Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра защиты информации

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

Лабораторный практикум
для студентов специальности
«Сети телекоммуникаций»
всех форм обучения

Минск 2006

УДК 681.326.7 (075.8)
ББК 32.973-04я73
З-40

Р е ц е н з е н т:
доцент Высшего государственного колледжа связи,
канд. техн. наук В.В. Соловьев

А в т о р ы:
Л.М. Лыньков, В.А. Богуш, Т.В. Борботько, А.М. Прудник

Защита информации в банковских технологиях: Лабораторный
З-40 практикум для студ. спец. «Сети телекоммуникаций» всех форм обуч. / Л.М. Лыньков, В.А. Богуш, Т.В. Борботько, А.М. Прудник. – Мн.: БГУИР, 2006. – 60 с.: ил.
ISBN 985-444-951-3

Лабораторный практикум содержит краткие теоретические сведения к темам курса, ход выполнения лабораторного задания, требования к оформлению отчета и вопросы для самоконтроля к каждой теме. При выполнении работ реализована возможность автоматизации контроля знаний студентов. Каждая работа содержит перечень контрольных вопросов, ответы на которые контролируются программной экспертной системой.

Предназначен для студентов высших учебных заведений, обучающихся по специальности «Сети телекоммуникаций».

УДК 681.326.7 (075.8)
ББК 32.973-04я73

ISBN 985-444-951-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационные технологии и электронная техника незаменимы в банковском деле и сейчас наступает новый этап повсеместной компьютеризации, когда человек, не выходя из дома, может пользоваться банковскими услугами посредством Интернета. При активном использовании информационной глобальной сети возникают проблемы, связанные с информационной безопасностью. Ее ключевыми направлениями являются: защита коммерческой информации при ее передаче по каналам связи, надежность долгосрочного хранения данных в электронном виде, контроль доступа к информации, в том числе и через Интернет, предотвращение несанкционированного доступа к информации, аутентификация ее пользователей.

В результате появления безналичных (электронных) денег наметилась устойчивая тенденция вытеснения их бумажного эквивалента. Электронные деньги представляющие собой серии зашифрованных наборов символов, заменяющие банковские купюры прочно входят во все сферы жизни человека. Как средство платежа и накопления они представляют собой информацию о количественном выражении стоимости денежного эквивалента. По мере того как человек использует их для совершения сделок и оплаты товаров или услуг, информация об их денежной стоимости, хранящаяся на электронном устройстве, изменяется. Отличительной чертой электронных денег от таких привычных банковских продуктов, как депозитные или кредитные карты, является то, что при их применении не используется банковский счет лица, которому они принадлежат.

С ростом числа услуг, предоставляемых современными банками, возникает проблема информационной безопасности банковских систем, наблюдается рост требований к повышению их защищенности, надежности, а также конфиденциальности проводимых транзакций, что делает проблему защиты информации в банковских технологиях весьма актуальной.

1. БАНКОВСКИЕ ЭЛЕКТРОННЫЕ ПЛАСТИКОВЫЕ КАРТЫ

Цель работы: Изучить принципы построения банковских электронных пластиковых карт, методы защиты информации в них.

1.1. Теоретическая часть

1.1.1. Общая характеристика карт

На сегодняшний день чип-карта, или карта с интегральной микросхемой, - это пластина из полимерного материала, по размерам идентичная карте с магнитными полосами (например, кредитной). Нововведение состоит в возможности разместить в карте обыкновенной толщины одну или несколько интегральных микросхем и в применении переходной (соединительной) платы, способной обеспечить электрический контакт со специальным переходным (интерфейсным) устройством.

Микромодулем принято называть очень тонкую печатную плату, которую можно увидеть на поверхности чип-карты. На внешней стороне микромодуля расположены контактные площадки для подключения к внешним устройствам; на внутренней стороне размещается кристалл микросхемы. Технология называется Chip on Board - кристалл на плате.

Чип-карты часто отличают друг от друга по функциональному назначению микромодуля, иначе говоря, по их внутренним интегральным микросхемам. С учетом этого можно выделить три большие группы чип-карт:

- карты с простой памятью;
- карты с программируемой памятью;
- карты с микропроцессором.

1.1.2. Анализ носителей информации

С точки зрения принципа хранения информации, карточки могут быть:

- со стилизованными шрифтами типа ORC;
- со штриховым кодом;
- с магнитной полосой;
- с кодом на основе эффекта Виганда;
- с ППЗУ или электрически стираемым программируемым запоминающим устройством;
- с прибором TOUCH MEMORY;
- с микропроцессором;

– с лазерной записью;
– комбинированные.

В настоящее время в мире нашли широкое применение машиночитаемые *стилизованные шрифты типа ORC*, которые используются в том числе и в банковской сфере для обработки информации с различных платежных документов, ценных бумаг, документов финансовой и статистической отчетности.

Машиночитаемые стилизованные шрифты применяются также для вкладыша паспорта, на который заносятся сведения о владельце, предназначенные для пограничного контроля. В паспорте указывается страна, номер документа, фамилия, имя и отчество, подданство и дата рождения владельца. Информация в виде стилизованного шрифта может наноситься при помощи универсальных (ударных матричных, струйных, лазерных) принтеров под управлением ПЭВМ.

Машинное считывание осуществляется путем разложения каждого символа на отдельные фрагменты и последующего сравнения с соответствующим эталоном в памяти считывающего устройства или ЭВМ. Особенность данного типа носителя информации заключается в возможности считывания одних и тех же данных специальным сканирующим устройством и непосредственно человеком. Для машинного способа считывания ORC-шрифтов требуются достаточно сложные программно-аппаратные средства.

Карточки со стилизованными шрифтами относятся к носителям с однократной записью и многократным считыванием информации.

Информация на карточку может быть нанесена в виде *штриховых кодов*, представляющих собой чередование вертикальных черных и белых полос разной ширины. Информацию несут относительные размеры ширины штрихов и пробелов и их сочетание. На сегодня созданы и находят различное применение в мире порядка 50 видов штриховых кодов. Однако на пластиковых карточках применение получили лишь несколько из них, а именно: «2 из 5», «2 из 5 чередующийся», EAN, «39», «Кода бар», «93» и «128». На перечисленные коды разработаны национальные стандарты, а на EAN и «2 из 5 чередующийся» разработаны международные рекомендации для национальных стандартов.

Штриховой код может наноситься при помощи универсальных принтеров под управлением ПЭВМ. Причем одновременно с кодом на карточку могут наноситься и все необходимые данные о владельце, что достаточно удобно для оперативного изготовления карточки, например, на предприятии. Карточки со штриховыми кодами также относятся к носителям с однократной записью и многократным считыванием информации.

Считывание штриховых кодов осуществляется оптическими считывающими устройствами (щелевым считывателем или световым пером), ПЗС-сканерами, лазерными сканерами различных конструкций (ручными или стационарными).

Штриховые коды имеют относительно невысокую информационную емкость. На карточке стандартных размеров может быть размещено до 16 символов. При скорости перемещения карточки через оптический щелевой считыватель 80 мм/с скорость считывания составляет 3 Кбит/с.

Для защиты от перекопированния штриховой код может быть закрыт черной пленкой.

Карточки со штриховыми кодами широко используются на предприятиях как личные карточки работников для комплексного применения в контрольно-пропускной системе, для учета норм выработки, сдачи-приемки продукции, для безналичных расчетов в филиале сбербанка и т.д.

При этом штриховым кодом, как правило, кодируют личный регистрационный номер владельца, код предприятия, версию документа, персональный идентификационный номер (ПИН).

Карточки *с магнитной полосой* – наиболее распространенный в мире носитель информации для автоматизированных информационных систем.

Карточки с магнитной полосой относятся к носителям с многократной записью и многократным считыванием информации. Данные на магнитную полосу записываются на три дорожки.

Информация, записанная на магнитной полосе, совпадает с данными, отображенными на лицевой стороне карточки, нанесенными рельефным способом-тиснением (кроме секретного персонального идентификационного номера (ПИН)). ПИН записывается на магнитной полосе в неявном, зашифрованном виде. Появление в технологии обработки карточек секретного ПИН-кода делает магнитную карточку достаточно защищенной от обманного получения полномочий. В некоторых системах безналичных расчетов ПИН хранится не на карточке, а в базе данных POS (Point of sale) терминалов или в расчетном центре, что наряду с другими средствами обеспечивает высокую степень защиты владельца карточки и системы от мошенничества.

В отличие от всех носителей, магнитная карточка полностью защищена международными стандартами ISO, что является фактом ее международного признания и распространения.

Карточки с носителями информации *на основе эффекта Виганда* нашли распространение как высокозащищенные и высоконадежные идентификационные карточки для контрольно-пропускных систем и систем санкционированного доступа.

Эффект Виганда заключается в резком изменении магнитного потока, происходящем в так называемой проволоке Виганда при определенных условиях приложения внешней магнитодвижущей силы. Эта проволока характеризуется разомкнутой петлей гистерезиса, что не наблюдается у других магнитных материалов. Карточка Виганда запатентована, и принцип кодирования с целью защиты от подделки держится в секрете. Современные карточки Виганда с однократной записью и многократным считыванием данных имеют информационную емкость порядка 32 бит. Большим достоинством карточки Виганда является отсутствие каких-либо внешних признаков носителя на поверхности карточки, а также бесконтактный способ считывания данных.

Пластиковая карточка *со встроенной микросхемой памяти* (ППЗУ или ЭС ППЗУ) называется, как и карточка с микропроцессором, чип-картой. Как правило, карточка памяти реализована или в виде однократно программируемого постоянного запоминающего устройства, которое можно считывать много раз, но данные в каждую ячейку памяти могут быть записаны только один раз, или в виде электрически стираемого программируемого постоянного запоминающего устройства, которое можно считывать много раз, но данные в каждую ячейку памяти могут быть записаны только один раз, или в виде ЭС ППЗУ, которое можно перезаписывать и считывать многократно. Объем памяти может составлять от 32 байт до 8 Кбайт (обычно – 256 байт). Уровень защиты информации карточки значительно невысокий, поэтому они нашли применение в прикладных системах, не требующих высокого уровня защиты, например, для оплаты телефонных разговоров, автостоянок и т.д.

Схемы памяти могут иметь раздельные области памяти (одна для данных, другая для хранения паролей, например, ПИН-владельца), а также встроенную управляемую логику для организации доступа к данным. Карточки памяти со встроенной управляемой логикой и микропроцессорные карточки называются смарт-карты.

Обычно фирмы специализирующиеся на выпуске карточек памяти, выпускают семейство чипов. Наиболее характерное семейство схем памяти приведено на примере продукции, выпускаемой фирмой GEMPLUS (Франция) – самой крупной среди производитей чип-карт в мире:

GSM – карточки с простой памятью без защиты.

GCM – карточки с управляемой памятью. Логическая схема в составе чипа осуществляет управление доступом к памяти с ПИН.

GPM – карточки с индивидуализацией памяти. Особая область памяти, защищенная перемычкой, может содержать данные об идентификации, которые нельзя изменить при сгорании перемычки. Доступ к остальной части памяти управляется встроенной логической схемой.

Приборы *TOUCH MEMORY* фирмы Dallas Semiconductor (США) – это семейство приборов с батарейным питанием в миниатюрном корпусе из прочной нержавеющей стали диаметром 16 мм и толщиной порядка 3 или 6 мм. Считать данные из TOUCH MEMORY или выполнить запись в него можно при помощи одной сигнальной и одной земляной линий. Для сохранения информации в памяти в корпусе размещена миниатюрная литиевая батарейка, обеспечивающая сохранность данных в памяти в течение 10 лет. Корпус прибора может выдержать более одного миллиона механических подключений без заметного износа и обеспечивает использование прибора в особо тяжелых условиях эксплуатации, в том числе в агрессивных средах.

Каждый прибор семейства имеет уникальный серийный 64-битовый номер, который заносится в процессе изготовления и который невозможно изменить в процессе эксплуатации. Завод гарантирует, что нет двух приборов с одинаковыми номерами.

Семейство TOUCH MEMORY включает пять приборов, одинаковых по конструкции, интерфейсу, но с различным типом и объемом памяти. Младшая модель имеет только постоянное запоминающее устройство (ПЗУ) с серийным номером, все остальные имеют дополнительно к ПЗУ перезаписывающую память объемом от 1 до 4 Кбит. Отдельные приборы семейства имеют независимые области памяти, которые защищены для считывания и записи паролями, что обеспечивает защиту памяти от несанкционированного изменения содержимого. Старшая модель семейства дополнительно к памяти объемом 4 Кбит имеет часы реального времени. По истечении установленного времени или числа обращений доступ к памяти блокируется.

Приборы TOUCH MEMORY находят широкое применение в системах санкционированного доступа, в системах автоматизации технологических процессов, в разнообразных системах автоматической идентификации.

Микропроцессорные карточки появились в результате научно-технического прогресса в области микропроцессорной техники и микроэлек-

троники. Представляют собой сочетание в одном чипе нескольких типов запоминающих устройств под управлением микропроцессора и операционной системы.

Микропроцессорная карточка включает в себя:

CPU – центральное процессорное устройство;

ROM – постоянное запоминающее устройство с набором программ, заложенных в процессе производства масочным методом;

RAM – запоминающее устройство с произвольной выборкой. Рабочая память для временного хранения данных;

EPROM – однократно программируемая, энергонезависимая память, содержащая произвольные прикладные подпрограммы пользователя, конфиденциальные коды для защиты областей памяти и т. д.;

EEPROM – электрически стираемое многократно программируемое ПЗУ, содержащее произвольные прикладные подпрограммы пользователя, конфиденциальные коды для защиты областей памяти;

OPERATING SYSTEM – операционная система или программное обеспечение карточки.

Микропроцессорная карточка обеспечивает выполнение следующих функций: идентификацию владельца карточки; идентификацию карточки с точки зрения возможности использования в данной системе; подтверждение наличия принятого или передаваемого сообщения для гарантии целостности; возможность накопления и управления данными и обеспечение их безопасности; генерацию ключей кодов; шифрование передаваемых данных с помощью сложных криптоалгоритмов, например, по стандарту DES.

Микропроцессорная карточка обеспечивает исключительно высокий уровень безопасности. В чипе защищена область памяти, содержащая секретную информацию (ПИН). При наличии неправильного исходного кода или трехкратного неправильного набора ПИН происходит автоматическая блокировка работы карточки. Нестираемая память EPROM характеризуется отсутствием чувствительности к магнитным полям, Х-лучам, УФ-лучам. Все это надежно защищает карточку от мошенничества.

Оптические лазерные карточки строятся по WORM-технологии (однократная запись и многократное чтение) и имеют информационную емкость порядка 16 Мбайт. Запись осуществляется при помощи лазера аналогично записи информации на цифровые оптические диски в аудиосистемах. Лазер–карточки

применяются в информационных системах, где требуется хранить большие массивы данных.

В настоящее время в мире находят широкое применение *комбинированные* карточки с носителями нескольких типов, но не более двух, например, магнитная полоса и штриховой код, микропроцессор и магнитная полоса. Такая карточка позволяет работать в разных системах или разделить обработку на две части:

- идентификация с помощью высокозащищенного маскированного штрихового кода или магнитной полосы;
- дебетирование с помощью микропроцессора.

1.1.3. Области применения пластиковых карт

Все различные носители информации, расположенные на пластиковых карточках, обеспечивают быстрое и надежное автоматическое считывание данных для дальнейшей обработки, однако каждый из носителей имеет свои отличительные особенности, технические и экономические показатели. Исходя из этого, каждый из них занимает определенное место в той или иной системе или потребительской нише.

На рис. 1.1 показаны области применения пластиковых карточек с различными носителями и выполняемые ими функции.

Все носители, кроме микропроцессора, являются пассивными и способны обрабатываться только под управлением интеллектуального терминала или ПЭВМ. Микропроцессорная карточка активна и способна самостоятельно под управлением собственной операционной системы выполнять сложные функции и операции.

Следует отметить, что указанные на рисунке системы можно построить практически на любом носителе. При этом выбор носителя будет определять:

- уровень интеллектуальной нагрузки на средства обработки (на POS-терминалы, банкоматы, локальные автоматизированные комплексы, средства связи, расчетные центры и т.д.);
- уровень защиты клиента и системы (от обманного получения полномочий, модификаций, «взломов»);
- удобство пользователей (с точки зрения времени обслуживания и предоставляемых услуг);
- стоимость и надежность системы в целом.

Рис. 1.1. Области применения электронных пластиковых карт

1.2. Лабораторное задание

1. Включить персональный компьютер.

2. Запустить файл bankcards.exe на выполнение.

3. Появившееся на экране окно содержит текстовый документ, который необходимо последовательно изучить.

4. Переход к следующей странице документа осуществляется с помощью органов управления (обозначенных в виде стрелок), находящихся в верхней части окна, которые позволяют осуществлять переход как к следующей странице документа, так и предыдущей. Перемещение документа в вертикальном направлении осуществляется с помощью полосы прокрутки, расположенной в правой части окна (рис. 1.2).

5. При переходе к очередной странице документа будет предложено ответить на контрольный вопрос (вопросы) по текущему пункту. Ниже текста вопроса располагаются варианты ответов. Необходимо выбрать правильный вариант (варианты) ответов из предложенного списка. Правильный ответ (если он есть) помечается специальным символом (рис. 1.3).

6. После выбора правильного ответа, необходимо нажать на панели управления кнопку (со стрелкой), символизирующую переход к следующей странице документа.

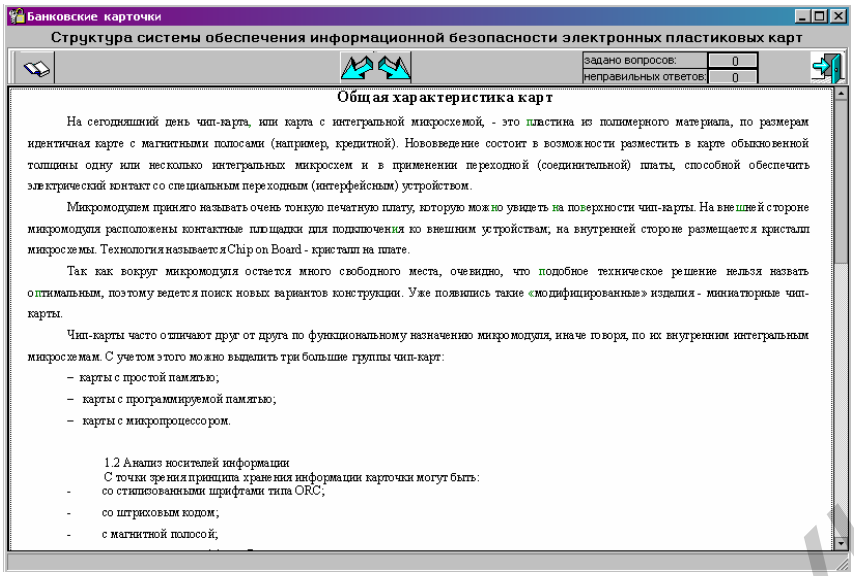


Рис. 1.2. Внешний вид окна программы

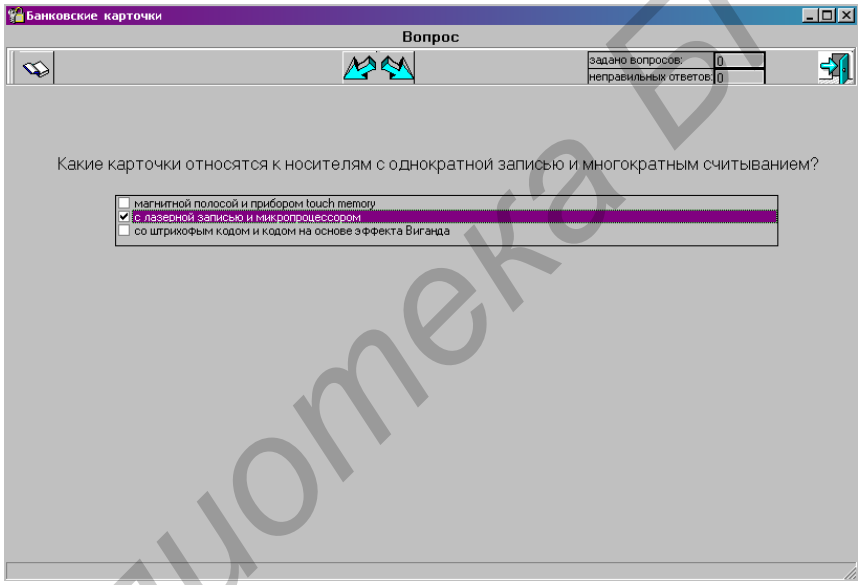


Рис. 1.3. Внешний вид окна вопроса

7. В случае верного ответа выдается соответствующее сообщение (рис. 1.4).

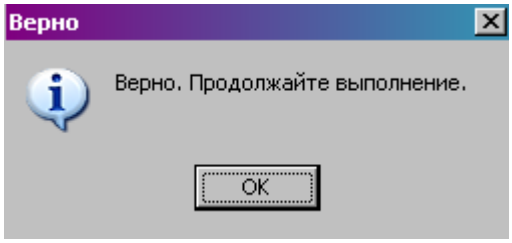


Рис. 1.4. Внешний вид всплывающего окна при верном ответе

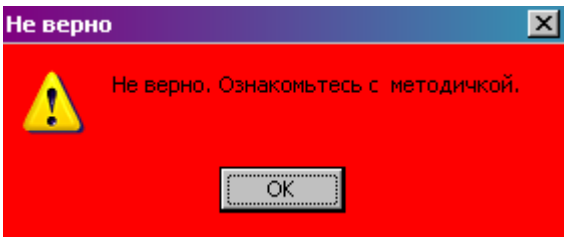


Рис. 1.5. Внешний вид всплывающего окна при неверном ответе

8. В случае неверного ответа выдается соответствующее сообщение и предлагается еще раз изучить предшествующий вопросу текст. Вернуться к данному материалу можно путем нажатия кнопки возврата к предыдущей странице (рис. 1.5).

9. Программа ведет учет количества заданных вопросов и числа неправильных ответов.

10 Лабораторная работа считается выполненной при изучении всего материала, представленного в данной программе, и наличии 90% правильных ответов.

11. Ответить на контрольные вопросы.

12. Оформить отчет.

1.3. Содержание отчета

1. Цель работы.
2. Ответы на контрольные вопросы.
3. Вывод.

1.4. Контрольные вопросы

1. Что называется банковской электронной пластиковой картой?
2. По каким классификационным признакам различаются ЭПК?
3. Каким образом защищается информация в ЭПК на семантическом уровне?
4. Какие печатные элементы, наносимые на ЭПК, защищают ее от подделки?
5. Чем обусловлен выбор тех или иных печатных элементов защиты ЭПК?
6. Какие из известных вам ЭПК имеют низкую степень защиты?
7. Чем обусловлена высокая степень защиты банковской ЭПК с микропроцессором?
8. Что называется персонализацией?
9. Что называется асинхронной ЭПК?
10. Принцип работы асинхронной карты?
11. Назначение микропроцессора ЭПК?
12. Что называется модулем безопасности?

2. ТЕЛЕФОННЫЕ ЭЛЕКТРОННЫЕ ПЛАСТИКОВЫЕ КАРТЫ

Цель работы: Изучить принципы построения телефонных электронных пластиковых карт, методы защиты информации в них.

2.1. Теоретическая часть

2.1.1. Система безопасности телефонных карт

Карта оплаты представляет собой платежный документ, содержащий закодированную информацию, используемую при оплате услуг, в случае таксофонов – услуг телефонной связи.

В таксофонах могут использоваться специализированные телефонные и универсальные карты, имеющие более широкий спектр применения.

Телефонные карты подразделяются на предварительно оплаченные (предоплаченные или дебетовые) карты и абонентские.

Предоплаченная карта, приобретаемая пользователем за деньги, рассчитана на оплату определенного объема предоставляемых услуг, в данном случае – телефонного разговора определенной длительности, определяемой тарифом соединения.

Абонентская карта – это идентификационная карта, несущая индивидуальный номер и номер телефонного счета владельца карты, на который списывается стоимость телефонных разговоров. На абонентской карте может записываться в секретном коде и персональный номер абонента (так называемый ПИН).

Универсальные карты подразделяются на предварительно оплаченные и кредитные. Предоплаченные универсальные карты, выполняющие функции наличных денег, могут использоваться, например, для оплаты телефонных разговоров, автомобильных стоянок и проезда в общественном транспорте. Кредитные универсальные карты, как и абонентские, идентифицированы и позволяют в силу своей универсальности списывать стоимость предоставляемого с таксофона разговора с личного банковского счета владельца карты.

В сетях таксофонов наибольшее распространение получили телефонные предоплаченные карты, выполняющие функции монет, удобные для операторов связи тем, что позволяют производить расчет с абонентами за предоставляемые услуги уже в момент приобретения карты.

Предоплаченные карты, используемые в настоящее время более чем в 110 странах мира, являются основным элементом, определяющим экономические

показатели таксофонного оборудования. Поэтому приобретает все большее значение защита их от различного рода фальсификаций.

Для безналичных расчетов за услуги связи практически используются два вида карт: магнитные и электронные.

На сегодняшний день чип-карта или карта с интегральной микросхемой, – это пластина из полимерного материала, по размерам идентичная карте с магнитной полосой. Нововведение состоит в возможности разместить в карте обыкновенной толщины одну или несколько интегральных микросхем и в применении переходной (соединительной) платы, способной обеспечить электрический контакт со специальным переходным (интерфейсным) устройством.

Микромодулем называется очень тонкая печатная плата, которую можно увидеть на поверхности чип-карты. На внешней стороне микромодуля расположены контактные площадки для подключения к внешним устройствам; на внутренней стороне размещается кристалл микросхемы.

Карта с магнитной полосой представляет собой пластину стандартных размеров (85,6х53,9х0,76 мм), изготовленную из специальной, устойчивой к механическим и термическим воздействиям пластмассы.

Магнитная карта отвечает формату ID-1 стандарта ISO 7810, в котором приводятся основные характеристики «карточек идентификации».

2.1.2. Структура системы обеспечения информационной безопасности электронных пластиковых карт

Основным элементом системы (рис. 2.1) является электронная пластиковая карта типа «Еврочип». Она реализована на базе кристаллов Ап 5001 производства ОАО «Ангстрем» (г. Зеленоград). Разработчики кристаллов учли и устранили ошибки, допущенные при проектировании SLE 4436 (наиболее близкого аналога). ЭПК имеет достаточно большой потенциальный ресурс – до 29000 тарифных единиц, имеет защиты от прерванной записи. Каждая ЭПК имеет индивидуальный ключ карты длиной 256 бит, зашифрованный по ГОСТ 28147-89 и хранящийся в области памяти, закрытой для чтения. Карта является автономным компонентом системы безналичных расчетов и может использоваться как самостоятельное платежное средство. Однако из-за жесткой логики работы ЭПК гарантировать высокую защищенность нельзя.

Поэтому в качестве второго компонента системы используется модуль безопасности (МБ). МБ представляет собой 8-разрядный микроконтроллер с RISK-архитектурой, внутренней операционной системой с протоколом обмена

T=0. Конструктивно выполнен под разъем «PLUG IN» по GSM 11.11 и предназначен для установки в таксофоны. В МБ могут храниться одновременно до 16 ключей, которые недоступны для чтения, модификации или удаления. Основное назначение МБ в платежной системе – аутентификация (удостоверение подлинности) кристалла на всех этапах производства и эксплуатации ЭПК.

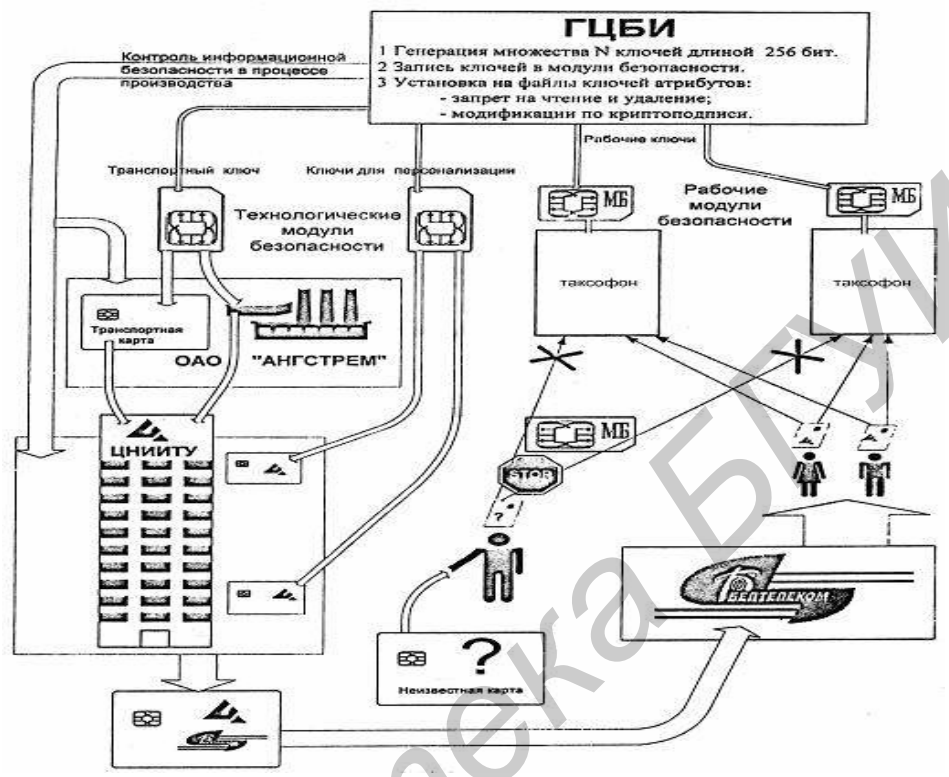


Рис. 2.1. Структура системы обеспечения информационной безопасности ЭПК

Для повышения стойкости системы к взлому в ней используются МБ с различными ключами на этапах изготовления и эксплуатации ЭПК. При изготовлении кристалла на завод-изготовитель передается МБ с транспортными ключами A_1-A_{16}. Изготовитель кристалла использует эти ключи для записи в кристалл зашифрованного транспортного кода и для создания транспортной карты, содержащей опять-таки зашифрованный ключ. При этом для каждой партии кристаллов используется один из ключей A_i, а по истечении определенного времени может быть произведена полная замена ключей. Прочитать исходные ключи A_i в открытом виде и получить информацию о работе ключей $Б_i$ изготовитель кристаллов не может.

После изготовления ЭПК транспортная карта и МБ с ключами A_i используются для входа в режим персонализации карты. Войти в этот режим возможно только, если зашифрованные транспортные ключи в кристалле и транспорт-

ной карте будут успешно расшифрованы и опознаны МБ с рабочими ключами $Б_i$, которые также должны содержать МБ, установленные в таксофонах. По окончании персонализации транспортный ключ из карты удаляется, но записывается индивидуальный ключ карты (ИКК) длиной 256 бит, зашифрованный на рабочем ключе $Б_i$, в закрытую для чтения область памяти. Изготовителю таксофонов передается МБ с рабочими ключами $Б_1$-$Б_{16}$, также недоступный для чтения, модификации и удаления, при этом ему неизвестны транспортные ключи.

На рабочем месте персонализации, где имеется МБ с обеими версиями ключей, они нигде не появляются в открытом виде и по вышеупомянутым причинам получить информацию о ключах невозможно. Генерация ключей, их запись в МБ и наложение соответствующих атрибутов на файлы ключей будут производиться с помощью специальной программы. Поэтому даже оператор, участвующий в генерации ключей, не будет их знать.

При работе ЭПК в таксофоне применена многоступенчатая система защиты от подделки. Во-первых, таксофон считывает служебную информацию с карты и сравнивает ее с шаблоном. В случае несовпадения работа прекращается. Характер этой информации, например серия карт, может со временем меняться или ограничиваться во времени.

Во-вторых, перед началом работы таксофон с помощью МБ проводит аутентификацию ЭПК. После очередного списания тарифных единиц модифицируется ИКК и аутентификация повторяется. При неподтверждении подлинности работа с картой запрещается.

В-третьих, в процессе работы обмен ключевой информацией производится в зашифрованном виде. Поэтому снятие временных диаграмм обмена между МБ и картой не позволит расшифровать ключи, так как временные диаграммы при последующих сеансах связи повторяться не будут. В процессе аутентификации восстановление ключевой информации также невозможно.

В-четвертых, выбор ключа может производиться по номеру его файла, записанному в карте. Принципиально возможен дистанционный выбор ключа.

2.1.3. Модуль безопасности

Интегральная схема модуля безопасности размещается в контроллере ридера таксофона и в аппаратуре персонализации. В совокупности с ИМС карточки КР 5004РР1 МБ обеспечивает высокий уровень защиты от несанкционированных действий.

МБ (рис. 2.2) выполняет следующие функции в таксофоне:

– проверка подлинности телефонной карты;
– хранение и защита ключей для работы с телефонной картой и компьютером телефонной станции;
– проведение двухсторонней аутентификации и обмен криптографически защищенными данными между МБ и компьютером центральной станции;
– хранение данных совокупной длительности телефонных звонков, обслуженных оператором;

в аппаратуре персонализации:

– проверка подлинности карты с использованием транспортного ключа;
– выработка индивидуального ключа карты (ИКК).

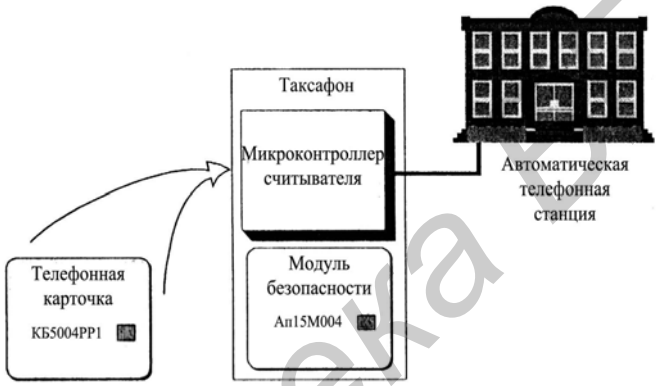


Рис. 2.2. Модуль безопасности

2.1.4. Персонализация

На этапе персонализации производится загрузка области персонализации карты, загрузка ИКК, установка счетчика.

Перед персонализацией карта защищена транспортным ключом карты, который передается с транспортной картой в зашифрованном виде и загружается в модуль безопасности.

Персонализация построена с использованием концепции высокой безопасности:

– доставка продукции потребителю защищается специальной транспортной картой;
– в процессе персонализации ИКК не появляется в открытом виде;
– загрузка данных в карту проверяется процедурой аутентификации.

Процедура персонализации приведена на рис. 2.3.

Рис. 2.3. Процедура персонализации

2.1.5. Аутентификация

КБ 5004РР1 содержит блок секретности, который позволяет проводить защищенную операцию аутентификации между карточкой и ридером, используя индивидуальный ключ карты.

Аутентификация проводится МБ, который поставляется вместе с телефонными картами. Каждая карта содержит:

- ИКК, который вычисляется в процессе персонализации, хранится в защищенной области ЭС ППЗУ и имеет объем 256 бит;
- блочный алгоритм шифрования (32 цикла с таблицами перестановки).

Под аутентификацией подразумевается передача на карту запроса (случайного числа) и получение ответа.

Процесс аутентификации повторяется в течение одного сеанса связи для каждого нового значения счетчика с целью исключения возможной подмены ЭПК. Функция предсказания ожидаемого ответа от карты возлагается на установленный в таксофоне МБ.

Процесс взаимодействия таксофона, МБ и ЭПК происходит следующим образом:

- чтение открытых данных ЭПК, пассивная аутентификация (проверка производителя карты по первым трем байтам карты), определение номера рабочего ключа (KEY0), проверка счетчика карты;
- проверка наличия в таксофоне МБ для данного типа ЭПК;
- передача открытых данных ЭПК в МБ. Расчет МБ ИКК (KEYi) на основе алгоритма f2 и рабочего ключа (KEY0), содержащегося в памяти МБ;

– генерация МБ случайного числа (CHALL).
– передача CHALL в ЭПК, запуск алгоритма f1 и получение ответа (RES) от карты;
– чтение счетчика карты;
– передача в МБ содержимого счетчика карты, запроса (CHALL), ответа от карты (RES) и получение ответа “свой-чужой”;
– уменьшение счетчика карты.

Процесс аутентификации в МБ состоит из двух этапов. В ходе первого – модулем вычисления ИКК (KEY_i), а во время второго – с помощью ответа ЭПК на данный запрос.

В течение одного сеанса связи нет нужды повторять первый этап, т.к. значение KEY_i для данной ЭПК сохраняется в памяти МБ. Второй этап необходимо повторять многократно после каждого уменьшения счетчика карты (рис. 2.4).

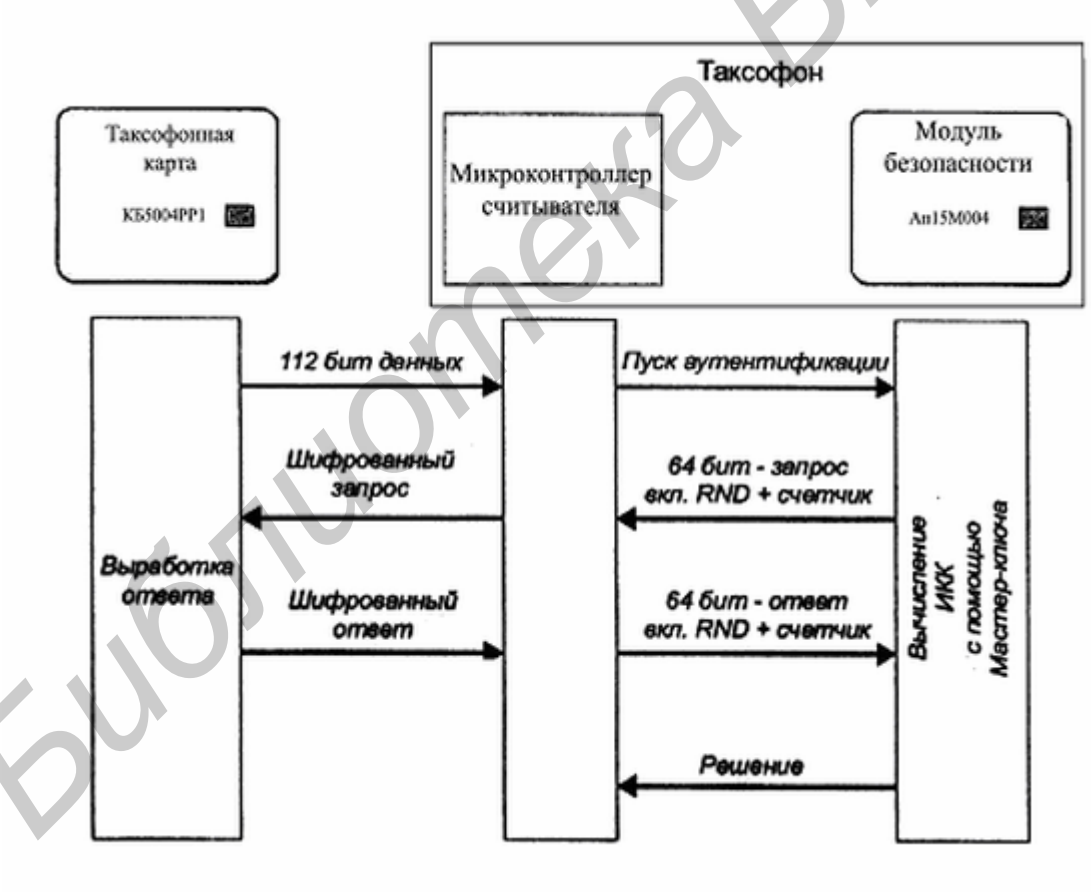


Рис. 2.4. Процедура аутентификации

2.2. Лабораторное задание

1. Включить персональный компьютер.

2. Запустить файл phonecards.exe на выполнение.

3. Появившееся на экране окно содержит текстовый документ, который необходимо последовательно изучить.

4. Переход к следующей странице документа осуществляется с помощью органов управления (обозначенных в виде стрелок), находящихся в верхней части окна, которые позволяют осуществлять переход, как к следующей странице документа, так и предыдущей. Перемещение документа в вертикальном направлении осуществляется с помощью полосы прокрутки, расположенной в правой части окна (рис. 2.5).

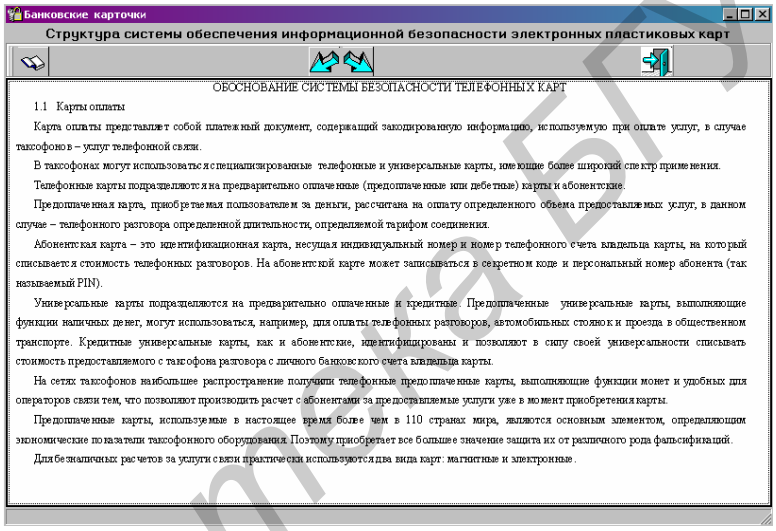


Рис. 2.5. Внешний вид окна программы

5. При переходе к очередной странице документа будет предложено ответить на контрольный вопрос (вопросы) по текущему пункту. Ниже текста вопроса располагаются варианты ответов. Необходимо выбрать правильный вариант (варианты) ответов из предложенного списка. Правильный ответ (если он есть) помечается специальным символом (рис. 2.6).

6. После выбора правильного ответа, необходимо нажать на панели управления кнопку (со стрелкой), символизирующей переход к следующей странице документа.

7. В случае верного ответа, выдается соответствующее сообщение (рис. 2.7).

8. В случае неверного ответа выдается соответствующее сообщение и предлагается еще раз изучить предшествующий вопросу текст. Вернуться к

данному материалу можно путем нажатия кнопки возврата к предыдущей странице (рис. 2.8).

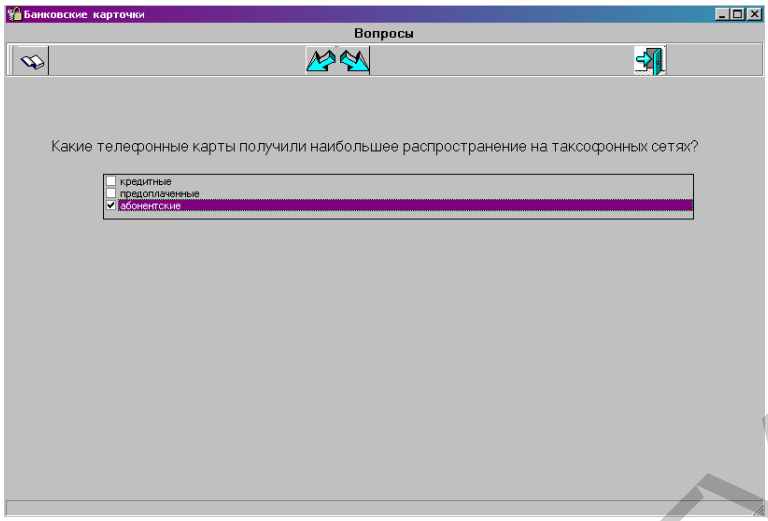


Рис. 2.6. Внешний вид окна вопроса

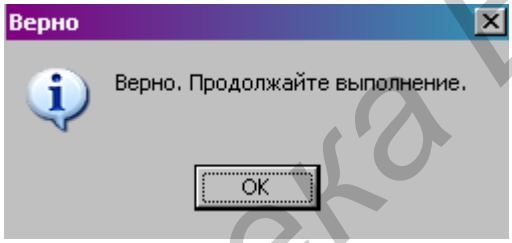


Рис. 2.7. Внешний вид всплывающего окна при верном ответе

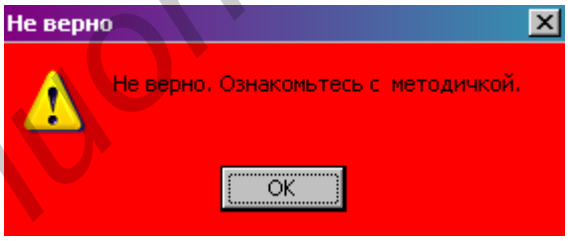


Рис. 2.8. Внешний вид всплывающего окна при неверном ответе

9. Лабораторная работа считается выполненной при изучении всего материала, представленного в данной программе, и при наличии 90% правильных ответов.

10. Ответить на контрольные вопросы.

11. Оформить отчет.

2.3. Содержание отчета

1. Цель работы.
2. Ответы на контрольные вопросы.
3. Вывод.

2.4. Контрольные вопросы

1. Что называется телефонной электронной пластиковой картой?
2. Какова структура дорожек магнитной полосы телефонной ЭПК?
3. Для чего проводится посимвольный контроль на четность записанной на магнитную полосу информации?
4. Какова структура декодера сигналов считываемых с телефонной ЭПК?
5. Чем отличаются печатные и интегрируемые элементы защиты телефонной ЭПК?
6. Чем обусловлен выбор печатных и интегрируемых элементов защиты информации, находящейся на магнитной полосе ЭПК?
7. Что называется телефонной картой с простой памятью?
8. Чем отличаются синхронные телефонные ЭПК от асинхронных?
9. Какие методы дифференциального анализа искажений криптоинформации вы знаете?
10. Что называется транспортным ключом?
11. Что называется счетчиком тарифных единиц?
12. Назначение модуля безопасности?
13. Для чего проводится процедура персонализации?
14. Назначение аутентификации?

3. АППАРАТНОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БАНКОМАТОВ DIEBOLD (IBM)

Цель работы: Изучить конструктивные особенности банкоматов, состав аппаратного и программного обеспечения.

3.1. Краткие теоретические сведения

3.1.1. Функции банкоматов и их классификация

Банкоматы используются для автоматического выполнения следующих операций:

- выдачи наличных денег,
- операций со счетами клиента,
- пополнения электронных кошельков,
- приема денег и документов (чеков) на хранение для последующей инкассации,
- документального подтверждения проведенных операций,
- печати информации о текущем состоянии лицевого счета,
- чтения информации с карточек (как с магнитной полосой, так и с микросхемой) и записи информации на них.

Как правило, банкоматы выпускаются в разных вариантах, различающихся функциональными возможностями и предназначенных для использования в различных условиях.

Так, простейшие банкоматы (cash dispenser) могут только выдавать наличные деньги. Более сложные, или полнофункциональные банкоматы (именно их называют Automated Teller Machine), способны при соответствующей комплектации не только выдавать деньги (как банкноты, так и монеты), но и предоставлять ряд других банковских услуг: доступ к работе с лицевыми счетами, прием вкладов, прием документов с их электронной обработкой, печать информации о состоянии лицевого счета и сберегательной или расчетной книжки.

Банкоматы различаются также размерами, местом установки и способом обслуживания (загрузки) персоналом. Они могут быть настольными и напольными, предназначаться для установки в помещениях или на улице, встраиваться в стену, вскрываться сзади или спереди. Банкоматы, предназначенные для установки на улице, отличаются от банкоматов, устанавливаемых в помещениях более широкими диапазонами допустимых атмосферных характеристик. Например, для банкоматов InterBold, предназначенных для установки на улице,

допустимы температуры от -34 до +54^{0}C и относительная влажность от 15 до 100%.

Крупные фирмы - изготовители банкоматов предлагают заказчикам широкий набор дополнительного рекламного, защитного (от погодных воздействий и пр.) и охранного оборудования для банкоматов.

3.1.2. Конструктивные особенности банкоматов

Модульная конструкция с открытой архитектурой предоставляет потребителю широкие возможности конфигурирования системы. Так, можно начать с базового варианта, обеспечивающего выдачу наличных денег по кредитным (дебетовым) карточкам, а затем постепенно добавлять такие возможности как цветная графика, речевой интерфейс с пользователем, принятие денег на депозит и т.д.

Основные функциональные модули банкоматов таковы:

- специальные принтеры;
- карт-ридер;
- клиентская клавиатура;
- графический монитор высокого разрешения;
- процессор и электронный накопитель данных;
- устройство выдачи банкнот (обеспечивает подачу банкнот из кассет, в которых они хранятся, до окошка выдачи их получателю);
- кассеты для хранения банкнот;
- устройство регистрации проведенных транзакций (может располагаться на удалении до 600 м);
- устройства приема денег и документов на депозит;
- устройства обеспечения безопасности.

3.1.3. Аппаратное обеспечение

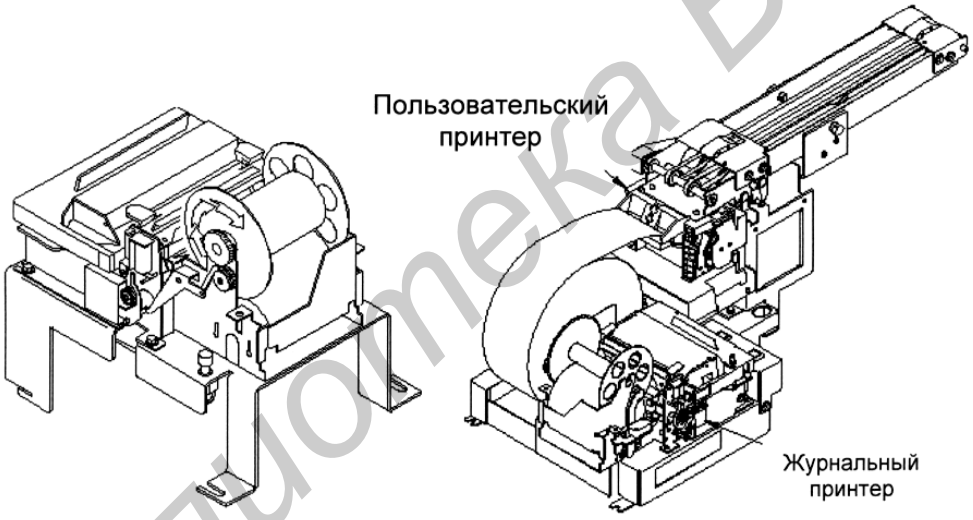
Журнальный принтер предназначен для вывода информации на печать. На журнальной ленте отражаются статусы состояния устройств банкомата и проводимые клиентами или обслуживающим персоналом банка операции. Лента журнального принтера является важным документом при инкассации банкомата и выявлении неисправностей, она находится внутри банкомата во время одного операционного дня.

Существуют две основные разновидности журнальных принтеров. Первая - отдельно стоящий журнальный принтер. Номера этих моделей 957 и 516. Вто-

рая - принтер расположен вместе с пользовательским принтером на одном основании. Номер модели этого принтера 112. Никаких коренных различий между ними нет: печатающий механизм идентичен, различается только схема крепления (рис. 3.1).

В основе принципа работы журнального принтера лежит принцип печати обычных матричных принтеров. Нанесение краски на бумагу происходит следующим образом.

В головке матричного принтера расположены девять иголок. Основание каждой иголки находится внутри соленоида. После того как на соленоид приходит управляющий электрический импульс, в соленоиде формируется магнитный импульс, который выбрасывает иглу. Она ударяется в ленту картриджа, на которую нанесена краска. В этот момент времени игла прижимает ленту картриджа к бумаге и на бумаге остается пятнышко краски, соответствующее своими размерами диаметру иглы.



а) б)

Рис. 3.1. Журнальные принтеры: а-модели 957(516), б-модель 112

Так как в матричном принтере имеется механизм подачи бумаги вверх, а сама головка принтера имеет возможность перемещаться вдоль листа бумаги по своим направляющим, то печатающий механизм принтера имеет возможность наносить знаки на всей ширине и протяженности листа бумаги. Таким образом, напечатанный знак имеет вид, представленный на рис. 3.2.

Чековый принтер предназначен для вывода информации на печать (рис. 3.3). На чековом принтере печатается информация по транзакциям (баланс счета, выдача наличных, перевод средств, депозит и т.д.), а также служебная

информация (баланс банкомата, показания счетчиков купюр, счетчиков задержанных карт, статус-лист и т.д.).

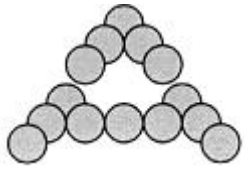


Рис. 3.2. Внешний вид печатаемого знака

Чеки, распечатанные на чековом принтере, являются важными финансовыми документами, подтверждающими выполнение финансовых операций с использованием банкомата.

В основе принципа работы чекового принтера лежит принцип печати обычных матричных принтеров. Нанесение краски на бумагу происходит таким же образом.

Устройство для чтения пластиковых карт, или карт-ридер предназначено для чтения и записи информации с магнитных дорожек или микропроцессора (если карт-ридер универсальный) пластиковых карточек (рис. 3.4) клиентов или обслуживающего персонала. Карт-ридер может иметь в своем составе только магнитную часть или магнитную и микропроцессорную вместе.

Магнитная часть ридера предназначена для работы с магнитными карточками, а микропроцессорная - с микропроцессорными или универсальными.

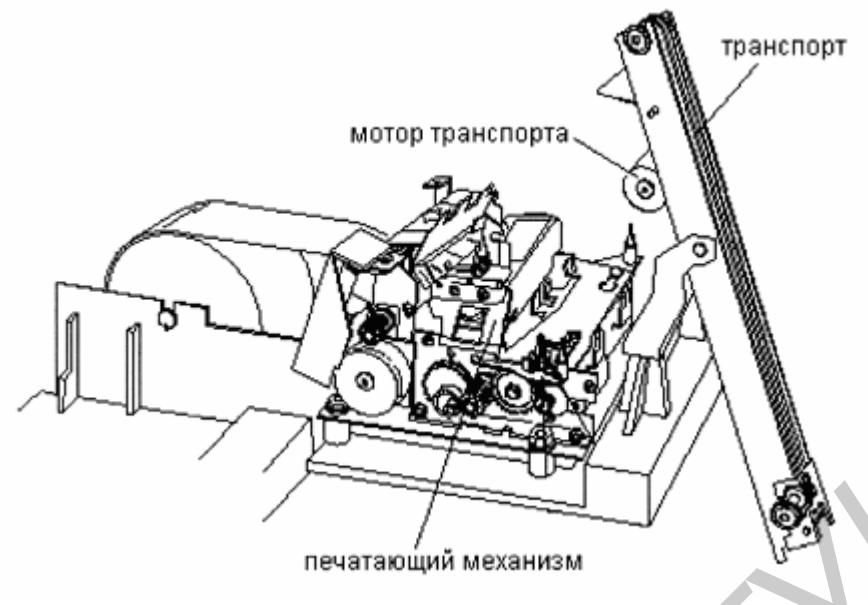
В данное время применяются три основных типа пластиковых карточек:

- магнитная;
- микропроцессорная;
- универсальная (на карточке присутствует как магнитная полоса, так и микропроцессор).

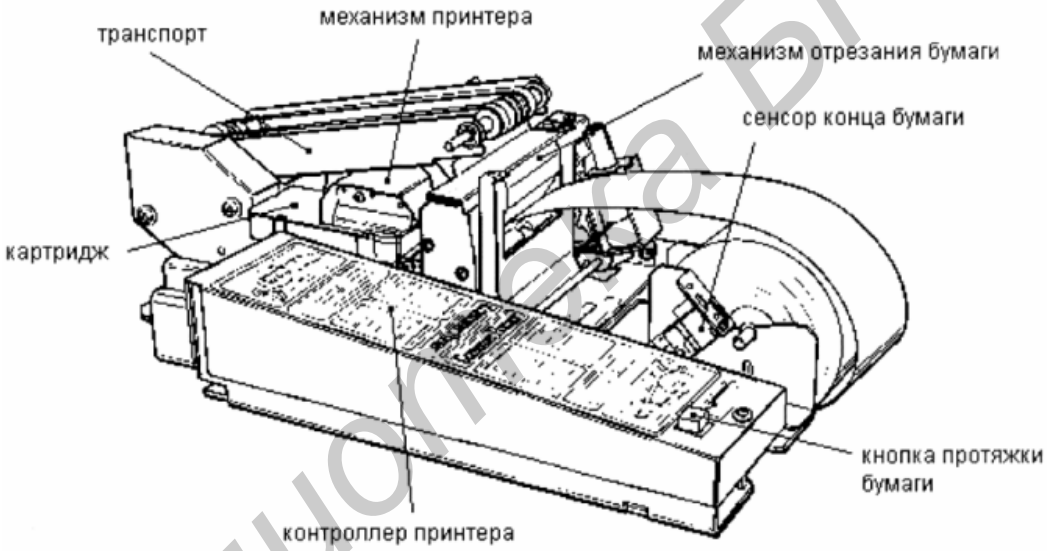
Существуют три основные группы карт-ридеров:

- моторизированные карт-ридеры;
- смарт-карт-ридер;
- универсальный карт-ридер.

Первая группа - моторизированные карт-ридеры, обладают возможностью считывать и записывать информацию только на магнитные карты. Устройства, относящиеся ко второй группе, могут работать как с магнитными карточками, так и с микропроцессорными. Универсальные карт-ридеры имеют две модификации, которые работают только с магнитными карточками, и две, которые могут работать с магнитными и микропроцессорными картами.



чековый принтер модели 245



чековый принтер модели 956

Рис. 3.3. Чековые принтеры 245 и 956 моделей

Каждая группа в своем составе имеет модели, которые могут только считывать информацию со второй дорожки, где находятся данные для доступа клиента к своему счету, другие могут считывать с первой, второй, третьей дорожки и записывать информацию на третью дорожку. Могут быть другие варианты.

Универсальные карт-ридеры семейства 101861 отличаются от остальных моделей тем, что имеют возможность преобразования из моторизированного ридера (модели A и B) в универсальный (модели C и D) и наоборот путем демонтажа или монтажа микропроцессорного модуля.

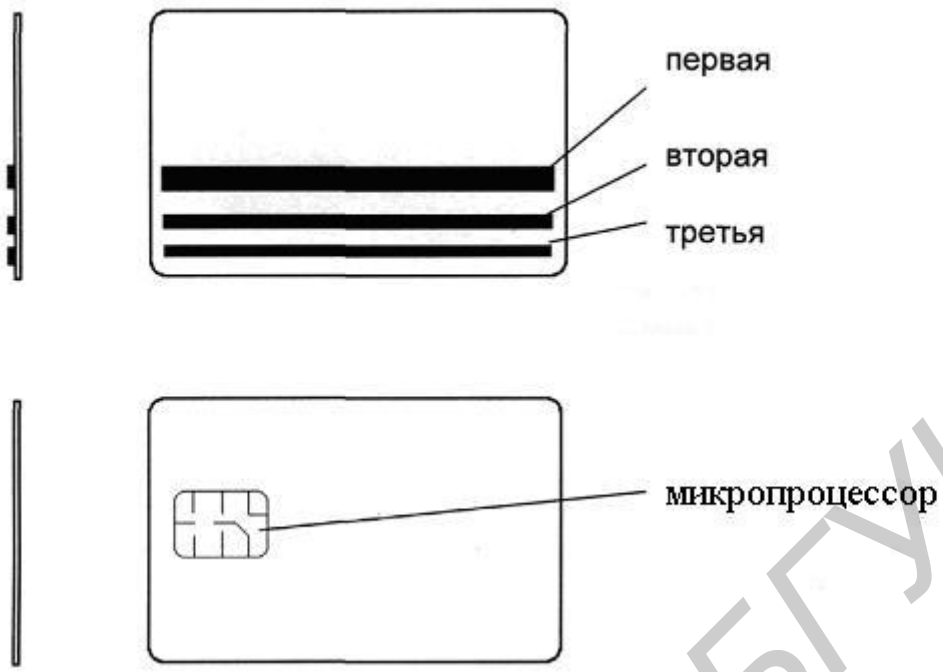


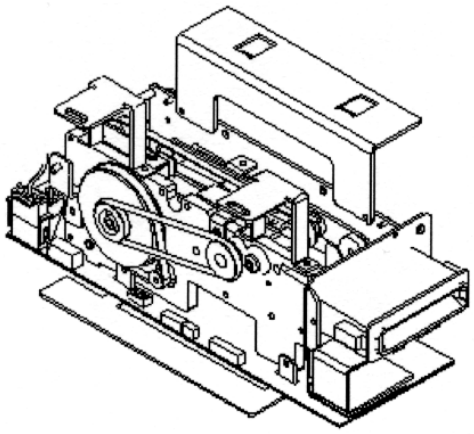
Рис. 3.4. Внешний вид пластиковых карточек

Карт-ридеры оснащаются специальными отсеками для задержанных карт. Они располагаются сзади карт-ридера на общей платформе. Карт-ридеры так же имеют возможность поддерживать работу дополнительного устройства для возврата пластиковой карты при внезапном пропадании питания банкомата. Устройство для возврата карты устанавливается опционально.

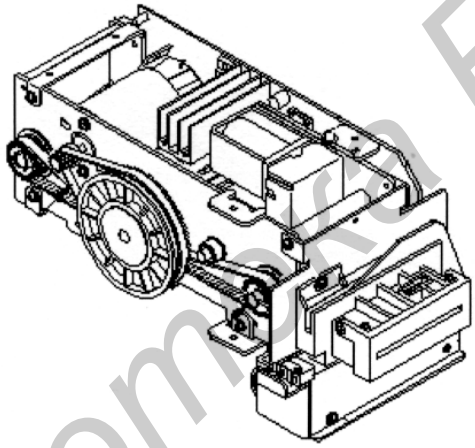
Принцип работы карт-ридера. После того как карта попала через входные ворота, она подхватывается транспортным механизмом и протягивается в положение считывания/записи к магнитной головке транспортом и несколько раз протягивается над магнитной головкой для того, чтобы магнитная головка могла прочитать данные с дорожек или записать на них информацию. После этого при нормальном завершении транзакции карта транспортом направляется в сторону входного модуля, открываются входные ворота и карта транспортом доставляется через щель клиенту.

Если используется микропроцессорная пластиковая карта, то транспорт протягивает карточку до конца транспортного пространства карт-ридера, где находится головка для работы с микропроцессором. После того как карта была доставлена транспортом и установлена в позицию, срабатывает соленоид, управляющий головкой для микропроцессора, и головка опускается своими контактами на контакты микропроцессора. Происходит чтение/запись карты. После этого карта так же возвращается клиенту. Позиции карты при чте-

нии/записи и ее движение по транспорту контролируется датчиками положения карты в транспорте.



а)



б)

Рис. 3.5. Карт-ридеры моделей: а-101050 и б-101861

Существует вероятность того, что во время проведения клиентом операции пропадет электропитание. При этом карта клиенту будет всегда возвращена. Для этого устанавливаются специальные возвратные емкости. При включении питания банкомата на них подается напряжение и имея определенную емкость они могут накапливать электрический заряд. После пропадания питания напряжение с контактов емкостей поступает на карт-ридер. Запускается транспорт карт-ридера, открываются выходные ворота и карта возвращается клиенту.

Клиентская клавиатура и монитор расположены на передней панели банкомата (рис 3.6).

Клиентская клавиатура может быть исполнена как с пластиковыми, так и с металлическими клавишами. Клавиши на клавиатуре могут различаться и по размеру. При приобретении банкомата необходимо учитывать данные особенности.

Клиентская клавиатура разделена на две части:

- функциональная клавиатура;
- пользовательская клавиатура.

Расположение пользовательской и функциональной клавиатур показано на рис. 11. Клавиатура состоит из трех основных частей:

- клавиши;
- платы клавиатуры;
- логического кабеля клавиатуры.

Функциональная клавиатура предназначена для выполнения стандартных операций, следуя указаниям на мониторе.

Существует несколько типов пользовательских клавиатур:

- 11-клавишная пользовательская клавиатура;
- 16-клавишная пользовательская клавиатура.
- 16-клавишная клавиатура отличается от 11-клавишной наличием дополнительных пользовательских клавиш, таких как CANCEL, CORECTION, CLEAR, ENTER.

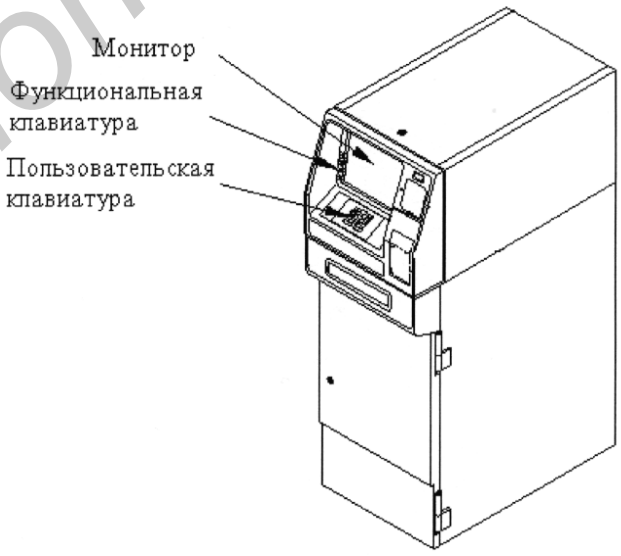


Рис. 3.6. Расположение клиентской клавиатуры и монитора

На банкоматах, выпускаемых фирмой Diebold устанавливаются мониторы с лучевыми трубками трех размеров 7', 9' и 15' дюймов по диагонали. Все они

поддерживают режим VGA 640x480 пикселов на дюйм, 16 цветов для цветных и 16 оттенков серого для черно-белых мониторов.

Девятидюймовые мониторы получили наибольшее распространение в связи с высокой надежностью и сравнительно невысокой стоимостью. Данные мониторы также оснащены фотодатчиком, определяющим интенсивность светового потока, что позволяет монитору автоматически, без вмешательства извне регулировать яркость экрана монитора. На рис. 3.7 показан монитор спереди и сзади.

На задней панели монитора расположены регуляторы для настройки видеоизображения на экране монитора. При их помощи можно отрегулировать:

- работу фотодатчика;
- яркость экрана;
- контрастность экрана;
- фокусировку экрана;
- вертикальную развертку экрана;
- горизонтальную развертку экрана.

При работе монитора, обращенного на солнечную сторону, ресурс электронно-лучевой трубки, а, следовательно, и самого монитора сокращается.

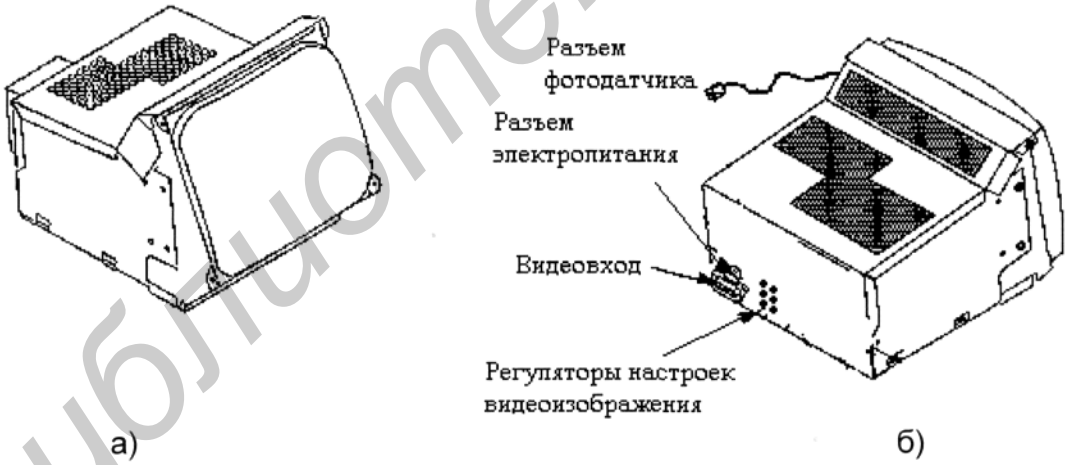


Рис. 3.7. 9-дюймовый монитор

15-дюймовый монитор - аналоговый цветной VGA-монитор. На рис. 3.8 показан внешний вид монитора и расположение основных регуляторов для настройки видеоизображения.

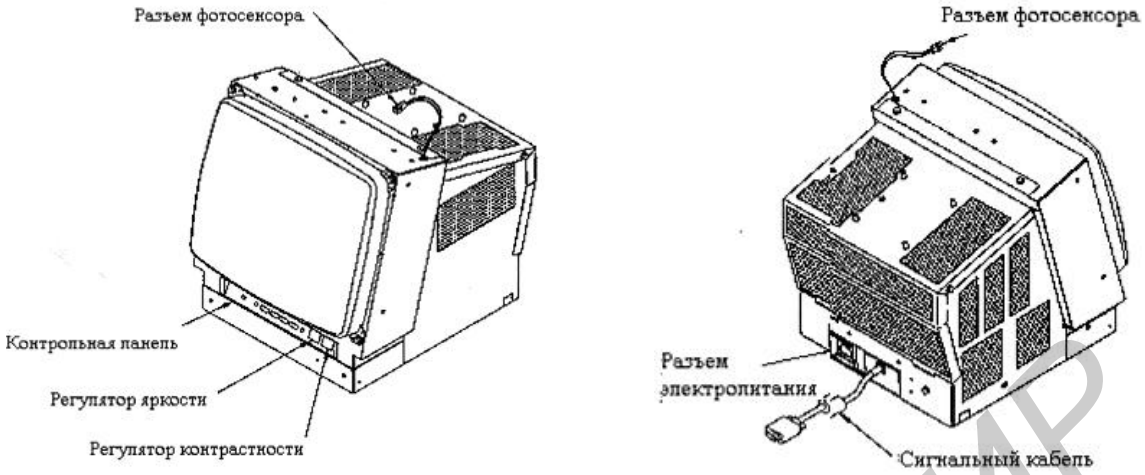


Рис. 3.8. 15-дюймовый монитор

Опция TOUCH SCREEN (сенсорный экран) предназначена только для 15-дюймового монитора. TOUCH SCREEN обеспечивает сенсорное управление выполнения операций. Сенсорный экран может работать в обычных условиях. Его защитное стеклянное покрытие защищает от преждевременного износа TOUCH SCREEN.

Благодаря своим свойствам TOUCH SCREEN может дублировать функциональную клавиатуру или вообще обойтись без нее. На работоспособность компонентов опции TOUCH SCREEN не влияют ни вибрации, ни высокая влажность.

Процессор терминала (CTP). CTP-модуль процессора, устанавливаемый на банкоматы серии i и ix, обладает достаточной мощностью обработки, расширенными функциональными возможностями и максимальной гибкостью. CTP-модуль включает в себя жесткий диск, один дисковод для гибких дискет и все требуемые разъемы и платы. CTP-модуль также поддерживает дополнительные слоты для плат. CTP работает с различными операционными системами типа OS/2, MS-DOS и Windows NT (рис. 3.9).

Компоненты CTP-модуля:

- CTP motherboard - системная плата;
- Riser card – плата расширений;
- ATM adapter card – ATM-адаптер;
- Secondary video card (optional) - дополнительная видеокарта;
- Hard drive - жесткий диск;
- Floppy drive-дисковод 3,5';
- Power adapter board - адаптер блока питания;

– Internal cabling - внутренние интерфейсные кабели.

СТР-системная плата. На банкоматах фирмы Diebold для СТР-модуля устанавливаются следующие системные платы:

– Pentium 166;
– Pentium 90;
– 486.

Для установки на банкоматы имеются системные платы Pentium 166 двух видов (рис. 3.10). Они выполняют одинаковые функции. Различия между ними следующие:

– наличие или отсутствие COM 2 (последовательного порта);
– наличие или отсутствие универсальной серийной шины (USB) и порта (USB);
– большинство системных плат Pentium 166 в комплектации имеет USB и порт USB на панели ввода - вывода и COM2, расположенные на системной плате или на панели ввода-вывода. В настоящее время USB шина в банкоматах фирмы Diebold не применяется.

Riser card имеет следующие особенности:

– Пять ISA-слотов (три полноразмерных, два половинного размера);
– Два PCI-слота.

Плата АТМ-адаптера. В настоящее время имеются три платы АТМ-адаптера, доступные для СТР, и используемые в зависимости от модификации системной платы СТР. Каждая из плат АТМ-адаптера имеет следующие особенности:

– энергозависимая SRAM;
– коммуникационный порт с возможностью подключения по протоколу X.25;
– порт АТМ-шины передачи данных;
– кнопка RESET и световые индикаторы текущего состояния.

Дисковод для гибких дискет. Стандартная СТР-конфигурация включает дисковод для 3,5' дисков.

Дополнительная видеоплата – PCI-плата видео. Она нужна для отображения видеоинформации на дополнительном мониторе. Наиболее часто используемые видеокарты производства компании “Matrox”.

Жесткий диск. Все СТР-системы имеют жесткий диск. В настоящее время используются жесткие диски емкостью от 850 MB и выше.

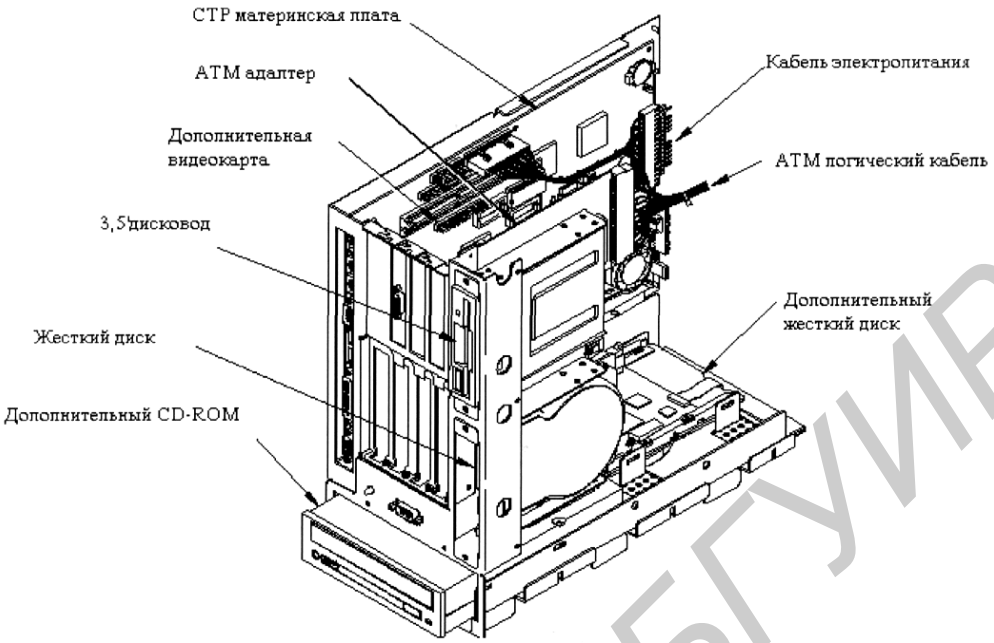


Рис. 3.9. Общий вид CTP-модуля

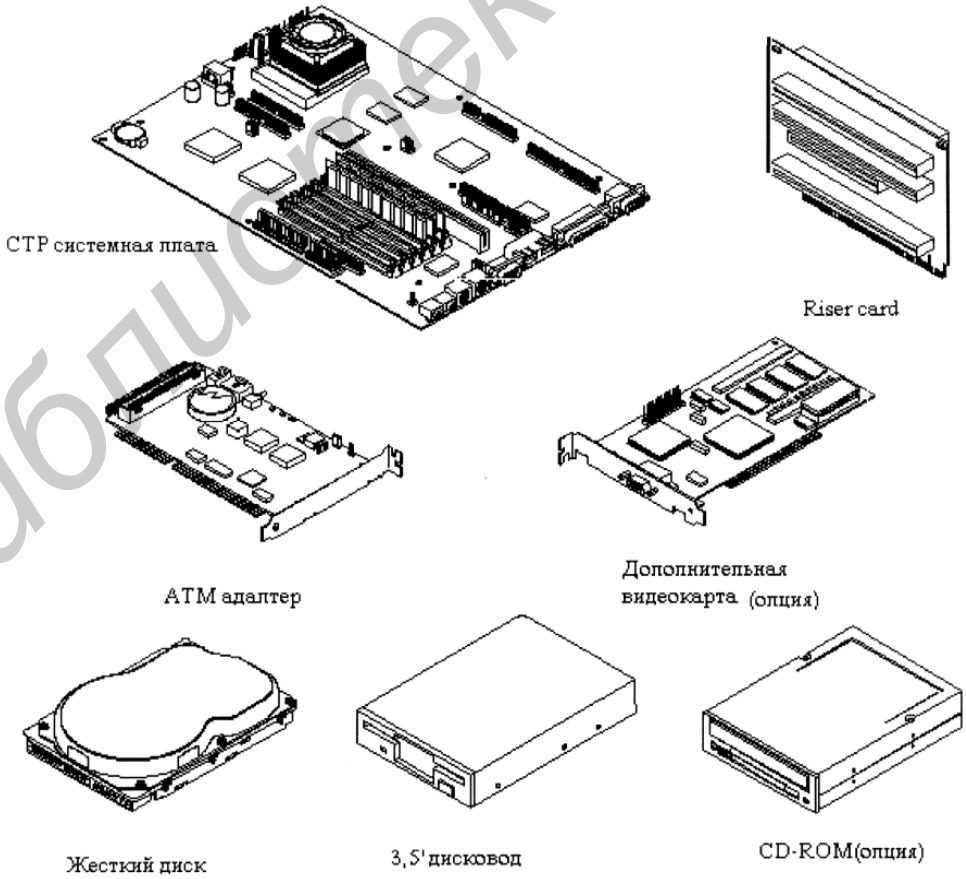


Рис. 3.10. Основные устройства, используемые в CTP

Устройство выдачи банкнот и кассеты. Устройство выдачи банкнот (multimedia dispenser) обеспечивает доставку купюр из кассет до окошка выдачи. При этом, как правило, обеспечиваются и дополнительные функции: отделение купюр друг от друга в момент их вытягивания из кассеты, транспортировка, сброс дефектных купюр в специальную кассету и, в некоторых моделях, втягивание невостребованных в течение определенного времени банкнот обратно в банкомат.

Существуют два принципиально различных типа устройств подачи купюр - вакуумные и фрикционные. Первые были созданы раньше, но некоторыми фирмами (NBS, De La Rue и др.) используются до сих пор. Фрикционные устройства, предложенные несколько лет назад фирмой Interinnovation, применяются в банкоматах фирм Bull, Olivetti, De La Rue. Аналогичные устройства впоследствии были разработаны и фирмой InterBold, которая постепенно заменила в своих банкоматах вакуумные устройства фрикционными.

Фрикционная работает быстрее и лучше подает мятые купюры, нечувствительна к атмосферным условиям, но зато не справляется с надорванными (длина надрыва более 2-2,5 см) купюрами. В пользу фрикционной технологии говорит и тот факт, что ни одна из фирм - изготовителей банкоматов, перешедших на фрикционную систему, не вернулась к более старой и проверенной вакуумной. Впрочем, это может быть следствием не технических, а маркетинговых и финансовых причин. В целом, мы не готовы дать однозначные рекомендации по этому вопросу, тем более что фирма De La Rue, владеющая патентными правами на обе технологии, выпускает параллельно устройства обоих типов.

Кассеты у разных изготовителей также могут быть разными. Их вместимость колеблется от примерно 2000 купюр в кассетах De La Rue до 3000 в кассетах ряда других фирм. Число кассет в разных моделях также различно, стандартные варианты - 1, 2 и 4. При эксплуатации необходимо также помнить о запасных кассетах, которые обязательно надо использовать для исключения лишних простоев. Ряд моделей может быть дополнительно оснащен устройством выдачи монет нескольких номиналов.

Депозитарий. Полнофункциональные банкоматы DieBold (IBM) могут комплектоваться депозитариями двух типов. Стандартный депозитарий предназначен для приема порядка 500 конвертов с документами, купюрами, монетами и другими ценностями. Хранилище принятых конвертов может находиться в специальном сейфе. Специальный принтер депозитария может печатать на не-

ровных поверхностях конверта и нечувствителен к изменениям толщины заполненного конверта. На конверте в автоматизированном режиме печатается информация о счете и выполненных операциях, используемая впоследствии для финансовых проверок.

Помимо описанного депозитария, которым оснащаются и банкоматы других фирм, например фирмы NBS, могут использоваться и так называемые интеллектуальные депозитарии. Помимо перечисленных выше стандартных функций, такое устройство способно сканировать (причем, с обеих сторон) помещаемые на хранение документы, хранить и/или передавать их изображения, распознавать рамки для вписывания денежных сумм, считывать коды, написанные магнитными чернилами, сортировать документы в три программируемых отсека с общей емкостью 650 единиц или в карман для конвертов и печатать с обеих сторон документа информацию объемом до 80 символов.

Средства обеспечения безопасности. Банкоматы обеспечивают многоуровневую защиту операций - механическую, оптическую, электрическую, программную - вплоть до установки системы сигнализации с видеокамерой.

Системные ключи шифрования можно хранить программным способом, однако, это не слишком безопасный метод. Как правило, для этой цели используется специальная аппаратная защита - так называемый "черный ящик".

Кассеты с банкнотами хранятся в сейфах различных конструкций, например, UL291, RAL-RG 626/3, C1/C2. Они различаются габаритами, толщиной стенок, весом. Запираются сейфы с помощью различных замков: с ключами, с одинарным или двойным цифровым набором, с электронным ключом. Бессейфовые модели и конфигурации банкоматов можно устанавливать только в операционных залах и необходимо инкассировать в конце каждого рабочего дня.

Для предотвращения взлома банкомата применяются датчики различного назначения, соединенные с системой сигнализации: тепловые (для выявления попытки плазменной резки металла), сейсмические (для выявления попытки увоза банкомата) и др.

Возможна установка видеокамеры с видеомагнитофоном, которые фиксируют все действия пользователей при работе с банкоматом. Наконец, для защиты от вандализма могут применяться специальные кабины, поставляемые, например, фирмой DIEBOLD. Такая кабина, в которой устанавливаются один или несколько банкоматов, запирается с помощью электронных замков, пропускающих в нее только владельцев карточек, и защищается системой сигнализации.

3.1.4. Программное обеспечение

Рассмотрим программное обеспечение для банкоматов класса BTP фирмы IBM. Нижний уровень этого программного обеспечения составляет программа Terminal Control Software (TCS), управляющая аппаратными модулями банкомата: устройством чтения/записи, клавиатурой, дисплеем, устройством подачи купюр, принтерами. Эта программа фактически реализует автомат конечных состояний, характеризуемый списком экранных форм, правилами проверки личного номера и т.д. Определение многочисленных параметров аппаратных модулей, а также настройку самой программы TCS осуществляет входящий в нее модуль Maintenance Manager. За обмен информацией (прием и передачу) отвечает пакет Communication Subsys (CSS), использующий специальные протоколы TABS 911 и TABS 912. Для непосредственного обмена информацией между банкоматом и главным компьютером может использоваться практически любой из широко применяемых протоколов, например, PSTN, X.25, Serial Line, LAN или TCP/IP. Выбор протокола осуществляется путем настройки и программному обеспечению банкомата фактически безразлично, с каким из двух протоколов работать.

Программой TCS управляют программы более высокого уровня, выдающие команды переключения из одного состояния в другое, передачи параметров состояний (например, суммы выданной наличности) и др. Здесь возможны два подхода: либо использование поставляемого вместе с банкоматом фирменного пакета Pace, либо непосредственное обслуживание банкомата программными комплексами центрального компьютера (поставляют эти комплексы системные интеграторы и разработчики программного обеспечения для платежных систем). Чтобы понять место этих программных элементов в системе, рассмотрим три топологические схемы ее построения:

- центральный компьютер непосредственно связан с произвольным числом банкоматов, работающих в режиме реального времени;
- центральный компьютер связан с узлом-контроллером, к которому подключено до 32 банкоматов, работающих в режиме реального времени;
- узел-контроллер связан с банкоматами (числом до 32), работающими в автономном режиме.

Прикладное программное обеспечение располагается на центральном компьютере, а пакет Pace - на узле-контроллере, функции которого может исполнять как отдельный компьютер, так и процессор самого банкомата. Основ-

ная функция пакета Pace - управление программой TCS. В случае трехзвенной схемы (главный компьютер - пакет Pace в узле-контроллере - программа TCS в банкомате), работающей в режиме реального времени, пакет Pace взаимодействует как с программой TCS, так и с прикладным программным обеспечением главного компьютера. Обмен данными между узлом-контроллером (банкоматом) и главным компьютером осуществляется по протоколу D1000 фирмы DieBold, практически ставшему общепризнанным мировым стандартом для фирм - изготовителей банкоматов.

Помимо программы TCS, управляющей работой аппаратуры и обменом информацией, и пакета Pace, который управляет работой этой программы, в поставляемое программное обеспечение могут входить средства самостоятельной разработки системы, состоящие из трех независимых пакетов:

COM SUBSYS SDK - позволяющего разрабатывать прикладные программы, в которых для обмена данными используется пакет CSS;

DESIGN UTILITY - средства разработки шрифтов и графических объектов (иконок) для использования в экранных формах;

PC BASED SOFTWARE TOOLS - средства разработки прикладных программ в рамках пакета Pace (создания файлов состояний, описания экранных форм, проверки личного номера владельца карточки).

3.2. Лабораторное задание

1. Последовательно изучить функции и классификацию банкоматов по тексту методических указаний.
2. Изучить состав и назначение аппаратного обеспечения банкомата, конструкции его отдельных узлов.
3. Изучить состав и назначение программного обеспечения банкомата.
4. Ответить на контрольные вопросы.
5. Оформить отчет.

3.3. Содержание отчета

1. Цель работы.
2. Ответы на контрольные вопросы.
3. Вывод.

3.4. Контрольные вопросы

1. По каким критериям классифицируются банкоматы?
2. Какие преимущества имеет модульный принцип построения банкоматов с открытой архитектурой?
3. Назначение журнального принтера?
4. Что называется чековым принтером?
5. На какие группы делятся карт-ридеры?
6. Чем отличается пользовательская клавиатура от функциональной?
7. Какие разновидности мониторов банкоматов вы знаете?
8. Каково назначение процессора терминала?
9. Состав CTP модуля?
10. Какие средства обеспечения безопасности имеются в банкомате?
11. Каков состав программного обеспечения банкомата?

4. ЗАЩИТА ИНФОРМАЦИИ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

Цель работы: Изучить принципы функционирования электронных платежных систем и методы защиты информации в них. Провести тестирование ПИС «PAY» в режимах: клиента Интернет-магазина «E-LUX»; менеджера Интернет-магазина «E-LUX»; клиента банка-эмитента «Белкредит-Банк», физическое лицо; клиента банка-эквайера «БелТорг-Банк».

4.1. Краткие теоретические сведения

4.1.1. Общие принципы организации и виды платежных Интернет-систем

Платежная Интернет-система – это система проведения расчетов между финансовыми, бизнес-организациями и Интернет-пользователями в процессе покупки/продажи товаров и услуг через Интернет. Именно платежная система позволяет превратить службу по обработке заказов или электронную витрину в полноценный магазин со всеми стандартными атрибутами: выбрав товар или услугу на сайте продавца, покупатель может осуществить платеж, не отходя от компьютера.

В системе электронной коммерции платежи совершаются при соблюдении ряда условий:

1. Соблюдение конфиденциальности. При проведении платежей через Интернет покупатель хочет, чтобы его данные (например, номер кредитной карты) были известны только организациям, имеющим на это законное право.

2. Сохранение целостности информации. Информация о покупке никем не может быть изменена.

3. Аутентификация. Покупатели и продавцы должны быть уверены, что все стороны, участвующие в сделке, являются теми, за кого они себя выдают.

4. Средства оплаты. Возможность оплаты любыми доступными покупателю платежными средствами.

5. Авторизация. Процесс, в ходе которого требование на проведение транзакции одобряется или отклоняется платежной системой. Эта процедура позволяет определить наличие средств у покупателя.

6. Гарантии рисков продавца. Осуществляя торговлю в Интернет, продавец подвержен множеству рисков, связанных с отказами от товара и недобросовестностью покупателя. Величина рисков должна быть согласована с провайде-

ром платежной системы и другими организациями, включенными в торговые цепочки, посредством специальных соглашений.

7. Минимизация платы за транзакцию. Плата за обработку транзакций заказа и оплаты товаров, естественно, входит в их стоимость, поэтому снижение цены транзакции увеличивает конкурентоспособность. Важно отметить, что транзакция должна быть оплачена в любом случае, даже при отказе покупателя от товара.

Все указанные условия должны быть реализованы в платежной Интернет-системе, которая в сущности представляют собой электронные версии традиционных платежных систем.

Таким образом, все платежные системы делятся на:

- дебетовые (работающие с электронными чеками и цифровой наличностью);
- кредитные (работающие с кредитными карточками).

4.1.2. Дебетовые системы

Дебетовые схемы платежей построены аналогично их офф-лайновым прототипам: чековым и обычным денежным. В схему вовлечены две независимые стороны: эмитенты и пользователи. Под эмитентом понимается субъект, управляющий платежной системой. Он выпускает некие электронные единицы, представляющие платежи (например, деньги на счетах в банках). Пользователи систем выполняют две главные функции. Они производят и принимают платежи в Интернет, используя выпущенные электронные единицы.

Электронные чеки являются аналогом обычных бумажных чеков. Это предписания плательщика своему банку перечислить деньги со своего счета на счет получателя платежа. Операция происходит при предъявлении получателем чека в банке. Основных отличий здесь два. Во-первых, выписывая бумажный чек, плательщик ставит свою настоящую подпись, а в онлайновом варианте - подпись электронная. Во-вторых, сами чеки выдаются в электронном виде.

Проведение платежей проходит в несколько этапов:

1. Плательщик выписывает электронный чек, подписывает электронной подписью и пересылает его получателю. В целях обеспечения большей надежности и безопасности номер чекового счета можно закодировать открытым ключом банка.

2. Чек предъявляется к оплате платежной системе. Далее (либо здесь, либо в банке, обслуживающем получателя) происходит проверка электронной подписи.

3. В случае подтверждения ее подлинности поставляется товар или оказывается услуга. Со счета плательщика деньги перечисляются на счет получателя.

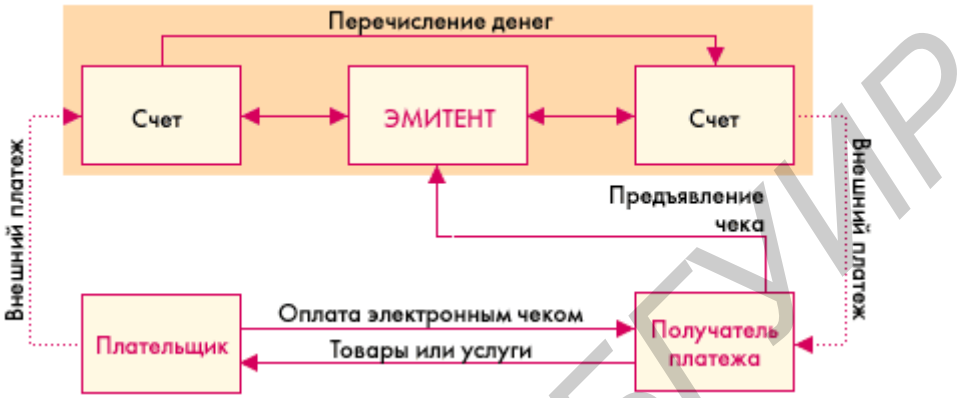


Рис. 4.1. Схема проведения платежей при помощи электронных чеков

Простота схемы проведения платежей (рис. 4.1), к сожалению, компенсируется сложностями ее внедрения из-за того, что чековые схемы пока не получили распространения и не имеется сертификационных центров для реализации электронной подписи.

В электронной цифровой подписи (ЭЦП) используют систему шифрования с открытым ключом. При этом создается личный ключ для подписи и открытый ключ для проверки. Личный ключ хранится у пользователя, а открытый может быть доступен всем. Самый удобный способ распространения открытых ключей - использование сертификационных центров. Там хранятся цифровые сертификаты, содержащие открытый ключ и информацию о владельце. Это освобождает пользователя от обязанности самому рассылать свой открытый ключ. Кроме того, сертификационные центры обеспечивают аутентификацию, гарантирующую, что никто не сможет сгенерировать ключи от другого лица.

Электронные деньги полностью моделируют реальные деньги. При этом эмиссионная организация - эмитент - выпускает их электронные аналоги, называемые в разных системах по-разному (например купоны). Далее, они покупаются пользователями, которые с их помощью оплачивают покупки, а затем продавец погашает их у эмитента. При эмиссии каждая денежная единица заверяется электронной печатью, которая проверяется выпускающей структурой перед погашением.

Одна из особенностей физических денег - их анонимность, то есть на них не указано, кто и когда их использовал. Некоторые системы, по аналогии, позволяют покупателю получать электронную наличность так, чтобы нельзя было определить связь между ним и деньгами. Это осуществляется с помощью схемы слепых подписей.

Стоит еще отметить, что при использовании электронных денег отпадает необходимость в аутентификации, поскольку система основана на выпуске денег в обращение перед их использованием.

На рис. 4.2 приведена схема платежа с помощью цифровых денег.

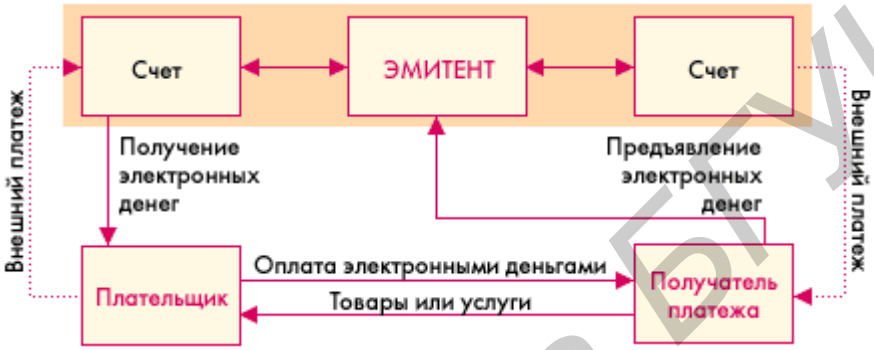


Рис. 4.2. Схема платежа с помощью цифровых денег

Механизм осуществления платежа следующий:

1. Покупатель заранее обменивает реальные деньги на электронные. Хранение наличности у клиента может осуществляться двумя способами, что определяется используемой системой:

– на жестком диске компьютера.
– на смарт-картах.

Разные системы предлагают разные схемы обмена. Некоторые открывают специальные счета, на которые перечисляются средства со счета покупателя в обмен на электронные купюры. Некоторые банки могут сами эмитировать электронную наличность. При этом она эмитируется только по запросу клиента с последующим перечислением на компьютер или карту этого клиента и снятием денежного эквивалента с его счета. При реализации же слепой подписи покупатель сам создает электронные купюры, пересылает их в банк, где при поступлении реальных денег на счет они заверяются печатью и отправляются обратно клиенту.

Наряду с удобствами такого хранения, у него имеются и недостатки. Порча диска или смарт-карты оборачивается невозвратимой потерей электронных денег.

2. Покупатель перечисляет на сервер продавца электронные деньги за покупку.

3. Деньги предъявляются эмитенту, который проверяет их подлинность.

4. В случае подлинности электронных купюр счет продавца увеличивается на сумму покупки, а покупателю отгружается товар или оказывается услуга.

Одной из важных отличительных черт электронных денег является возможность осуществлять микроплатежи. Это связано с тем, что номинал купюр может не соответствовать реальным монетам (например 37 копеек).

Эмитировать электронные наличные могут как банки, так и небанковские организации. Однако до сих пор не выработана единая система конвертирования разных видов электронных денег. Поэтому только сами эмитенты могут гасить выпущенную ими электронную наличность. Кроме того, использование подобных денег от нефинансовых структур не обеспечено гарантиями со стороны государства. Однако малая стоимость транзакции делает электронную наличность привлекательным инструментом платежей в Интернет.

4.1.3. Кредитные системы

Интернет-кредитные системы являются аналогами обычных систем, работающих с кредитными картами. Отличие состоит в проведении всех транзакций через Интернет, и как следствие, в необходимости дополнительных средств безопасности и аутентификации.

В проведении платежей через Интернет с помощью кредитных карт участвуют:

1. **Покупатель.** Клиент, имеющий компьютер с Web-браузером и доступом в Интернет.

2. **Банк-эмитент.** Здесь находится расчетный счет покупателя. Банк-эмитент выпускает карточки и является гарантом выполнения финансовых обязательств клиента.

3. **Продавцы.** Под продавцами понимаются серверы электронной коммерции, на которых ведутся каталоги товаров и услуг и принимаются заказы клиентов на покупку.

4. **Банки-эквайеры.** Банки, обслуживающие продавцов. Каждый продавец имеет единственный банк, в котором он держит свой расчетный счет.

5. **Платежная система Интернет.** Электронные компоненты, являющиеся посредниками между остальными участниками.

6. **Традиционная платежная система.** Комплекс финансовых и технологических средств для обслуживания карт данного типа. Среди основных задач, решаемых платежной системой, - обеспечение использования карт как средства платежа за товары и услуги, пользование банковскими услугами, проведение взаимозачетов и т.д. Участниками платежной системы являются физические и юридические лица, объединенные отношениями по использованию кредитных карт.

7. **Процессинговый центр платежной системы.** Организация, обеспечивающая информационное и технологическое взаимодействие между участниками традиционной платежной системы.

8. **Расчетный банк платежной системы.** Кредитная организация, осуществляющая взаиморасчеты между участниками платежной системы по поручению процессингового центра.

Общая схема платежей в такой системе приведена на рис. 4.3.

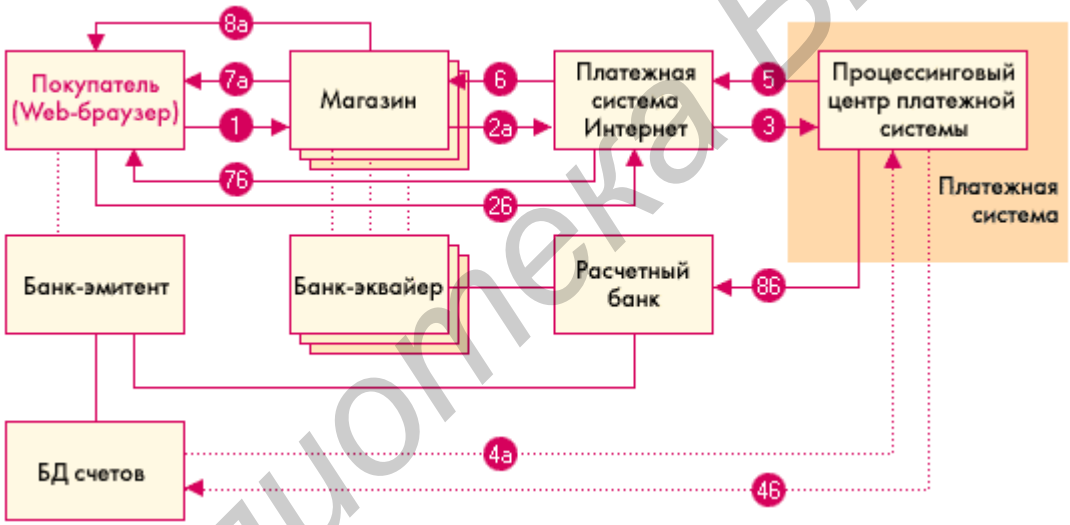


Рис. 4.3. Общая схема платежей в кредитной Интернет-системе

1. Покупатель в электронном магазине формирует корзину товаров и выбирает способ оплаты "кредитная карта".

2. Параметры кредитной карты (номер, имя владельца, дата окончания действия) должны быть переданы платежной системе Интернет для дальнейшей авторизации. Это может быть сделано двумя способами:

а) через магазин, то есть параметры карты вводятся непосредственно на сайте магазина, после чего они передаются платежной системе Интернет;

б) на сервере платежной системы.

Очевидны преимущества второго пути. В этом случае сведения о картах не остаются в магазине и, соответственно, снижается риск получения их третьими лицами или обмана продавцом. И в том, и в другом случае при передаче реквизитов кредитной карты все же существует возможность их перехвата злоумышленниками в сети. Для предотвращения этого данные при передаче шифруются.

Шифрование, естественно, снижает возможности перехвата данных в сети, поэтому связи покупатель/продавец, продавец/платежная система Интернет, покупатель/платежная система Интернет желательно осуществлять с помощью защищенных протоколов. Наиболее распространенными из них на сегодняшний день являются протокол SSL (Secure Sockets Layer), а также стандарт защищенных электронных транзакций SET (Secure Electronic Transaction), призванный со временем заменить SSL при обработке транзакций, связанных с расчетами за покупки по кредитным картам в Интернет.

3. Платежная система Интернет передает запрос на авторизацию традиционной платежной системе.

4. Последующий шаг зависит от того, ведет ли банк-эмитент он-лайновую базу данных (БД) счетов. При наличии БД процессинговый центр а) передает банку-эмитенту запрос на авторизацию карты и затем, б) получает ее результат. Если же такой базы нет, то процессинговый центр сам хранит сведения о состоянии счетов держателей карт, стоп-листы и выполняет запросы на авторизацию. Эти сведения регулярно обновляются банками-эмитентами.

5. Результат авторизации передается платежной системе Интернет.

6. Магазин получает результат авторизации.

7. Покупатель получает результат авторизации а) через магазин или б) непосредственно от платежной системы Интернет.

8. При положительном результате авторизации:

а) - магазин оказывает услугу, или отгружает товар;

б) - процессинговый центр передает в расчетный банк сведения о совершенной транзакции. Деньги со счета покупателя в банке-эмитенте перечисляются через расчетный банк на счет магазина в банке-эквайере.

Для проведения подобных платежей в большинстве случаев необходимо специальное программное обеспечение (называемое электронным кошельком). Оно может поставляться покупателю, продавцу и обслуживающему его банку.

4.2. Лабораторное задание

1. Включить персональный компьютер.

2. Запустить файл index.html на выполнение. Данная программа имитирует платежную Интернет-систему (ПИС) «PAY», в которой можно выступать в ролях (рис. 4.4):

– клиента Интернет-магазина «E-LUX»;
– менеджера Интернет-магазина «E-LUX»;
– клиента банка-эмитента «Белкредит-Банк», физическое лицо;
– клиента банка-эквайера «БелТорг-Банк», юридическое лицо.

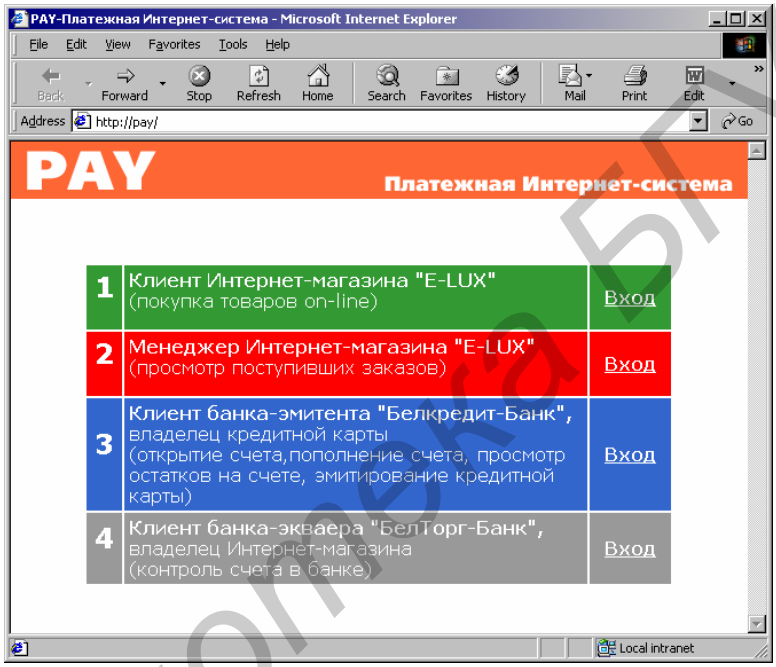


Рис. 4.4. Внешний вид главной страницы программы

3. **Режим «Клиент банка-эмитента».** В данном режиме можно выполнить следующие операции:

– открыть счет;
– пополнить счет;
– просмотреть баланс счета;
– эмитировать кредитную карту.

4. Для открытия счета в банке выбрать пункт меню «Открыть счет». После чего ввести имя, фамилию и адрес владельца счета, а также количество средств, зачисляемых на счет в долларах США (рис.4.5). Необходимо отметить, что «Имя» (Name) и «Фамилия» (Last Name) вводятся латинскими буквами, поскольку платежные карточки систем VISA, MasterCard, American Express являются международными.

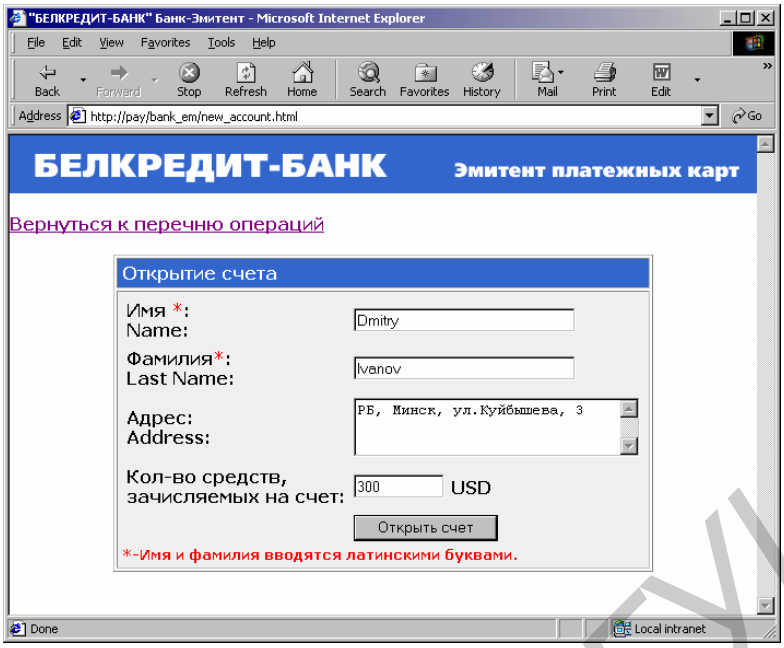


Рис. 4.5. Данные для открытия счета в банке-эмитенте

5. После заполнения формы нажать кнопку «Открыть счет». После чего будет выдан номер счета, а также имя, фамилия и адрес владельца счета.

6. Процедура эмитирования кредитной карты выполняется путем выбора пункта меню «Эмитирование кредитной карты», находящегося на главной странице программы.

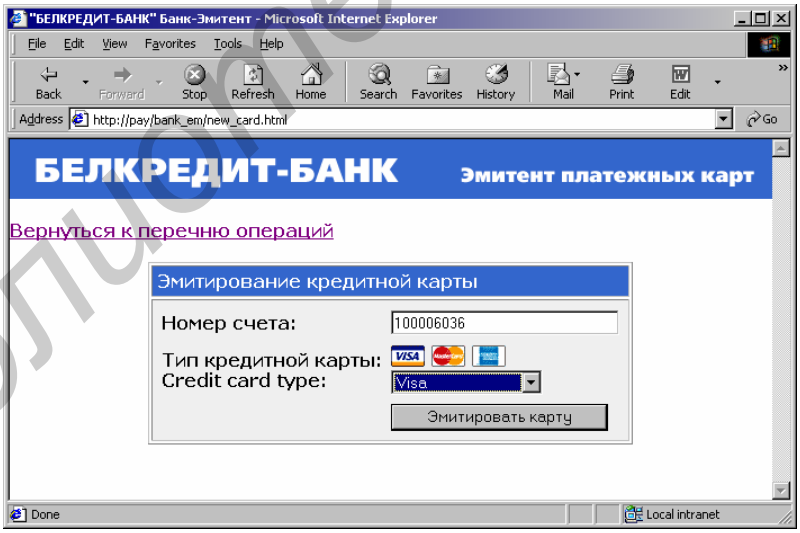


Рис. 4.6. Ввод данных для эмитирования кредитной карты

7. В появившемся окне необходимо ввести номер счета, а также выбрать тип кредитной карты (VISA, MasterCard, American Express) (рис. 4.6).

8. После заполнения формы нажать кнопку «Эмитировать карту». Следующее окно будет содержать параметры эмитированной кредитной карты:

– тип кредитной карты (VISA, MasterCard, American Express);

– номер карты (16 цифр);
– срок действия карты (2 года);
– имя держателя карты;
– фамилия держателя карты.

9. Счет пополняется путем выбора в перечне операций банка пункта «Пополнение счета», после чего необходимо ввести номер счета и количество средств, зачисляемых на счет.

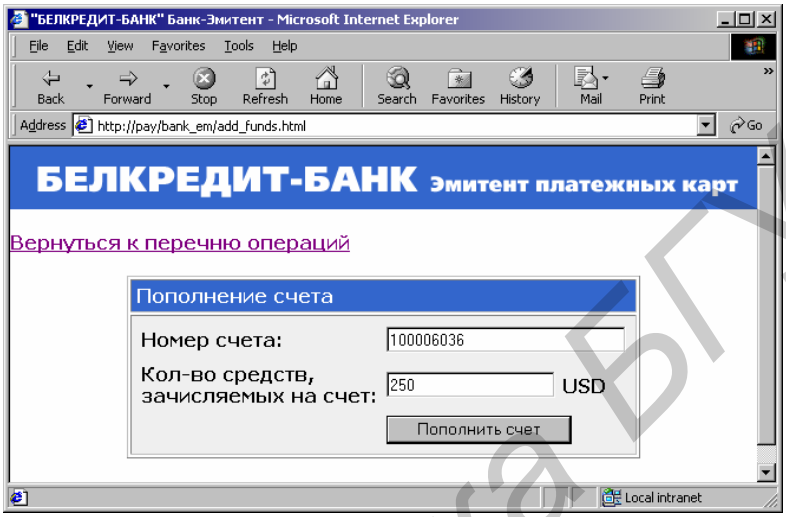


Рис. 4.7. Ввод параметров для пополнения счета

10. Подтверждение данной операции проводится путем нажатия кнопки «Пополнить счет», после чего появляется окно, содержащее номер счета, сумму, зачисленную на счет, и баланс счета.

11. Для просмотра баланса счета необходимо воспользоваться соответствующим пунктом меню операций банка и ввести номер счета.

12. После нажатия кнопки «Просмотреть» выдается баланс счета.

13. **Режим «Клиент Интернет-магазина».** На главной странице программы выбрать режим работы «Клиент Интернет-магазина». После выполнения данного действия открывается страница Интернет-магазина «E-LUX», на которой можно ознакомиться с перечнем товаров, выбрать необходимый товар и оформить его заказ.

14. Выбор заинтересовавшего товара осуществляется нажатием кнопки «Купить», относящейся к выбранному товару (рис. 4.8).

15. Способы оплаты заказа следующие:
– оплата наличными курьеру при получении заказа;
– оплата по кредитной карте.

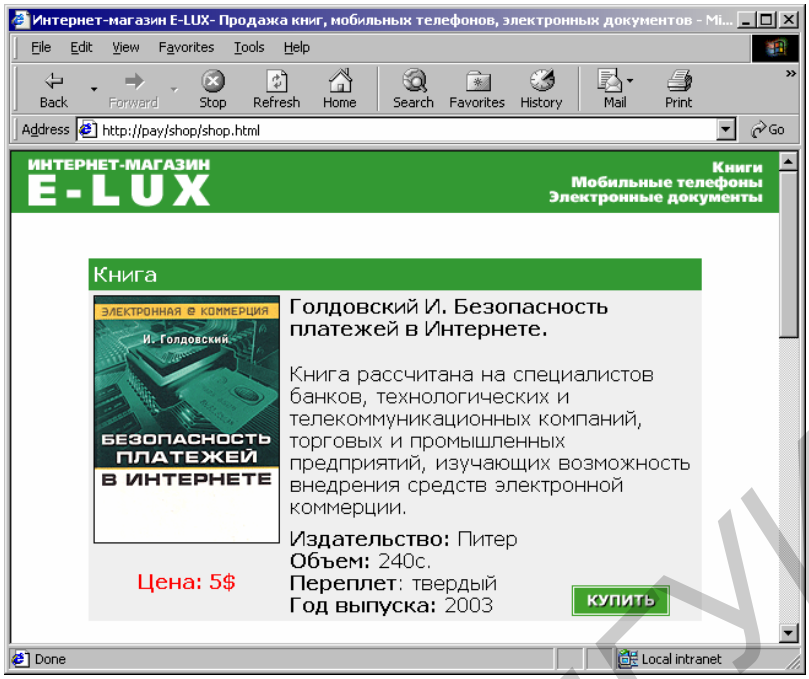


Рис. 4.8. Главная страница Интернет-магазина «E-LUX»

16. При выборе первого способа необходимо ввести свои имя и фамилию, номер телефона, адрес доставки товара и подтвердить заказ нажатием кнопки «Заказать» (рис. 4.9). Подтверждение принятия заказа сопровождается соответствующим уведомлением.

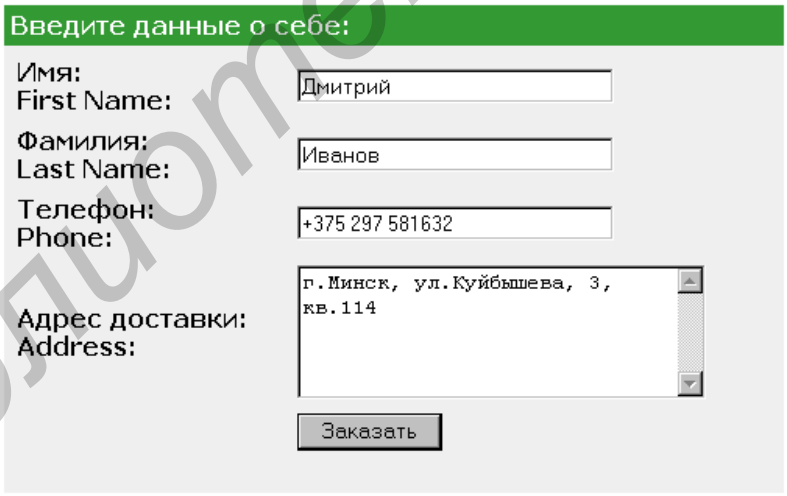


Рис. 4.9. Ввод данных для доставки заказа курьером

17. При выборе способа оплаты по кредитной карте пользователь переадресовывается на авторизационный сервер ПИС «PAY» (рис. 4.10). Все информационное взаимодействие между Интернет-магазином и ПИС “PAY” происходит по защищенному протоколу SSL и заверяется ЭЦП сторон.

18. ПИС «PAY» устанавливает с Покупателем соединение по защищенному протоколу (SSL) и просит ввести параметры кредитной карты, которые

будут переданы в защищенном виде только в ПИС «PAY» и не будут предоставлены Интернет-магазину в целях безопасности реквизитов платежной карты.

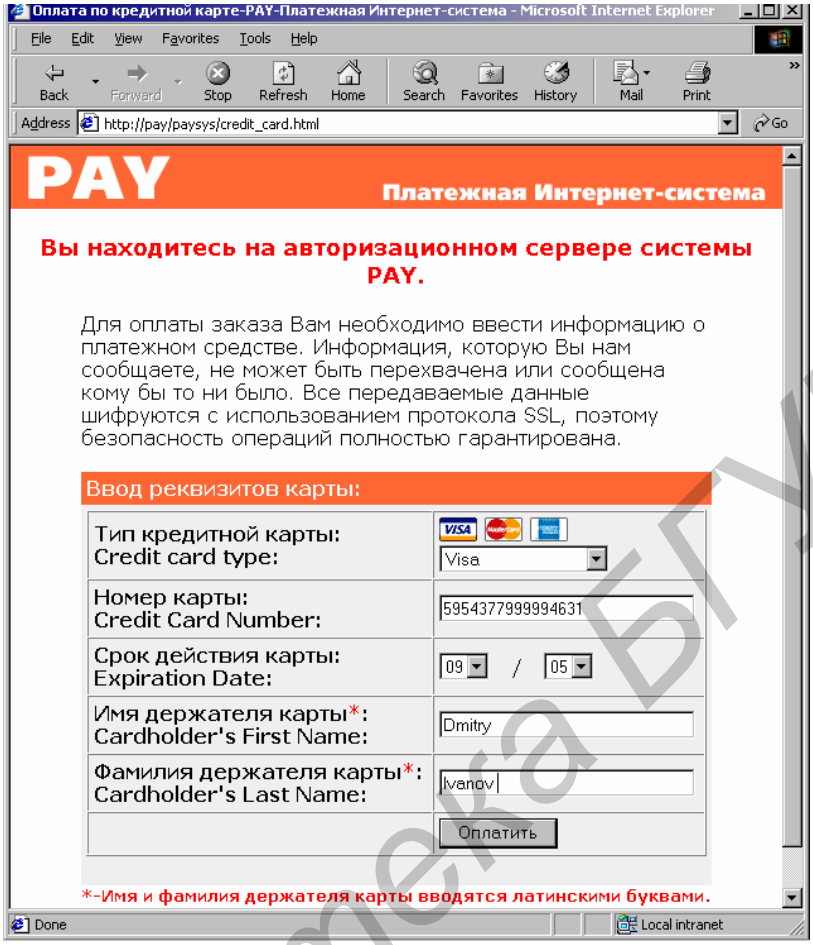


Рис. 4.10. Страница авторизационного сервера ПИС «PAY»

19. Ввод реквизитов платежной карты подтвердить нажатием кнопки «Оплатить». Запрос на авторизацию передается через закрытые банковские сети процессинговому центру карточной платежной системы, а затем банку-эмитенту карточки.

20. В случае положительного результата авторизации, полученного от процессингового центра карточной платежной системы:

– ПИС «PAY» передает Интернет-магазину положительный результат авторизации с номером заказа;
– ПИС «PAY» блокирует средства, необходимые для оплаты заказа, в банк-эмитенте покупателя.

21. В случае отказа в авторизации:

ПИС «PAY» передает отказ с описанием причины. Причины получения отказа:

– введены неверные параметры кредитной карты;

– на карточке недостаточно средств для оплаты заказа.

В случае отказа необходимо либо пополнить счет в банке-эмитенте, либо повторить ввод параметров кредитной карты.

22. При положительном результате авторизации Интернет-магазин выдает «электронный чек» на отпускаемый товар, который является доказательством проведения оплаты за какой-либо заказ и может быть использован обеими сторонами (магазином и покупателем) при возникновении спорных ситуаций (рис. 4.11).

Электронный чек	
Название торговой точки	Интернет-магазин E-Lux
URL электронного магазина	www.elux.com
Контактные координаты	info@elux.com
Сумма операции в валюте транзакции	5$
Дата заказа	03.03.2003 15:45:10
Номер заказа	00215
Покупатель	Dmitry Ivanov
Описание услуг	Книга "Голдовский И. Безопасность платежей в Интернет"

Рис. 4.11. Внешний вид «электронного чека»

23. **Режим «Менеджер “Интернет-магазина».** В данном режиме отслеживается поступление заказов, оформляются доставки заказов, принимаются решения о перечислении заблокированных средств со счета покупателя на счет Интернет-магазина.

24. Просмотр содержимого заказа осуществляется путем выбора номера заказа из соответствующего перечня. При этом для удобства менеджера все заказы имеют поле «Отметка о выполнении», которое может иметь значение «Выполнен» или «Не выполнен» (рис. 4.12).

25. Менеджер просматривает содержимое заказа, оформляет доставку заказа клиенту (доставка осуществляется собственной службой доставки, службой экспресс-доставки, почтовым отправлением). При успешной доставке заказа клиенту оформляется документ, подтверждающий получение заказа клиентом (документ, подписанный клиентом - слип/ карточка службы экспресс-доставки/ почтовое извещение), на основании которого менеджер ставит отметку о выполнении заказа.

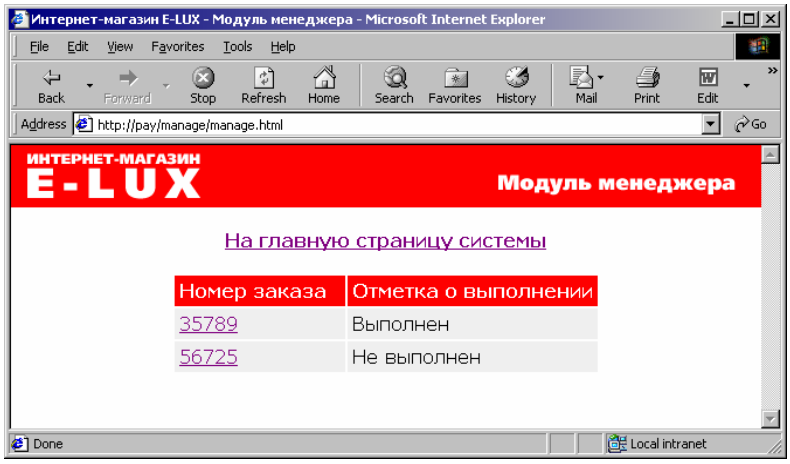


Рис. 4.12. Выбор заказа для просмотра

26. При принятии значения «Выполнен» отметкой о выполнении заказа средства, заблокированные на счете покупателя в банке-эмитенте перечисляются на счет Интернет-магазина в банк-эквайер.

27. В случае отказа клиента от получения доставленного товара менеджер помечает пункт «Отказ от заказа» в графе «Отметка о выполнении», заказ удаляется из общего перечня заказов Интернет-магазина, а ПИС «PAY» осуществляет операцию разблокирования средств на карточном счете клиента в банке-эмитенте (рис. 4.13).

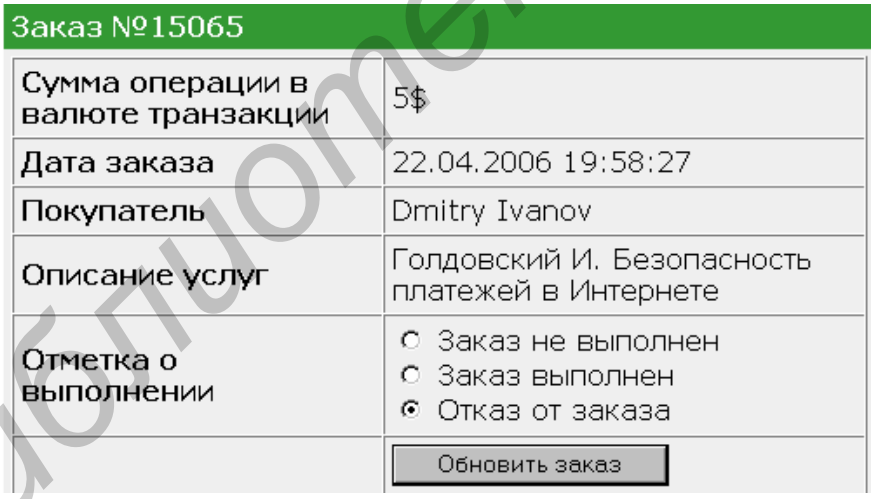


Рис. 4.13. Просмотр заказа

28. **Режим «Клиент банка-эквайера».** В этом режиме вы выступаете в роли владельца Интернет-магазина или иного лица, которое имеет право контролировать счет магазина в банке-эквайере.

29. Введите номер счета Интернет-магазина в банке-эквайере. Для Интернет-магазина «E-LUX» номер счета 100005894 (рис. 4.14).

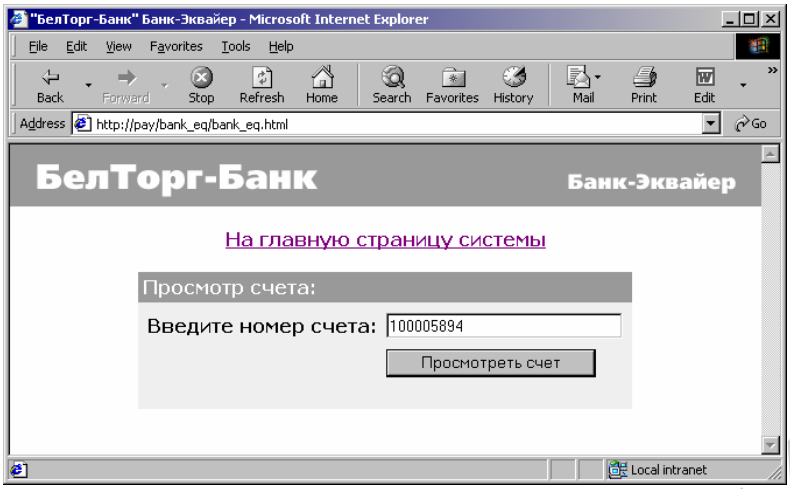


Рис. 4.14. Просмотр заказа

30. Нажатие кнопки «Просмотреть счет» позволяет просмотреть поступление денег на счет Интернет-магазина по датам, номеру заказа и сумме.

Дата платежа	№Заказа	Сумма, USD
01.08.2003	35789	5
03.08.2003	56725	5
05.08.2003	48657	85
07.08.2003	89764	15
	Итого:	110

Рис. 4.15. Просмотр счета

31. Ответить на контрольные вопросы.

32. Оформить отчет.

4.3. Содержание отчета

1. Цель работы.
2. Ответы на контрольные вопросы.
3. Вывод.

4.4. Контрольные вопросы

1. Что называется платежной Интернет-системой?
2. Чем вызвана необходимость соблюдения определенных условий при проведении электронных платежей?
3. Что называется дебетовой системой?
4. Какое назначение имеют электронные чеки?
5. Что называется электронными деньгами?

6. Какими преимуществами обладают электронные деньги?

7. Что называется кредитной Интернет-системой?

8. Какие защищенные протоколы, используемые в платежных Интернет-системах, вы знаете?

9. Что называется авторизацией?

10. Что такое банк-эквайер?

11. Что такое банк-эмитент?

ЛИТЕРАТУРА

1. Бабенко Л.К., Ищуков С.С., Макаревич О.Б. Защита информации с использованием смарт-карт и электронных брелоков. М.: Гелиос АРВ, 2003. – 352 с.

2. Деднев М.А. Защита информации в банковском деле и электронном бизнесе. М.: Кудиц-образ, 2004. – 512 с.

3. Голдовский И. Безопасность платежей в Интернете. – СПб.: Питер, 2001. – 240 с.

Св. план 2006, поз. 102

Учебное издание

Лыньков Леонид Михайлович,
Богуш Вадим Анатольевич,
Борботько Тимофей Валентинович,
Прудник Александр Михайлович

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

Лабораторный практикум

для студентов специальности
«Сети телекоммуникаций»
всех форм обучения

Редактор Т.Н. Крюкова

Подписано в печать 23.05.2006. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 3,6.
Уч.-изд. л. 3,1. Тираж 100 экз. Заказ 636.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131518 от 30.04.2004.
220013, Минск, П. Бровки, 6