УСТРОЙСТВО ИДЕНТИФИКАЦИИ ОТПЕЧАТКА ПАЛЬЦА ВЛАДЕЛЬЦА ДЛЯ СМАРТ-КАРТ ДИСТАНЦИОННОГО СЧИТЫВАНИЯ

Мытник И.С.

Мытник Иван Сергеевич – магистр техники и технологии,
кафедра инфокоммуникационных технологий и систем связи, физико-технический факультет,
Балтийский федеральный университет им. Канта,
инженер–оператор станков с числовым программным управлением,
Технопарк «Кванториум», г. Калининград

Аннотация: *в ходе статьи проанализированы виды мошенничества, представляющие потенциальную опасность для пользователей смарт-карт, в частности для денежных средств, хранящихся на картах, и проиллюстрировано техническое решение проблемы в виде сборки смарт-карты из электронных компонентов на отладочных приборах.*

Ключевые слова: *смарт-карта, дистанционное считывание, биометрические технологии, система защиты, несанкционированный доступ.*

Основные определения.

Смарт-карта — пластиковая карта со встроенной микросхемой, в большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти [1].

Биометрические технологии – технологии, основанные на измерении уникальных биологических и поведенческих характеристиках отдельно взятого человека [2].

Near field communication NFC — технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров [3].

Существенную роль в функционировании банковской отрасли любой страны играют банковские денежные карты.

Известно множество случаев мошенничества и краж денег у владельцев смарт-карт, которые причиняют значительный материальный ущерб потребителям банковских услуг. Обеспечение безопасности проведения платежных и иных операций со смарт-картами дистанционного считывания является важнейшей задачей

В целях обеспечения безопасности проведения платежей, ношения и хранения денежных карт осуществляются развернутые технические и организационные меры, основными решениями которых являются:

– защитное шифрование данных на картах;
– подтверждение операций с банком непосредственно во время совершения операции;
– автоматические оповещения владельцев карт при совершении каких-либо операций;
– введение кода карты перед совершением платежа или иной операции [1].

Виды мошенничеств со смарт-картами.

В настоящее время в основной группе риска контактные карты, но, в случае если терминал не оснащен NFC-системой, под угрозой оказываются и бесконтактные карты, ведь пользователь будет вынужден вставить карту в терминал. В таком случае у мошенников намного больше путей незаконного изъятия денежных средств. Устройства – скиммеры [4], считывающие данные с пластиковых карт для их подделки и дальнейшего использования. Скиммеры выглядят, как терминал, или могут быть в него встроены, так же крепятся к корпусу банкоматов, и, будучи внешне трудноотличимы от настоящих картоприемников, несут большую угрозу владельцам карт.

Намного более опасным видом мошенничества является кража данных с помощью устройств – шиммеров [5], которые в отличие от наружной скимминговой накладки вводят в банкомат, где он приклеивается к внутренней части картоприемника, точно пристраиваясь к его контактам. Фактически это подключение изнутри банкомата. Пластиковая болванка вынимается обратно, а закладка остается внутри устройства. Функционирует она так же как обычный скиммер, — перехватывает данные и посредством микропередатчика ретранслирует их на принимающее устройство.

И на сегодняшний день, самый современный вид кражи данных и денежных средств – дистанционный, который работает только с бесконтактными картами на малой дистанции до 30-35 сантиметров. Мошенники носили с собой считывающее устройство, работающее по принципу банковского терминала, и в час-пик снимали деньги с карт владельцев.

Всех этих видов мошенничества можно избежать, если перед проведением какой-либо операции со смарт-картой будет произведена аутентификация владельца по отпечатку его пальца, хранящегося в памяти карты.

Логика работы описываемой смарт-карты.

Описать логику работы защищенной смарт-карты могут следующие схемы.

На рис. 1 представлена общая схема разрабатываемой карты

Рис. 1. Блок-схема разрабатываемой карты

При использовании карты в первую очередь, до запроса данных из банка терминалом, срабатывает емкостной датчик отпечатка пальца, его работу можно увидеть на рисунке 2.

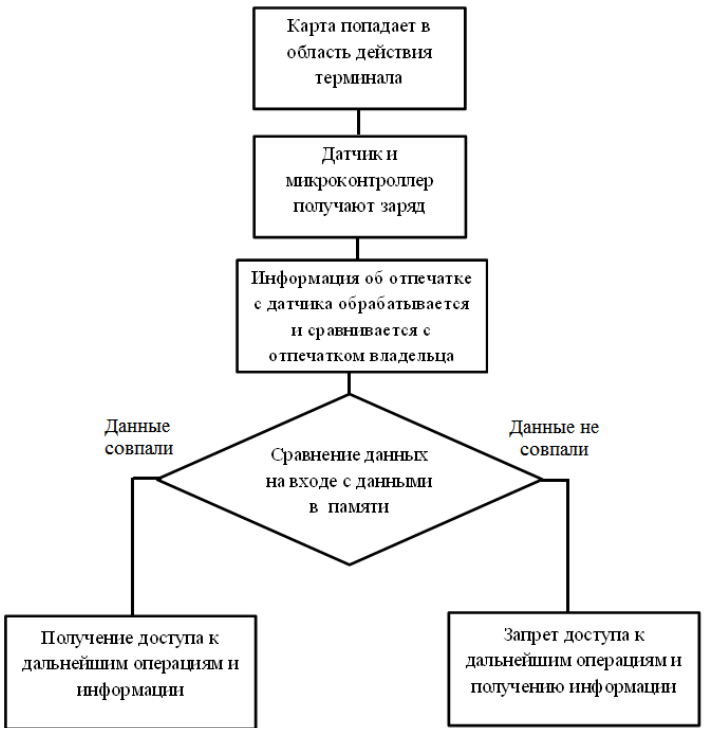

Рис. 2. Блок-схема взаимодействия датчика и микропроцессора

После идентификации владельца карты (получении доступа к дальнейшим операциям и информации), терминал отправит запрос для получения информации о карте и дальнейшей оплате товара по следующей схеме:

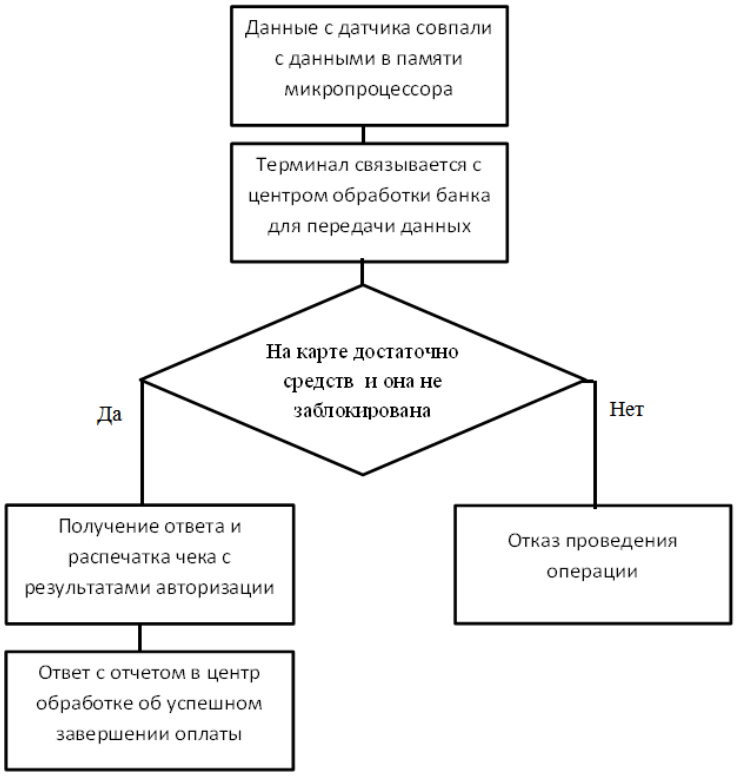

Рис. 3. Блок схема проведения платежной операции

Разработка принципиальной схемы разрабатываемой смарт-карты.

Работу смарт-карты с биометрической аутентификацией можно проиллюстрировать с помощью электронных компонентов, руководствуясь протоколом ISO 7816 – международный стандарт, применяемый к электронным картам, в частности к смарт-картам дистанционного считывания. Используются следующие компоненты: микроконтроллер PIC16F84 с частотой радиоканала 13,56 МГц и 24C16 - электрически стираемое перепрограммируемое ПЗУ, один из видов энергонезависимой памяти необходимый для хранения идентификационных данных необходимых для аутентификации владельца. Т.е. с помощью микросхем PIC16F84, 24C16 и контактной площадки можно эмитировать работу банковской карты с микропроцессором.

Память программы находится в области памяти ROM (микросхема 24C16) и программируется на заводе изготовителе. Программа смарт-карт микроконтроллера создается в форме операционной системы и имеет возможность гибкой настройки, что дает возможность включить в схему датчик отпечатка пальца и наладить его работу [1].

Микроконтроллер PIC 16F84 (CPU) оперирует всеми элементами периферии, производит вычислительные операции и управляет криптозащитой. Микроконтроллер при помощи устройства управления памятью обеспечивает распределение памяти и управление программами, записанными в однократно программируемую память (ROM, 24C16), оперативную память (RAM), которые предназначены для хранения операционной системы и программ смарт-карт микроконтроллера.

Далее в схему, представленную на рисунке 4, согласно цели работы, необходимо внедрить датчик отпечатка пальца для биометрической аутентификации владельца и повышения надежности и безопасности использования смарт-карты.

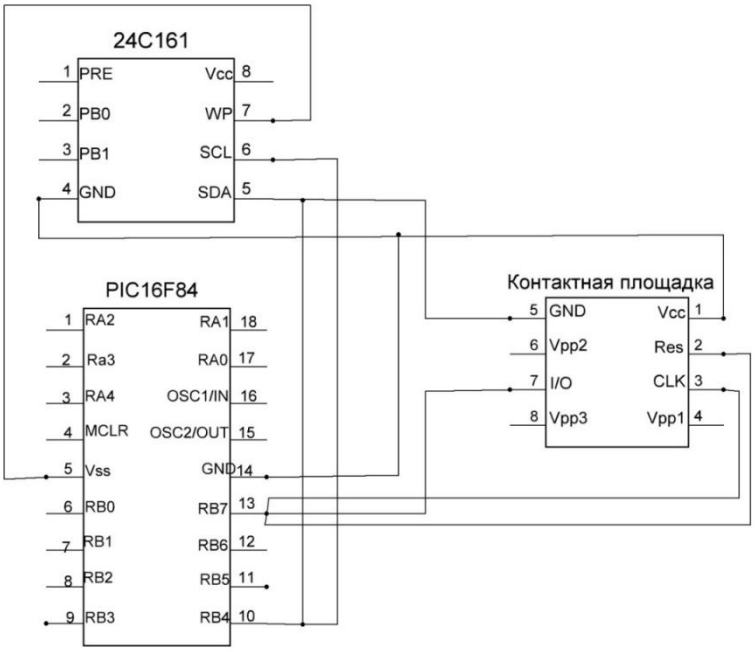

Рис. 4. Принципиальная схема внутреннего устройства банковской карты с микропроцессором

На рисунке 5 представлена схема смарт-карты, оснащенная датчиком отпечатка пальцев модели FPS GT511C3.

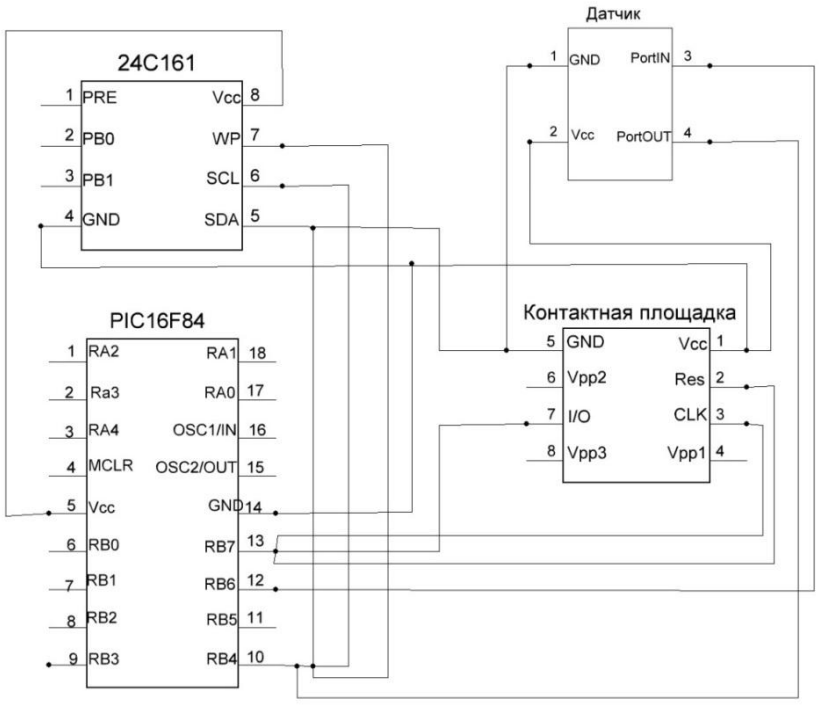

Рис. 5. Принципиальная схема внутреннего устройства банковской карты с микропроцессором и датчиком отпечатка

Заключение.

Очевидно, что с уровнем развития беспроводных информационных технологий растет и уровень устройств, предназначенных для хищения информации и денежных средств с банковских смарт-карт.

Для предотвращения случаев мошенничества, описанных в работе, необходим новый уровень защиты потребителей банковских услуг.

Список литературы

1. *Юргенсен Т.М., Гатери С.Б.*. Смарт-карты. Настольная книга разработчика // КУЛИЦ-ОБРАЗ, январь 2003. ISBN 978-0-470-74367-6.
2. *Мыльников С*. Учебно-методическое пособие. Азы биометрии// Н-Л 2007. 60 стр. ISBN 978-5-94869-040-7.
3. *Paret* Dominique. RFID and Contactless Smart Card Applications// Willey, August 2005. 348 p. ISBN: 978-0-470-01195-9.
4. Ставим на карту. Как выбрать карту для расчетов в интернете – простых, удобных, безопасных // [Электронный ресурс]. Режим доступа: http://myfin.by/stati/view/3533-stavim-na-kartu-kak-vybrat-kartu-dlya-raschetov-v-internete--prostyh-udobnyh-bezopasnyh/ (дата обращения: 18.08.2015).
5. Ставим на карту. Скимминг, траппинг, ливанские петли и три действенных способа защиты // [Электронный ресурс]. Режим доступа: http://myfin.by/stati/view/3715-stavim-na-kartu-skimming-trapping-livanskie-petli-i-tri-dejstvennyh-sposoba-zashhity/ (дата обращения: 19.08.2015).
6. PIC16F84A Datasheet, Microchip Technology.-2002 Microchip Technology Inc. 337 c.
7. 24C16 Datasheet – STMicroelectronics, 1999 STMicroelectronics GROUP OF COMPANIES. 17 c.