должен быть небольшим (удобным для постоянного ношения), устойчивым к воздействию температуры и внешних электромагнитных полей, герметичным и механически прочным. Он должен гарантировать длительный срок хранения данных, быть достаточно универсальным и позволять работать с различными типами аппаратного и программного обеспечения.

До недавнего времени в свободном доступе не было носителей информации, которые могли бы использоваться в качестве базового устройства персонального МЕП. Поэтому концепции современных МИС исключительно на сетевых технологиях хранения персональных данных. Возможность создания МЕП появилась после широкого распространения носителей на основе флэш-памяти, существенного улучшения их характеристик и уменьшения стоимости.

Основными аппаратными элементами стандартного USB-носителя являются микросхема флэш-памяти и микроконтроллер, обеспечивающий взаимодействие управляющего устройства (ПК, планшета, проигрывателя и т.д.) с самой микросхемой памяти и определяет разрешенные режимы работы (запись, воспроизведение, удаление). В большинстве USB-носителей все операции являются разрешенными, некоторые производители предлагают пользователям носители с закрытой областью, доступ к которой предоставляется с помощью пароля или отпечатка пальца. Такое «незначительное» усовершенствование приводит к необходимости использовать более производительный микроконтроллер.

В результате роботы был специальный USB-носитель, в котором на аппаратном уровне реализовано: информация записывается без возможности ее изменения или удаления, что также существенно повышает срок хранения данных; многоуровневый доступ к отдельным областям памяти носителя.

Для реализации описанных функций был использован специальный микроконтроллер с оригинальной прошивкой. На базе выбранного микроконтроллера и микросхемы флэш-памяти на 4 ГБ был построен персональный МЭП (рис. 1).

Как и для накопителей на магнитных дисках, в твердотельных носителях используются стандартные файловые системы (FAT16, FAT32, NTFS). В случае хранения файлов с медицинскими записями, размеры которых не превышают 1 КБ, данные системы являются неэффективными из фиксированного раз-

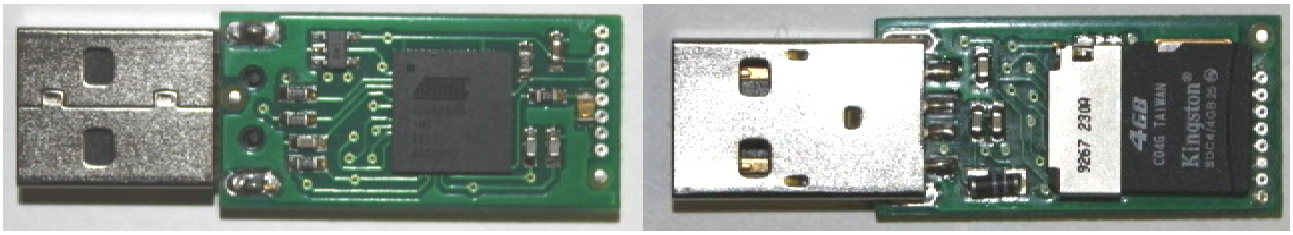

Рис. 1. Персональный носитель медицинской информации.

мера кластера. Например, размер кластера файловой системы FAT для носителя емкостью 4 ГБ составляет 32 КБ, т.е. при размере файла 1 КБ будет потеряно 31 КБ дискового пространства. Чтобы этого избежать была разработана специальная файловая система, которая эффективно использовала дисковое пространство при сохранении небольших файлов.

Вопрос о недопустимости изменения записанных данных является принципиальным для медицинской информации. В большинстве МИС защита информации реализуется программно на уровне системы управления базой данных, т.е. на физическом уровне остается возможность их изменения или удаления. Поэтому защита от этих действий была реализована на уровне контроллера. Для обеспечения необходимой механической защиты носитель МЭП был помещен в металлический корпус и герметизирован.

Необходимо отметить, что на МЭП должна храниться вся информация о пациенте, в том числе и данные с ограниченным доступом. Т.е. сам пациент должен иметь полный доступ к своим данным, а другим пользователям должен предоставляться доступ в соответствии с их правами. Для реализации многоуровневого доступа память персонального носителя медицинской информации была разбита на две области: открытую (Раздел 0) и закрытую, которая также разбита на 4 раздела (рис. 2). Раздел 0 предоставляет свободный доступ на чтение данных и ограничение на запись. Этот раздел может использоваться для идентификации пациента и предоставления о нем основной информации (группа крови, аллергические реакции, восприимчивость для препаратов и др.). Также на открытой области может находиться программное обеспечение, с помощью которого будет обеспечиваться доступ к закрытой области.

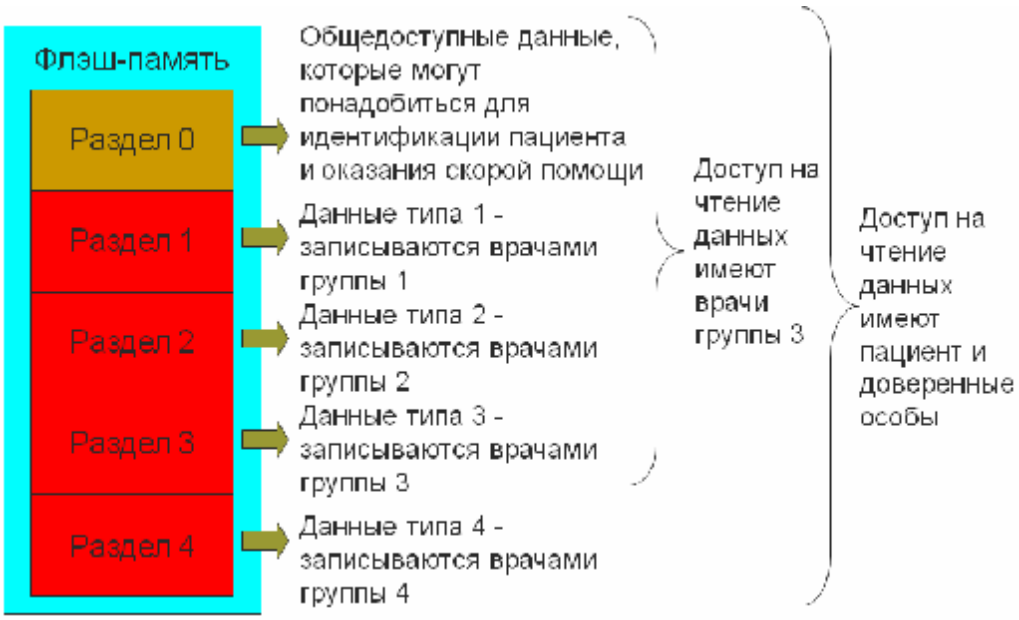

Рис. 2. Многоуровневый доступ к данным МЭП.

На данном этапе исследований закрытая область была разбита на 4 раздела, доступ к которым предоставляется в соответствии с правами пользователя. Пользователи 1-го уровня могут записывать и читать данные только раздела 1. Этот раздел может использоваться врачами группы 1 для сохранения медицинских данных определенной узкой специальности. Пользователи 2-го уровня могут записы-

вать и читать данные только раздела 2, который аналогично может использоваться врачами группы 2. Пользователи третьего уровня имеют больше прав, они могут записывать данные в раздел 3 и считывать данные с 1-го, 2-го и 3-го разделов. Такие права могут быть предоставлены врачам группы 3, например, главврач или лечащий врач. Права пользователей 4-го уровня схожи с правами 1-го, однако данные с этого раздела не могут быть прочитанными пользователем 3-го уровня, т.е. врачам других групп доступ к этим данным предоставляться не будет. Пятый уровень пользователя был введен специально для пациента или его доверенных лиц. Этот уровень позволяет пользователю воспроизводить данные со всех разделов, но не позволяет ничего записывать.

Для реализации доступа к закрытой области была разработана специальная библиотека DLL, которая позволяет интегрировать МЭП в уже существующие МИС. Также на базе этой библиотеки была разработана программа, которая идентифицировала пользователя по паролю и предоставляла доступ к соответствующим разделам. Уровень пользователя для врача может определяться электронным ключом, который также будет генерировать цифровую подпись для всех записей. Такой подход позволит гарантировать целостность данных и повысит личную ответственность врачей за поставленный диагноз. Кроме того, МЭП может использоваться для контролируемого распространения лекарственных средств.

Выводы. Разработаны и изготовлены экспериментальные образцы персонального МЭП. Создано внутреннее программное обеспечение микроконтроллера, обеспечивающее многоуровневый доступ к данным и предотвращающее их изменение или удаление, а также обеспечивающее эффективное использование памяти носителя. Разработана динамическая библиотека DLL, позволяющая использовать такие носители в рамках уже созданных МИС. Разработано программное обеспечение, распределяющее права доступа в соответствии со специализацией врача, выполняющее запись данных во время приема пациента и позволяющее пациенту просматривать свои медицинские данные без возможности их редактирования или удаления.