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

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ:

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО вузов Республики Беларусь
по образованию в области информатики и радиоэлектроники
в качестве учебно-методического пособия
для студентов учреждений, обеспечивающих
получение высшего образования по специальности
«Защита информации в телекоммуникациях»

Минск БГУИР 2011

УДК 004.056:336.717(076.5)
ББК 32.973.26-018.2+65.262.1я73
З-40

А в т о р ы:
Б. И. Беляев, Т. В. Борботько, И. В. Гасенкова, О. Б. Зельманский,
Л. В. Катковский, Л. М. Лыньков, Л. Л. Утин

Р е ц е н з е н т ы:
заведующий кафедрой информационных технологий в управлении Белорусского национального технического университета, доктор технических наук, профессор В. Ф. Голиков;

заведующий кафедрой управления информационными ресурсами Академии управления при Президенте Республики Беларусь, кандидат технических наук, доцент В. И. Новиков

Защита информации в банковских технологиях: лабораторный
З-40 практикум : учеб.-метод. пособие / Б. И. Беляев [и др.]. – Минск : БГУИР, 2011. – 127 с.
ISBN 978-985-488-630-5

Пособие состоит из шести лабораторных работ, каждая из которых содержит краткие теоретические сведения к теме работы, ход выполнения лабораторного задания, требования к оформлению отчета и вопросы для самоконтроля, ответы на которые контролируются программной экспертной системой. При выполнении работ реализована возможность автоматизации контроля знаний студентов.

УДК 004.056:336.717(076.5)
ББК 32.973.26-018.2+65.262.1я73

ISBN 978-985-488-630-5

СОДЕРЖАНИЕ

Лабораторная работа №1. ЗАЩИТА ЭЛЕКТРОННОГО ОБМЕНА ДАННЫМИ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ 5

1.1. Теоретическая часть 5
1.2. Лабораторное задание 18
1.3. Содержание отчета 21
1.4. Контрольные вопросы 22

Лабораторная работа №2. ЗАЩИТА ПЕРСОНАЛЬНЫХ ПЛАТЕЖЕЙ 23

2.1. Теоретическая часть 23
2.2. Описание программы 39
2.3. Лабораторное задание 46
2.4. Содержание отчета 47
2.5. Контрольные вопросы 47
2.6. Приложение 48

Лабораторная работа №3. ЗАЩИТА УДАЛЕННЫХ БАНКОВСКИХ ТРАНЗАКЦИЙ 49

3.1. Теоретическая часть 49
3.2. Лабораторное задание 67
3.3. Содержание отчета 69
3.4. Контрольные вопросы 69

Лабораторная работа №4. ЗАЩИТА АВТОМАТИЧЕСКИХ КАССОВЫХ АППАРАТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА 70

4.1. Теоретическая часть 70
4.2. Лабораторное задание 100
4.3. Содержание отчета 102
4.4. Контрольные вопросы 102

Лабораторная работа №5. ЗАЩИТА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ В POS-СИСТЕМАХ 103

5.1. Теоретическая часть 103
5.2. Лабораторное задание 113

5.3. Содержание отчета 114
5.4. Контрольные вопросы 114
Лабораторная работа №6. ЗАЩИТА ТРАНЗАКЦИЙ В СИСТЕМАХ МИКРОПЛАТЕЖЕЙ 115
6.1. Теоретическая часть 115
6.2. Лабораторное задание 122
6.3. Содержание отчета 125
6.4. Контрольные вопросы 125
ЛИТЕРАТУРА 126

Лабораторная работа №1

ЗАЩИТА ЭЛЕКТРОННОГО ОБМЕНА ДАННЫМИ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Цель работы: изучить основные принципы построения, методы и средства защиты систем электронного обмена данными.

1.1. Теоретическая часть

1.1.1. Основные принципы построения систем EDI

Системы электронной коммерции B2B типа (Business to Business) характеризуются взаимодействием между относительно постоянными партнерами, связанными единой цепочкой бизнес-процесса и интенсивным двухсторонним информационным обменом. К примеру, это долгосрочные отношения между крупными компаниями. При этом вопрос взаимного недоверия стоит менее остро и может быть отрегулирован на начальном этапе взаимодействия обменом юридически значимыми документами.

Деятельность любого крупного предприятия – совокупность деловых отношений с поставщиками, партнерами, клиентами и банками, которые неизбежно приводят к необходимости обмена информацией. Как правило, большие объемы данных преобразуются из одной формы в другую внутри предприятия. В ряде случаев финансовые затраты на обработку контрактных документов могут составлять до 7 % от общей стоимости контрактов. Целью развития технологии электронного обмена данными (Electronic data interchange – EDI) является создание процедур обмена информацией с предопределенной структурой между различными информационными системами двух и более организаций в процессе заключения сделок, выполнения заказов и контрактов. Электронный обмен данными (рис. 1.1) включает в себя просмотр каталогов, коммерческих предложений, транзакций приобретения товаров, уведомлений о поставке, подтверждений приобретения наряду с финансовой информацией, циркулирующей в банковских сетях.

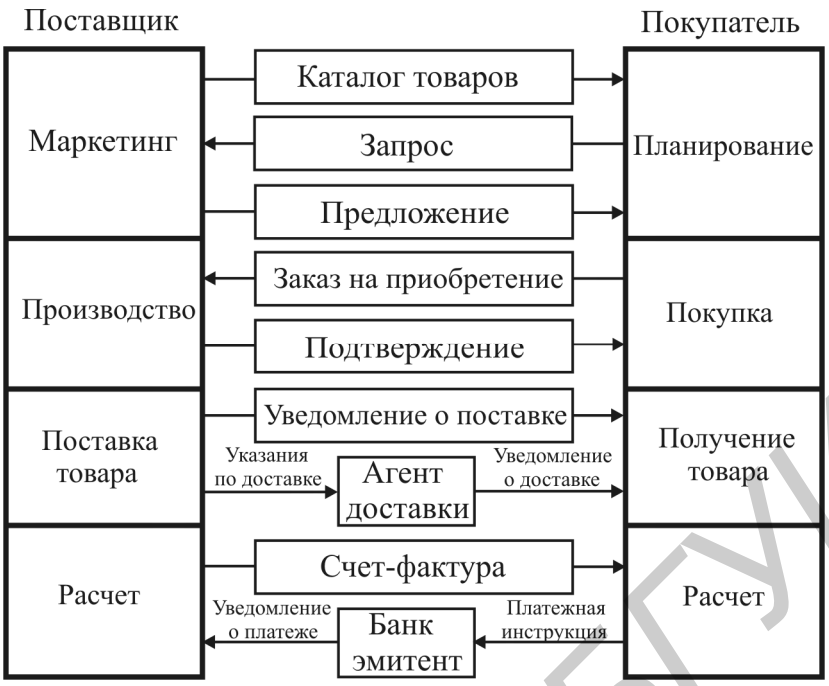

Рис. 1.1. Обмен информацией в процессе электронного обмена данными

Технология EDI позволяет создать поток транзакций между партнерами (например между поставщиком и потребителем). Предположим, что покупатель выбрал объект заказа на основе полученной от поставщика информации. Покупатель заполняет электронный документ, частично сформированный автоматически. Далее заполненный документ передается напрямую в систему обработки входных данных поставщика.

Программное обеспечение (ПО) последнего формирует для ПО покупателя ответ, который содержит информацию о стоимости заказа. Если покупателя она устраивает, процесс обмена информацией продолжается. Покупатель, используя свое программное обеспечение, производит формирование заказа на основе полученной ранее информации с последующей его отправкой поставщику. Программное обеспечение поставщика, получив заказ от покупателя, производит преобразование полученных данных к внутреннему формату представления данных и передает преобразованные данные в различные подразделения поставщика, такие, как бухгалтерия, производственный цех или склад. Кроме того, после получения заказа ПО поставщика отправляет покупателю

подтверждение получения заказа. После выполнения заказа формируется уведомление о поставке, которое передается как покупателю, так и в бухгалтерию поставщика. Получение уведомления о поставке или получение счета-фактуры приводит к созданию и сохранению данных для завершения поставки заказанных товаров.

Если информационная система компании, занимающейся доставкой, интегрирована в общую EDI систему, появляется возможность автоматического создания документов, необходимых для выполнения доставки заказов на основе информации от исполнителя заказов. Кроме того, появляется возможность автоматического запуска финансовых процедур покупателя при получении уведомления о доставке. Далее квитанции могут быть автоматически приведены в соответствие с изначальным содержимым заказа и содержимым полученного счета-фактуры для подготовки платежных инструкций для банка покупателя.

Если банковские расчеты осуществляются с использованием электронных средств оплаты, на банки ложится ответственность за доставку платежных уведомлений поставщикам в соответствии с временными рамками, указанными в условиях заказа. В свою очередь информационная система поставщика должна привести полученный платеж в соответствие со сформированным ранее счетом-фактурой для поддержания целостности финансовой информации о счетах. Другие сервисы включают в себя подготовку счетов и пакетов налоговой информации наряду с архивацией данных транзакции (транзакция – группа последовательных операций, которая представляет собой логическую единицу работы с данными).

Приложения электронного обмена данными (ЭОД) отвечают за управление внутренними сообщениями системы (проверка, сохранение, получение, доставка и т. д.) и синхронизацию данных различных подразделений предприятия. Также может осуществляться глобальный аудит транзакций для поддержания целостности данных системы и увеличения ее защищенности. Приложе-

ния ЭОД могут выполнять задачи архивации для выполнения требований по сохранению и продолжительному использованию документов.

Технология EDI приводит к исчезновению необходимости повторного ввода одних и тех же данных, упрощает сортировку введенных данных, поиск и автоматическое сравнение информации и документов на всех этапах их прохождения. Указанная возможность автоматического сравнения данных позволяет получить уверенность в правильности полученного результата и связи его с исходными данными, что приводит к уменьшению накладных расходов.

Электронный обмен данными включает в себя следующие аспекты работы систем:

– обеспечение соответствия структуры данных, используемой в процессе обмена, общепринятому формату;

– обеспечение безопасности при выполнении основных процедур;

– передачу данных с использованием телекоммуникационных сетей;

– преобразование полученных ранее данных во внутренний формат внутри системы, использующейся на предприятии.

В процессе создания структурированных данных, связанных с транзакцией, происходит их извлечение из соответствующей базы данных и преобразование к общему формату, известному всем участникам проекта, с использованием специализированного ПО. Данное ПО выполняет две основные функции: преобразование данных из внутреннего формата, использующегося для хранения данных, к общему формату процесса обмена данными и обратное преобразование данных из общего формата в соответствии со спецификациями общей структуры данных. На рис. 1.2 представлены компоненты системы EDI.

Процедуры преобразования используют формат представления данных в алфавитно-цифровой форме, однако использование различных видов представления информации в различных сочетаниях (текст, графические файлы, аудиофайлы и т. д.) становится все более распространенным.

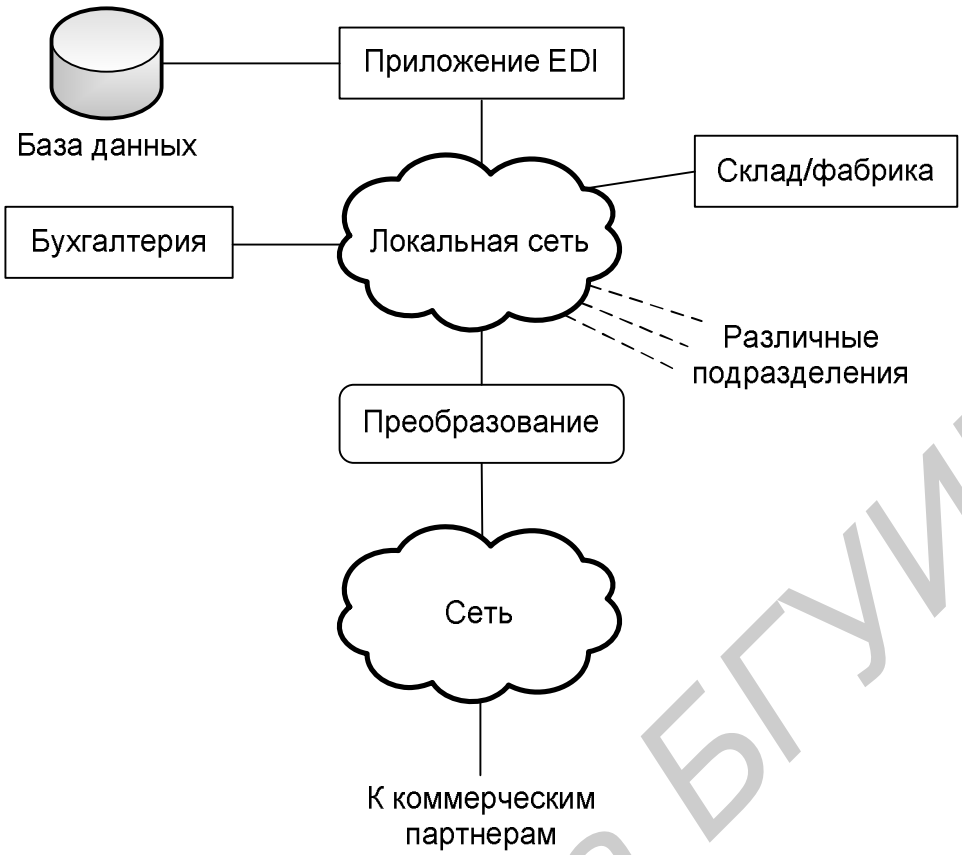

Рис. 1.2. Компоненты системы EDI

Перед передачей преобразованных данных, как правило, производится выполнение процедур обеспечения безопасности в виде шифрования передаваемых данных. В этом случае получатель после получения данных и перед преобразованием их в свой внутренний формат должен выполнить процедуры расшифрования полученной информации. После выполнения процедур преобразования результат передается приложению, отвечающему за обработку полученных данных. Программное обеспечение, реализующее функции преобразования и связи с внутренними приложениями, часто называют транслятором, или преобразователем. Расположение транслятора в структуре бизнес-приложений показано на рис. 1.3.

Управление передачей должно производиться как внутри организации, так и во внешней телекоммуникационной сети. Полученные сообщения должны быть переданы приложению, ответственному за их обработку, в то время как сообщения для партнеров обычно состоят из частей, полученных от раз-

личных подразделений организации, и, таким образом, должны объединяться в единое сообщение перед отправкой получателю. Телекоммуникационные функции должны реализовывать как внутренние протоколы обмена данными, так и протоколы, использующиеся партнерами. Список реализуемых протоколов может быть очень объемным и включать в себя различные протоколы от X.25 до IP, SNA или FR. Сеть передачи данных может быть сформирована с использованием выделенных линий, арендуемых или предоставляемых оператором специализированных сетей.

Рис. 1.3. Положение EDI трансляторов

Оператор сети передачи данных может предоставлять услуги преобразования различных протоколов между различными участниками сети, которые представляют особенный интерес для тех участников сети, которые не обладают приложениями EDI. Использование глобальной сети Интернет в качестве сети передачи данных может полностью изменить природу специализированных сетей передачи данных, заставляя их переходить в область предоставления сервисов обеспечения безопасности, таких, как сертификация участников обмена или заверение транзакций.

1.1.2. Структурирование данных в системах EDI

Рассмотрим вопрос структурного представления данных на примере системы ANSI X12. Базовым элементом в процессе обмена рассматриваемых систем является элемент данных, определенный в соответствии со словарем данных. С функциональной точки зрения элемент данных является либо сервис-

ным, либо прикладным элементом. Сервисные элементы используются в процессе структурирования передаваемых данных для формирования сервисных сегментов. В противоположность им прикладные элементы являются данными, определенными и согласованными участниками транзакции.

Под сегментом понимают множество элементов, простых или составных, которое может включать в себя другие сегменты. Порядок, содержание, максимальное число возможных повторений составляющих и способ организации этих составляющих должны быть определены в словаре сегментов. Сегменты могут образовывать группы сегментов для достижения целей расширения функциональности.

Существует два разных типа сегментов: первые определены как контрольные сегменты в спецификациях X12, другим типом сегментов являются прикладные сегменты. Контрольные сегменты используются для структурирования передаваемых данных и для распознавания участвующих сторон. Прикладные сегменты данных содержат данные приложений, организованные по функциональному признаку. За управление приложениями, ответственными за определение формата и формирование прикладных сегментов данных, отвечает компания, владеющая данными приложениями.

Множество транзакций (X12) является совокупностью структурированных сегментов в порядке, определенном в реестре стандартных сообщений. Данные сообщения представляют реализации функций, общих для различных секторов деятельности. Например, платёжные системы основываются на универсальных правилах и не зависят от вида предприятия. Существует два класса сообщений: сервисные сообщения, формирующиеся из сервисных сегментов и предназначенные для коррекции синтаксиса или ошибок приложений, и прикладные сообщения, состоящие из прикладных сегментов.

В соответствии с терминологией X12 множество транзакций соответствует передаче полезной информации, адекватной содержимому бумажного документа (форма заказа, счет-фактура и т. д.), между вычислительными системами

двух организаций. Каждое множество транзакций состоит из трех частей: заголовка, тела и замыкающей части. Заголовок описывает характеристики передаваемых данных, в то время как замыкающая часть предназначена для проверки целостности переданной информации.

Тело множества транзакций представлено в виде строк или сегментов, которые описывают отдельные аспекты общего документа. В свою очередь сегмент состоит из элементов данных и кодов, обозначающих различные функции, которые должны быть заполнены. Порядок расположения элементов, их композиция и значимость их кодов определены в словаре данных. Например, звездочка (*) обозначает два последовательных элемента, а две звездочки показывают, что необязательный элемент был удален. Если опущенные элементы находились в конце сегмента, то они замещаются маркером конца сегмента.

Существует два типа сегментов: контрольные и прикладные (сегменты данных). Сегменты заголовков и замыкающих частей наряду с циклическими сегментами формируют контрольные сегменты.

1.1.3. Обеспечение безопасности в процессе формирования сообщений

При организации безопасной передачи данных в системах X12 используются структуры, определенные в спецификациях X12.58. В процессе аутентификации для создания кода аутентификации сообщения (Message Authentication Code – MAC) используется алгоритм шифрования DES. Для защиты от атак, основанных на использовании ранее переданных данных, используется вставка, состоящая из даты создания сообщения и уникального идентификатора сообщения. Для обеспечения строгого выполнения обязательств используются алгоритмы шифрования с открытым ключом и временные отметки.

Электронно-цифровая подпись применяется для подтверждения деловых намерений. Заверение содержится в двух сегментах: S3A (или S4A) и SVA. Данные сегменты добавляются перед созданием кода MAC или электронно-цифровой подписи для сообщения. Комбинация сегментов S4A/SVA окружает транзакцию перед ее шифрованием или аутентификацией и является первым

уровнем защиты функциональной группы (табл. 1.1). На каждом уровне защиты применяются свои собственные ключи шифрования. На каждом уровне обеспечения безопасности ключи, используемые для определенного сервиса обеспечения безопасности (например шифрование или аутентификация), различаются.

Таблица 1.1

Значения заголовков

Заголовок	Значение
ISA*	Заголовок сообщения
GS*	Заголовок функциональной группы
S3S*	Заголовок для обеспечения безопасности – уровень 1
S3A*	Заголовок заверения – уровень 1
ST*	Заголовок множества транзакций
S4S*	Заголовок для обеспечения безопасности – уровень 2
S4A*	Заголовок заверения – уровень 2
Сегменты	Форма заказа
SVA*	Данные для обеспечения безопасности – уровень 2
S4E*	Замыкающая часть – уровень 2
SE*	Замыкающая часть множества транзакций
SVA*	Данные для обеспечения безопасности – уровень 1
S3E*	Замыкающая часть – уровень 1
GE*	Конец функциональной группы
IEA*	Замыкающая часть сообщения

Стандарт предусматривает возможность использования алгоритмов сжатия передаваемой информации, которая является необязательным требованием и должна происходить перед выполнением операций шифрования. Кроме того, зашифрованные данные могут быть подвергнуты необязательной операции фильтрации, которая может использоваться для предотвращения появления двоичных последовательностей, которые могут быть некорректно обработаны сетевыми средствами передачи информации.

Виды используемых фильтров:

– фильтр преобразования каждого байта в два шестнадцатеричных символа;

– фильтр преобразования двоичных данных в строку символов ASCII, что приводит к росту требуемой пропускной способности канала передачи данных;

– фильтр ASCII/Baudot, преобразующий двоичные данные в строки символов, которые принадлежат как к набору символов ASCII, так и к набору символов Baudot, что также приводит к росту требуемой пропускной способности канала связи.

Механизмы обеспечения безопасности позволяют реализовать одинаковый уровень безопасности для всех частей транзакции. Системы стандарта X12 могут напрямую использовать сертификаты X.509, полученные от центров сертификации или созданные с использованием специализированного ПО.

1.1.4. Обеспечение безопасности в процессе передачи сообщений

В связи с удаленностью участников процесса ЭОД друг от друга связь между ними осуществляется посредством общедоступных сетей передачи данных, в частности Интернет. Обеспечение защиты ЭОД при передаче сообщений реализуется за счет модульной защиты.

В основе модуля лежат две пары отказоустойчивых межсетевых экранов, защищающих серверы приложений, EDI-трансляторы и рабочие станции пользователей. Дополнительная защита обеспечивается периферийными маршрутизаторами корпоративной и сети провайдера (Internet Service Provider – ISP).

Участник, входящий в систему ЭОД, инициирует соединение с EDI-транслятором после получения IP-адреса с сервера DNS, находящегося в сети ISP (рис. 1.4). Сервер DNS находится в другой сети для того, чтобы сократить число протоколов, необходимых для приложения EDI. Первая группа межсетевых экранов обеспечивает передачу трафика по требуемому адресу. Ответный трафик по этому же каналу следует через межсетевой экран, что не требует инициации EDI-транслятором нового соединения для выхода в Интернет. Меж-

сетевой экран блокирует этот маршрут, чтобы ограничить возможности злоумышленников, если они завладели одним из EDI-трансляторов.

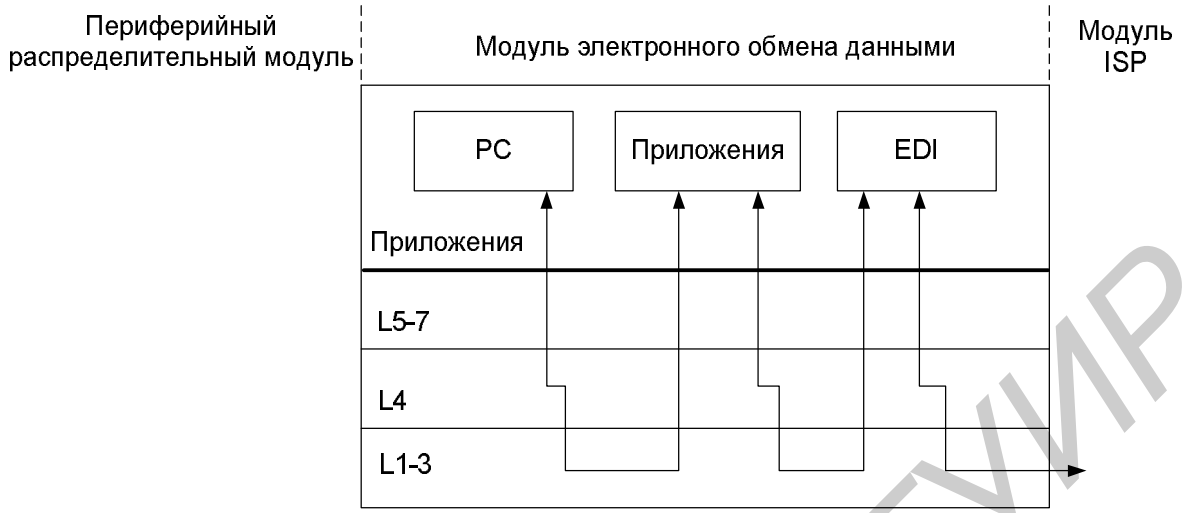

Рис. 1.4. Передача трафика в системе EDI

EDI-транслятор инициирует запросы к серверу приложений. Это соединение вместе с ответным трафиком также разрешается первым межсетевым экраном. Как и в случае с EDI-транслятором, серверу приложений не нужно инициировать соединение с EDI-транслятором или выход в Интернет.

Для защиты сети ЭОД используются следующие средства (рис. 1.5):

– межсетевые экраны (Firewall) – фильтрация пакетов с учетом состояния соединения (Firewall 1), базовая фильтрация пакетов на уровне 7 модели OSI (Firewall 1 и 2), анализ пакетов на уровнях 4–7 модели OSI (Firewall 2), противодействие атакам DoS (Firewall 2);

– средства HIDS (Host Intrusion Detection Service) – позволяет обнаруживать сетевые атаки;

– средства NIDS (Network Intrusion Detection System) – обеспечивают мониторинг ключевых сетевых сегментов на уровнях 4–7 модели OSI;

– коммутатор третьего уровня – позволяет обеспечить контроль доступа и расширенный анализ пакетов на уровнях 4–7 модели OSI;

– маршрутизатор с модулем ISP – масштабируемое устройство ввода с функцией противодействия IP-спуфингу, противодействия атакам (D)DoS, фильтрации пакетов на уровне 4 модели OSI.

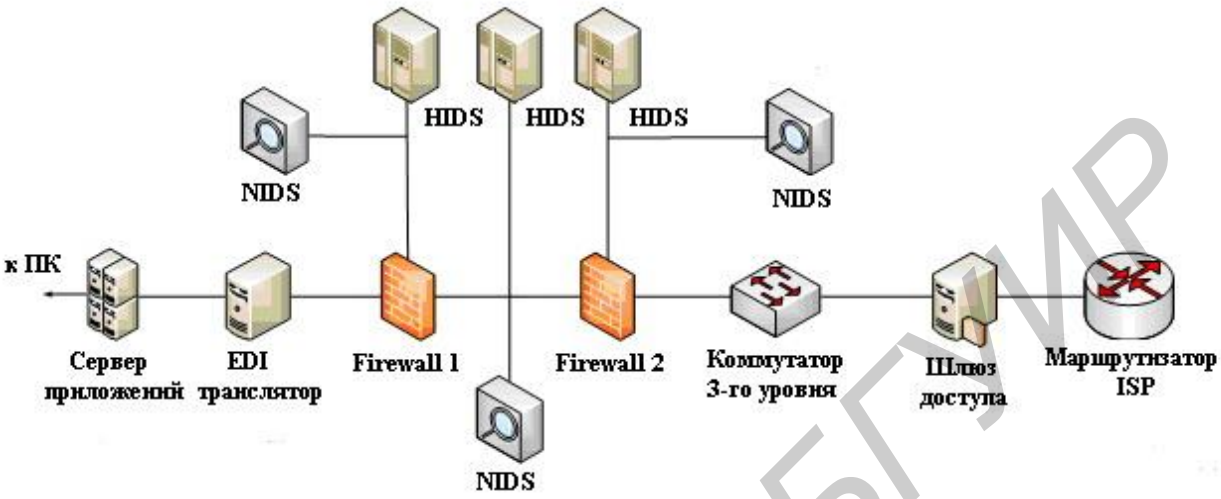

Рис. 1.5. Пример построения системы защиты сети электронного обмена данными

Межсетевые экраны должны обеспечивать передачу трафика только по трем маршрутам, каждый из которых работает со своим протоколом, и блокировку всех остальных соединений, если они не представляют собой передачу пакетов в ответ на запросы, поступившие по трем первоначальным маршрутам. Сами серверы также должны быть защищены. Особое внимание уделяется защите EDI-транслятора, предназначенного для общего доступа. Необходимо пользоваться самыми последними версиями операционной системы и приложений. Кроме того, эти средства должны находиться под постоянным наблюдением со стороны средств обнаружения атак (HIDS). Эти меры позволят снизить эффективность большинства первичных и вторичных атак, включая переадресацию портов.

Межсетевые экраны сети ЭОД обычно защищаются периферийным маршрутизатором заказчика, установленным у провайдера. В точке выхода этого маршрутизатора по направлению к сети предприятия провайдер может макси-

мально ограничить количество протоколов, необходимых для электронной коммерции, а также разрешить передачу трафика только в адрес EDI-трансляторов.

Для борьбы с атаками типа (D)DoS провайдер должен ограничивать объем трафика, кроме того, он должен выполнять фильтрацию пакетов в соответствии со стандартами RFC 1918 и RFC 2827. В помещении предприятия маршрутизатор ISP служит только в качестве интерфейса для связи с провайдером. Задачи по обеспечению соединений возлагаются на коммутатор третьего уровня.

Коммутаторы третьего уровня обеспечивают маршрутизацию, определяя оптимальный маршрут для того или иного пользователя. Кроме того, они выполняют фильтрацию пакетов в соответствии с фильтрацией, выполняемой на стороне провайдера, что повышает уровень безопасности системы в целом. Средства NIDS, находящиеся с внутренней стороны межсетевого экрана, проверяют сегменты для распознавания атак. Связи между различными уровнями системы защиты должны быть защищенными и обладать надежной системой аутентификации.

1.1.5. Обеспечение безопасности внутри сети предприятия

Обеспечение безопасности внутри сети предприятия необходимо проводить по следующим основным направлениям:

– противодействие вредоносному программному обеспечению;

– контроль доступа к информации;

– разграничение прав доступа пользователей;

– резервирование критической информации,

что может быть реализовано за счет:

– использования антивирусного программного обеспечения;

– многофакторной аутентификации пользователей;

– обеспечения авторизации пользователей;

– ведения системного журнала;

– резервного копирования критической информации.

1.2. Лабораторное задание

1. Включить персональный компьютер.

2. Запустить файл EDI.exe на выполнение.

3. Появившееся на экране главное окно программы содержит пункты меню «Приступить к выполнению» и «Теория». Выбор пункта меню «Теория» позволит получить общие сведения о технологии EDI. Выполнение работы начинается при выборе пункта меню «Приступить к выполнению».

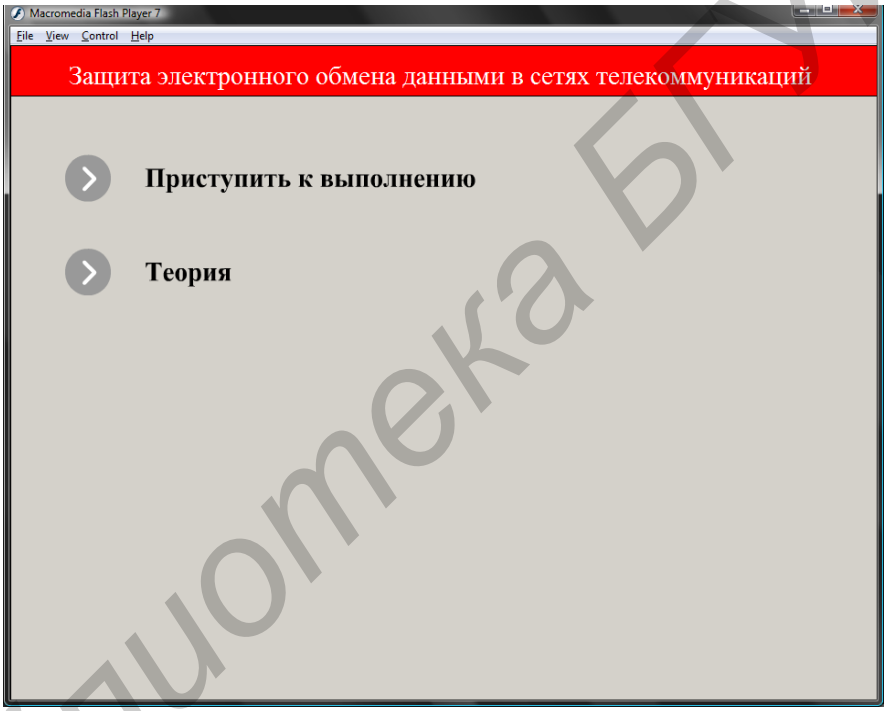

Рис. 1.6. Внешний вид главного окна программы

4. При нажатии ссылки «Приступить к выполнению» на экране появится окно программы (рис. 1.7), разделенное на две части. В одной части находятся меню выбора участников ЭОД и методов, и средств обеспечения защиты информации. В другой части отображена модель системы ЭОД, которая используется для демонстрации построения схемы системы.

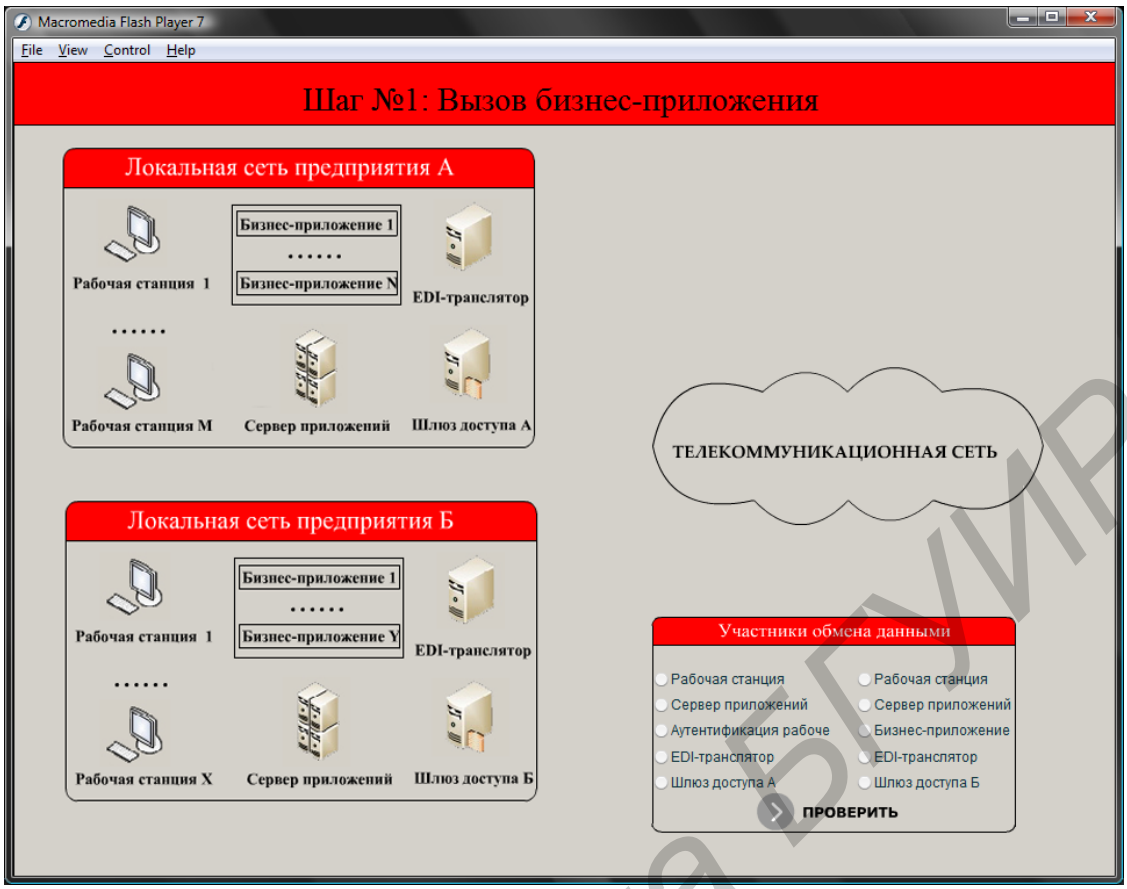

Рис. 1.7. Внешний вид окна программы

5. Выполнение работы заключается в пошаговом составлении схемы процесса ЭОД между двумя предприятиями и выборе средств защиты для каждого шага. В схеме используются следующие элементы:

– локальная сеть предприятия А;

– локальная сеть предприятия Б;

– телекоммуникационная сеть.

Локальные сети предприятий включают в себя следующие компоненты:

– рабочие станции;

– сервер приложений;

– бизнес-приложения;

– EDI-транслятор;

– шлюз доступа.

6. Для выбора участников ОЭД в меню «Участники обмена данными» выбирают из двух столбцов необходимые варианты. В первом столбце указыва-

ется участник, передающий данные, а во втором – участник, их принимающий. После того как выбор сделан, необходимо нажать кнопку «Проверить». При выборе неверных вариантов на экран выводится сообщение об ошибке «Неверно» (рис. 1.8). Для исправления ошибки необходимо нажать ссылку «Выбрать заново». В случае верного выбора выводится сообщение «Верно» и приводится описание процесса, происходящего на данном шаге. Дальнейшее выполнение работы происходит при выборе ссылки «Далее».

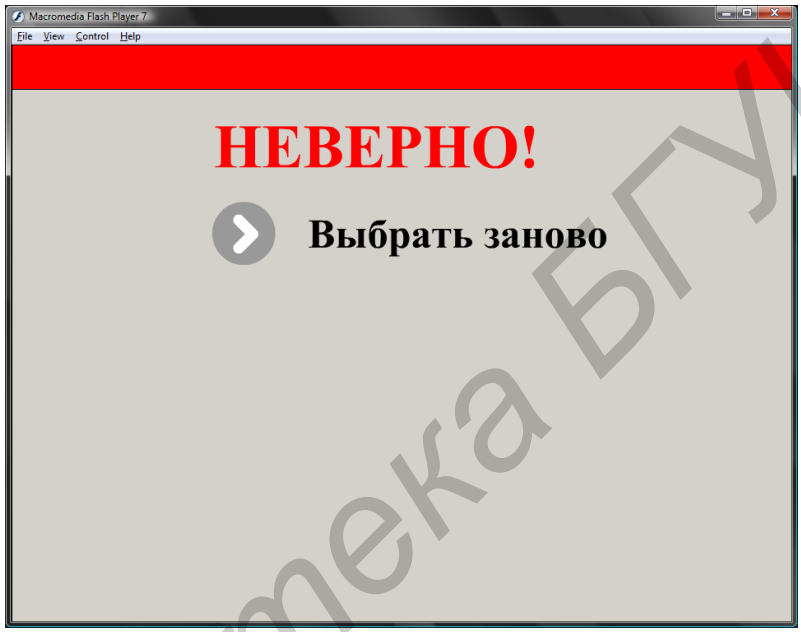

Рис. 1.8. Внешний вид окна с сообщением об ошибке

7. После выбора пары участников ОЭД необходимо выполнить выбор средств защиты для данного этапа взаимодействия участников из предлагаемого перечня (рис. 1.9).

8. После завершения выполнения работы на экран выводится информация об допущенных ошибках (рис. 1.10).

9. Лабораторная работа считается выполненной при наличии не более 10 ошибок в разделах «Участники обмена данными» и «Обеспечение защиты информации».

10. Ответить на контрольные вопросы.

11. Оформить отчет.

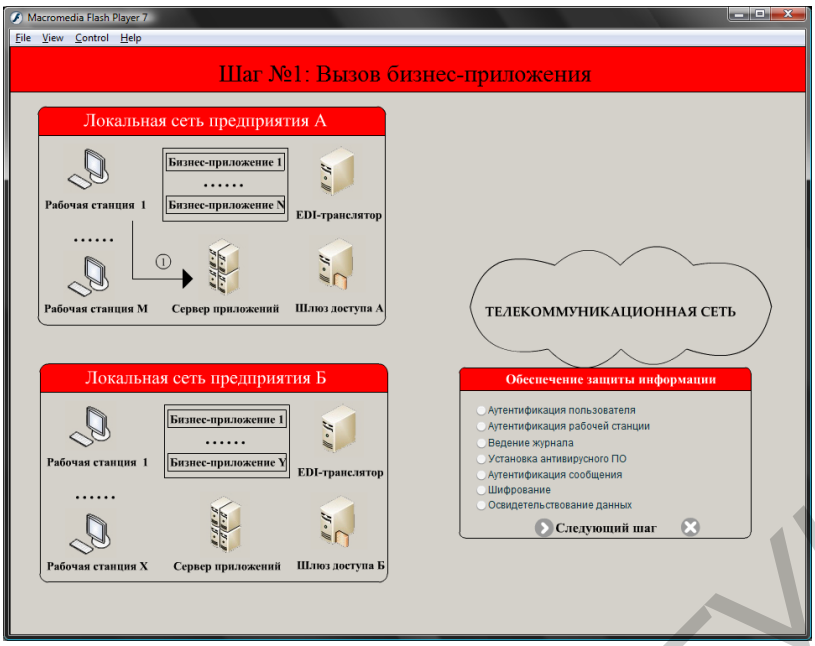

Рис. 1.9. Внешний вид окна для выбора средств защиты

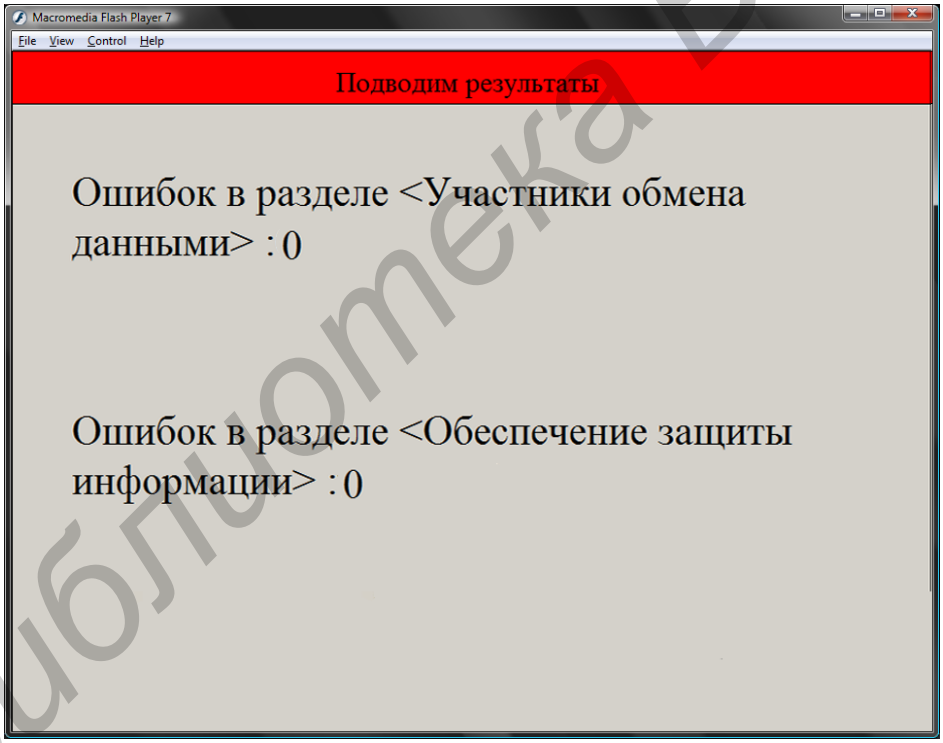

Рис. 1.10. Внешний вид окна с сообщением об ошибке

1.3. Содержание отчета

1. Цель работы.
2. Таблица результатов выполнения работы:

Номер шага	Участники обмена данными	Описание характера взаимодействия

3. Вывод по работе.

4. Ответы на контрольные вопросы.

1.4. Контрольные вопросы

1. Назначение технологии электронного обмена данными.

2. Функции, выполняемые EDI-транслятором.

3. Особенности обеспечения безопасности при формировании сообщений в системах ANSI X12.

4. Назначение аппаратно-программных средств защиты систем электронного обмена данными.

5. Функции защиты электронного обмена данными, реализуемые провайдером.

Лабораторная работа №2

ЗАЩИТА ПЕРСОНАЛЬНЫХ ПЛАТЕЖЕЙ

Цель работы: изучить основные виды атак в системах персональных платежей и методы защиты от них. Получить практические навыки по моделированию защищенной системы персональных платежей.

2.1. Теоретическая часть

2.1.1. Электронная коммерция

Сфера электронной коммерции – область экономической деятельности, представляющая собой совокупность организационных, правовых, экономических и технических мероприятий. Она позволяет автоматизировать процессы как персональных платежей физических и юридических лиц, так и межбанковские расчеты, являющиеся основой банковской деятельности государства.

Основными функциями электронной коммерции являются:

– предоставление пользователям (клиентам) набора услуг в банковской сфере;

– обеспечение доступа пользователям к своей финансовой информации;

– автоматизация внутри- и межбанковских операций, введение бухгалтерии и составление сводных отчетов;

– расширение клиентской базы за счет удаленного доступа.

Развитие электронной коммерции стало следствием развития систем и сетей передачи данных, увеличения документооборота и ужесточения требований к скорости и качеству передачи информации. Построение систем электронной коммерции на основе уже существующих сетей (Internet, ТфОП, SDH, ATM и др.) способствует значительной экономии средств и расширяет их географическое распространение. Интегрированное оборудование позволяет использовать одну и ту же транспортную систему для передачи различных видов информации с заданной скоростью и качеством.

Сфера электронной коммерции представляет собой систему самостоятельных организаций (например банков), объединенных в единую телекоммуникационную сеть. Эти организации предоставляют некоторые услуги своим клиентам, используя собственные либо арендуемые направляющие системы. Обеспечением координации и обмена данных между организациями занимается провайдер, имеющий необходимые ресурсы и предоставляющий услуги передачи данных. Иерархия такой системы представлена на рис. 2.1.

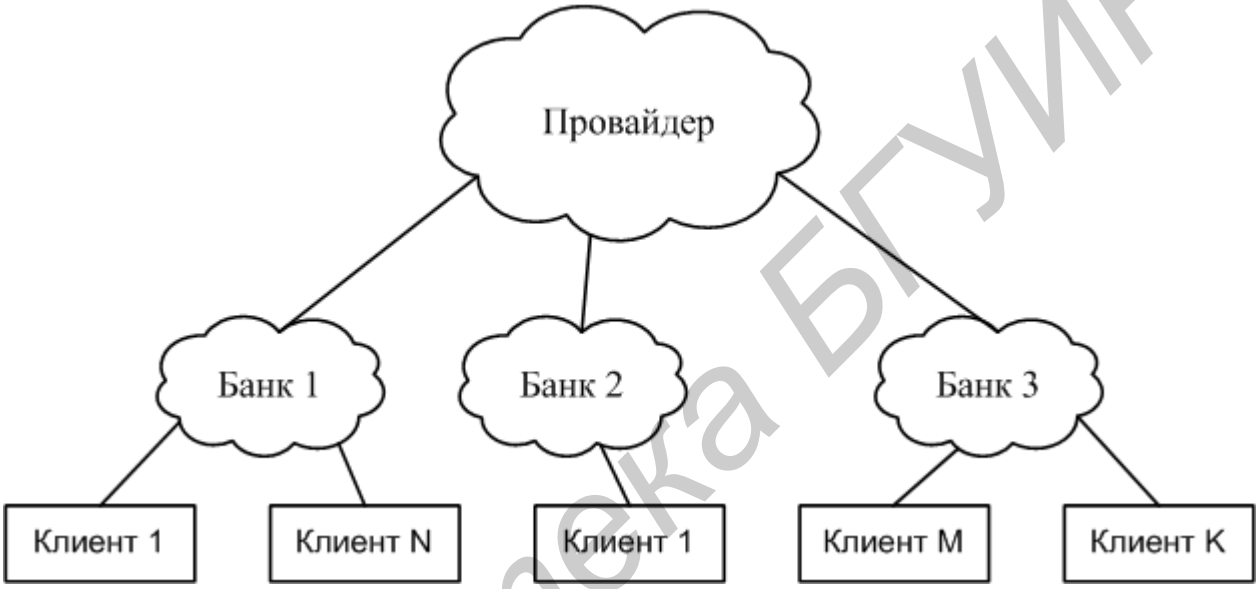

Рис. 2.1. Иерархическая модель системы электронной коммерции

2.1.2. Объекты защиты

В общем случае система электронной коммерции представляет собой автоматизированную систему, состоящую из трех основных подсистем:

– банк;

– клиент;

– коммуникации.

Подсистема Банк обеспечивает прием и обработку электронных расчетных документов и запросов клиента, предоставление клиенту запрашиваемой информации и выписок по его счетам.

Подсистема Клиент реализует формирование электронных расчетных документов и запросов, просмотр запрашиваемой информации.

Подсистема Коммуникаций обеспечивает информационное взаимодействие подсистем Клиент и Банк. В общем случае информационное взаимодействие подсистем Клиент и Банк основывается на обмене электронными сообщениями, содержащими передаваемые между подсистемами данные. Обмен электронными сообщениями может осуществляться как с использованием средств электронной почты, так и с помощью специально разработанных для этих целей средств.

Подсистема Банк может быть одним из компонентов автоматизированной системы банка (АСБ) и взаимодействовать с другими подсистемами этого же учреждения. При этом для реализации функций данная подсистема может комплектоваться выделенным оборудованием или использовать ресурсы АСБ совместно с другими подсистемами.

Подсистема Клиент может одновременно являться компонентом информационной системы клиента и взаимодействовать с некоторыми подсистемами его информационной системы. Такая организация подсистемы Клиент характерна для предприятий, являющихся клиентами банка. Кроме того, для реализации подсистемы может применяться автономный компьютер, не входящий в состав телекоммуникационной сети клиента. Такая организация наиболее характерна для физических лиц, пользующихся услугами банка.

Подсистема Коммуникаций использует ресурсы как локальных сетей банка и клиента, так и сетей общего доступа.

Объектами защиты в системах и сетях электронной коммерции являются:

– данные пакетов, передаваемые по защищенному каналу в рамках частной виртуальной сети (VPN);

– инфраструктура передачи данных (аппаратные и программные средства, встроенное программное обеспечение, каналы связи, интерфейсы к сетью передачи данных);

– атрибуты безопасности узлов сети (криптографические ключи, таблицы маршрутизации, списки доступа и информация о конфигурации системы);

– аутентификационные данные пользователей;

– аппаратные и программные средства управления безопасностью;

– сообщения инцидентов безопасности, данные аудита безопасности и статистика по работе сети;

– информация управления сетью.

2.1.3. Основные виды атак

Сниффер пакетов. Представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен.

Снифферы пакетов используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например имена пользователей и пароли). Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

IP-спуфинг. Когда злоумышленник – сотрудник организации (outsider) или вне ее, выдает себя за санкционированного пользователя, он может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, что позволяет получить доступ к сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для других видов атак.

Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами.

Для двусторонней связи злоумышленник должен изменить таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые злоумышленники, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от u1089 системы важного файла, ответы приложений не имеют значения. Если же злоумышленнику удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, он получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Отказ в обслуживании. (Denial of Service – DoS) – является наиболее известной формой атак, против которой достаточно сложно создать надежную защиту.

Тем не менее именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Существуют следующие наиболее известные разновидности DoS атак:

– TCP SYN Flood;

– Ping of Death;

– Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K);

– Trinco;

– Stacheldracht;

– Trinity.

Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к телекоммуникационной сети организации или на получение из этой сети какой-либо информации. Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

В случае использования некоторых серверных приложений (таких, как web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, не допуская обслуживания

обычных пользователей. В ходе атак DoS могут использоваться стандартные протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или уязвимости в системе безопасности, а на недостатки системной архитектуры сети.

Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов. Сложность предотвращения этого типа атак заключается в том, что для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть это сделать невозможно, потому что вся полоса пропускания канала связи будет занята. Когда атака этого типа проводится одновременно через множество устройств, имеет место распределенная атака DoS (DDoS – distributed DoS).

Парольные атаки. Злоумышленник может проводить парольные атаки с помощью целого ряда методов, таких, как простой перебор (brute force attack), «троянский конь», IP-спуфинг и сниффинг пакетов.

Хотя логин и пароль часто можно получить при помощи IP-спуфинга и сниффинга пакетов, злоумышленники часто пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название простого перебора (brute force attack).

Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например к серверу). Если в результате злоумышленник получает доступ к u1088 ресурсам, он получает его на правах обычного пользователя, пароль которого был подобран. Если этот пользователь имеет значительные привилегии доступа, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если пользователь изменит свой пароль и логин.

Еще одна проблема возникает, когда пользователи применяют один и тот же пароль для доступа ко многим системам: корпоративной, персональной и

системам Интернет. Поскольку устойчивость пароля определяется устойчивостью самого слабого хоста, хранящего его, злоумышленник, узнавший пароль через этот хост, получает доступ ко всем остальным системам, где используется тот же пароль. Хост (host – хозяин, принимающий гостей) – любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определенное на этих интерфейсах.

Прежде всего парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, ресурсы и устройства поддерживают указанные выше методы аутентификации.

Атаки типа «Man-in-the-Middle». Для этого злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Атаки на уровне приложений. Самый распространенный способ проведения такой атаки состоит в использовании известных уязвимостей серверного программного обеспечения (sendmail, HTTP, FTP), используя которые, злоумышленник может получить доступ к компьютеру от имени пользователя, работающего с приложением. Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой

экран. К примеру, злоумышленник, эксплуатирующий известную уязвимость web-сервера, часто использует в ходе атаки TCP порт 80. Поскольку web-сервер предоставляет пользователям web-страницы, межсетевой экран должен предоставлять доступ к этому порту. С точки зрения межсетевого экрана атака рассматривается как стандартный трафик для порта 80.

Полностью исключить атаки на уровне приложений невозможно. Злоумышленники постоянно открывают и публикуют в Интернете все новые уязвимые места прикладных программ. Противодействовать этому можно за счет системного администрирования.

Сетевая разведка. Такой атакой называется u1089 получение информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты работают в данной среде. Получив список хостов, злоумышленник использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И наконец, злоумышленник анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для несанкционированного доступа.

Злоупотребление доверием. Представляет собой злонамеренное использование отношений доверия, существующих в сети. Классическим примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP.

Поскольку все они принадлежат к одному и тому же сегменту, доступ к одному из них приводит к доступу ко всем остальным, так как эти серверы «доверяют» другим системам своей сети. Отношения доверия должны ограничи-

ваться определенными протоколами и по возможности аутентифицироваться не только по IP-адресам, но и другим параметрам.

Переадресация портов. Представляет собой разновидность злоупотребления доверием, когда хост, к которому злоумышленник получил несанкционированный доступ, используется им для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отфильтрован. Допустим, что межсетевой экран имеет три интерфейса, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны межсетевого экрана. Хост общего доступа может подключаться и к внутреннему, и к внешнему хостам. Если злоумышленник получит возможность распоряжаться ресурсами хоста общего доступа, он сможет установить на нем программное обеспечение, перенаправляющее трафик с внешнего на внутренний хост. В этом случае межсетевой экран не обеспечит защиту такой сети, а внешний хост в результате переадресации получает прямой доступ к защищенному хосту.

Основным способом борьбы с переадресацией портов является использование надежных моделей доверия. Кроме того, противодействие злоумышленнику в плане установки своего программного обеспечения может оказать система обнаружения вторжений IDS (HIDS).

Несанкционированный доступ. По сути своей является не отдельным типом атаки, а ее результатом.

Противодействие ***вредоносному программному обеспечению*** ведется с помощью антивирусных программных средств, которые обеспечивают их обнаружение и локализацию.

2.1.4. Протоколы безопасности

Протокол PPP CHAP. Используется для периодической аутентификации центрального компьютера или конечного пользователя с помощью согласования по трем параметрам. Аутентификация происходит в момент установления связи, но может повторяться и после нее.

Маршрутизатор предприятия проводит аутентификацию сервера сетевого доступа (NAS) или «аутентификатора». CHAP обеспечивает безопасность сети, требуя от операторов обмена «текстовым секретом». Эта ключевая информация не передается по каналу связи. По завершении этапа установления связи аутентификатор передает вызывающему аппаратно-программному средству (далее – компьютеру) запрос, который состоит из аутентификатора (ID), случайного числа и имени центрального компьютера (для местного устройства) или имени пользователя (для удаленного устройства).

Вызывающий компьютер проводит вычисления с использованием односторонней хэш-функции. Аутентификатор, случайное число и общий «текстовый секрет» один за другим используются для вычисления хэш-функции. После этого вызывающий компьютер отправляет серверу ответ, который состоит из хэша и имени центрального компьютера или имени пользователя удаленного устройства. По получении ответа аутентификатор проверяет в ответе имя и выполняет те же вычисления. Затем результат этих вычислений сравнивается с аналогичной величиной, содержащейся в ответе вызывающего компьютера. Если эти величины совпадают, результат аутентификации считается u1087 положительным, система выдает соответствующее уведомление, и соединение устанавливается. Пока данная процедура не будет выполнена, удаленное устройство не сможет подключиться к местному устройству.

CHAP обеспечивает защиту от использования чужих паролей за счет пошаговых изменений аутентификатора и применения переменной величины запроса. Повторяющиеся запросы предназначены для ограничения времени, в течение которого система теоретически остается подверженной любой отдельной атаке. Частоту и количество неудачных попыток входа в систему контролирует аутентификатор. Обычно в качестве односторонней хэш-функции CHAP используется MD5, а общий секрет хранится в текстовой форме.

Протокол SSL. Открытый протокол, определяющий механизм поддержки безопасности данных на уровне между протоколами приложений (Hypertext

Transfer Protocol (HTTP), Telnet, Network News Transfer Protocol (NNTP) или File Transfer Protocol (FTP)) и протоколом TCP/IP. Он поддерживает шифрование данных, аутентификацию серверов, проверку целостности сообщений и аутентификацию клиентов в канале TCP/IP (опционально).

Основное назначение протокола SSL состоит в том, чтобы обеспечить защищенность и надежность соединения между двумя взаимодействующими приложениями. Этот протокол состоит из двух уровней. Нижний уровень, который располагается поверх транспортного протокола (например TCP), называется SSL Record Protocol. SSL Record Protocol используется для встраивания различных протоколов высокого уровня. Один из таких встроенных протоколов, SSL Handshake Protocol, позволяет серверу и клиенту аутентифицировать друг друга и согласовывать алгоритм шифрования и криптографические ключи, прежде чем протокол приложения произведет обмен данными. Одно из преимуществ SSL состоит в том, что он независим от протоколов приложений. Протокол высокого уровня может совершенно прозрачно располагаться поверх протокола SSL. Протокол SSL поддерживает безопасность связи, придавая ей следующие свойства:

– защищенность. После первоначального квитирования связи применяются средства шифрования и определяется секретный ключ. Для шифрования данных используются средства симметричной криптографии (DES, RC4 и т. д.);

– участник сеанса связи может быть аутентифицирован и с помощью общих ключей, то есть средствами асимметричной криптографии (RSA, DSS и т. д.);

– надежность связи. Транспортные средства проводят проверку целостности сообщений с помощью зашифрованного кода целостности (MAC). Для вычисления кодов MAC используются безопасные хэш-функции (SHA, MD5 и т. д.).

На каждом уровне протокола сообщения имеют ряд полей для указания длины, описания и содержания. SSL воспринимает данные, предназначенные

для передачи, делит их на управляемые блоки, проводит сжатие данных (при необходимости), использует код MAC, производит шифрование и передает результат. Принятые данные расшифровываются, проверяются, декомпрессируются и реассемблируются, а затем передаются клиентам более высокого уровня. Протокол SSL принят только в рамках протокола HTTP.

Протокол SSH (Secure Shell). Предназначен для защиты удаленного доступа и других сетевых услуг в сети общего пользования. Он поддерживает безопасные удаленный вход в сеть, передачу файлов и эстафетную передачу сообщений по протоколам TCP/IP и X11. SSH может автоматически шифровать, аутентифицировать и сжимать передаваемые данные.

Протокол SSH состоит из трех основных компонентов:

– протокол транспортного уровня. Обеспечивает аутентификацию сервера, конфиденциальность и целостность данных с отличной защищенностью эстафетной передачи. В качестве опции может поддерживаться компрессия данных;

– протокол аутентификации пользователя позволяет серверу аутентифицировать клиента;

– протокол соединения мультиплексирует зашифрованный туннель (защищенная среда в канале связи общего пользования), создавая в нем несколько логических каналов.

Все сообщения шифруются с помощью IDEA или одного из нескольких других средств шифрования (Triple DES с тремя ключами, DES, RC4-128, Blowfish). Обмен ключами шифрования происходит с помощью RSA, а данные, использованные при этом обмене, уничтожаются каждый час без сохранения ключей. Каждый центральный компьютер имеет ключ RSA, который используется для его аутентификации при использовании технологии аутентификации RSA. Для защиты сети от IP-спуфинга используется шифрование, а для защиты от DNS и спуфинга маршрутизации используется аутентификация с помощью

общих ключей. Кроме того, ключи RSA применяются для аутентификации центральных компьютеров.

Недостатком протоколов безопасности, действующих на уровне сессий, является их зависимость от инструкций протокола транспортного уровня. В случае SSL это означает, что атака на TCP может быстро прервать сессию SSL и потребовать формирования новой сессии, в то время как TCP будет считать, что все идет нормально.

Преимущества средств безопасности транспортного уровня (например SSL или SSH) включают:

– возможность действий на сквозной основе (end-to-end) с существующими стеками TCP/IP, существующими интерфейсами прикладного программирования (API) (WinSock, Berkeley Standard Distribution (BSD) и т. д.);

– высокую эффективность по сравнению с низкоскоростными каналами передачи данных, поддержку технологии Van Jacobson для сжатия заголовков и различных средств контроля за переполнением сети, просматривающих заголовки TCP/IP;

– отсутствие каких-либо проблем с фрагментацией, определением максимального объема блоков, передаваемых по данному маршруту (MTU) и т. д.;

– сочетание сжатия с шифрованием данных. На данном уровне такое сочетание оказывается гораздо более эффективным, чем на уровне пакетов.

Протокол HTTPS. Представляет собой защищенный протокол HTTP, ориентированный на передачу данных и разработанный для использования в сочетании с HTTP. Он предоставляет клиенту и серверу одинаковые возможности, при этом сохраняется модель транзакций и эксплуатационные характеристики HTTP.

Клиенты и серверы HTTPS допускают использование нескольких стандартных форматов криптографических сообщений. Клиенты, поддерживающие HTTPS, могут устанавливать связь с серверами HTTPS и наоборот, эти серверы могут связываться с клиентами HTTPS, хотя в процессе подобных транзакций

функции безопасности HTTPS использоваться, скорее всего, не будут. HTTPS не требует от клиента сертификатов общих ключей (или самих общих ключей), потому что этот протокол поддерживает только операции с симметричными ключами шифрования.

Протокол HTTPS поддерживает безопасные сквозные (end-to-end) транзакции, что выгодно отличает его от базовых механизмов аутентификации HTTP, которые требуют, чтобы клиент попытался получить доступ и получил отказ, и лишь затем включают механизм безопасности. Клиенты могут быть настроены таким образом, чтобы любая их транзакция автоматически защищалась (обычно с помощью специальной метки в заголовке сообщения). Такая настройка, к примеру, часто используется для передачи заполненных бланков.

HTTPS поддерживает высокий уровень гибкости криптографических алгоритмов, режимов и параметров. Для того чтобы клиенты и серверы смогли выбрать единый режим транзакции, используется механизм согласования опций, криптографических алгоритмов (RSA или Digital Signature Standard (DSA) для подписи, DES или RC2 для шифрования и т. д.) и выбора сертификатов (например: «Подписывайтесь своим сертификатом Verisign»). HTTPS поддерживает криптографию общих ключей и функцию цифровой подписи и обеспечивает конфиденциальность данных.

Протокол IPsec. Представляет собой набор u1089 стандартов, используемых для защиты данных и аутентификации на уровне IP. Текущие стандарты IPsec включают независимые от алгоритмов базовые спецификации, которые являются стандартными RFC. Протокол IPsec также включает криптографические методы, удовлетворяющие потребности управления ключами на сетевом уровне безопасности.

Протокол IPsec позволяет поддержать на уровне IP потоки безопасных и аутентичных данных между взаимодействующими устройствами, включая центральные компьютеры, межсетевые экраны различных типов и маршрутизаторы.

В табл. 2.1 приведено соответствие открытых протоколов, протоколов безопасности и уровней моделей OSI и TCP/IP.

Таблица 2.1

Сетевые протоколы

Номер уровня	ISO OSI	TCP/IP	Open Protocols	Security Protocols
7	Прикладной	Прикладной	FTP, HTTP, Telnet, SMTP, DNS	HTTPS, SSL
6	Представления			
5	Сеансовый			
4	Транспортный	Хост – Хост	TCP, UDP	SSH
3	Сетевой	Интернет	IP, ICMP, ARP, RARP	IPSec (AH, ESP)
2	Канальный	Сетевой доступ	Ethernet, Fast Ethernet	PPP CHAP
1	Физический			

2.1.5. Программно-аппаратные средства обеспечения безопасности

Некоторые производители сетевого оборудования организуют отдельную линию по производству оборудования, специально предназначенного для защиты информации. Одним из таких производителей является компания Cisco Systems. В табл. 2.2 приведены основные классы оборудования и функции, которые они выполняют.

Функция «AntiDoS» заключается в обнаружении атак типа «DoS» и «DDoS» путем анализа характеристик трафика и ограничения пакетной нагрузки, проходящей через устройство. Такой функцией обладают некоторые устройства третьего уровня модели OSI (маршрутизаторы, межсетевые экраны и др.) и специальное программное обеспечение, устанавливаемое на сервера и рабочие станции.

AVP (Anti Virus Protection) – обобщенное название технологий, программных средств и их обновлений, служащих для обнаружения таких атак и их предотвращения. Основным средством антивирусной защиты являются программные антивирусы и их базы данных, содержащие код известных вирусов.

Они устанавливаются на сервера и рабочие станции и требуют регулярного обновления. Основным источником вирусных атак является сеть Интернет, в частности, сеть ISP (Internet Service Provider).

Таблица 2.2

Оборудование и его функции

Наименование оборудования	Функции						
	Anti DoS	AVP	URL filter	SSH	IPSec	SSL	NAT
PIX FireWall	+		+		+		+
Intrusion Detection Service	+		+		+	+	
Adaptive Security Appliance	+		+				+
Traffic Anomaly Detection	+						
Service Control Engine	+	+					
Network Intrusion Detection System	+			+	+	+	
Advanced Security	+	+		+	+		

Контроль Интернет-трафика позволяет снизить вероятный ущерб с помощью установки фильтров ссылок (***URL filter***) и списков доступа (Access-Control List). Фильтр ссылок ограничивает возможность «заходов» на непроверенные сайты по вводу их Интернет-адресов. Списки доступа создают фильтры на определенные параметры пакетов: адреса источников, получателей и порты. Например, для ограничения FTP-трафика на маршрутизаторе устанавливается список доступа на порт 21 (протокол FTP).

Сеть Интернет по умолчанию считается незащищенной, поэтому при передаче критически важной информации через эту сеть необходимо использовать протоколы шифрования и аутентификации данных (***SSH, IPsec, SSL***), позволяющие обеспечить целостность и конфиденциальность передаваемой информации.

Структура сети любого предприятия, в том числе и в области электронной коммерции, является конфиденциальной информацией. Открытость сетевой иерархии и IP-адресации позволяют злоумышленнику не только получить сведения о сетевом оборудовании, но и, присвоив себе внутренний IP-адрес, выдать себя за пользователя сети. В целях скрытия внутренней сетевой адресации широко применяется технология трансляции сетевых адресов (***Network Address Translation – NAT***), заменяющая адреса источников в пакетах, выходящих за границы сети, на адреса, не использующиеся внутри сети.

2.2. Описание программы

Главное окно программы. В левом верхнем углу окна (рис. 2.2) размещается поле ввода количества денежных средств для приобретения средств защиты. Таблица наименований средств защиты и их стоимости находится в правой части главного окна. Эквалайзер вероятностей атак по их типам позиционируется в левом нижнем углу. Запуск программы обеспечивается нажатием кнопки «Start».

Рабочее окно программы. Здесь размещаются: меню пользователя (верхняя часть окна) (рис. 2.3); схема банковской сети; окно баланса денежных средств (левый верхний угол окна), значение которого дебетируется на величину стоимости устанавливаемого средства защиты; кнопки (в правом верхнем углу) запуска банковской сети (ее включение обеспечивает генерацию пакетов, относящихся к совершаемым платежам и атакам) и паузы (временная остановка генерации пакетов); панель выбора средств защиты (нижняя часть окна).

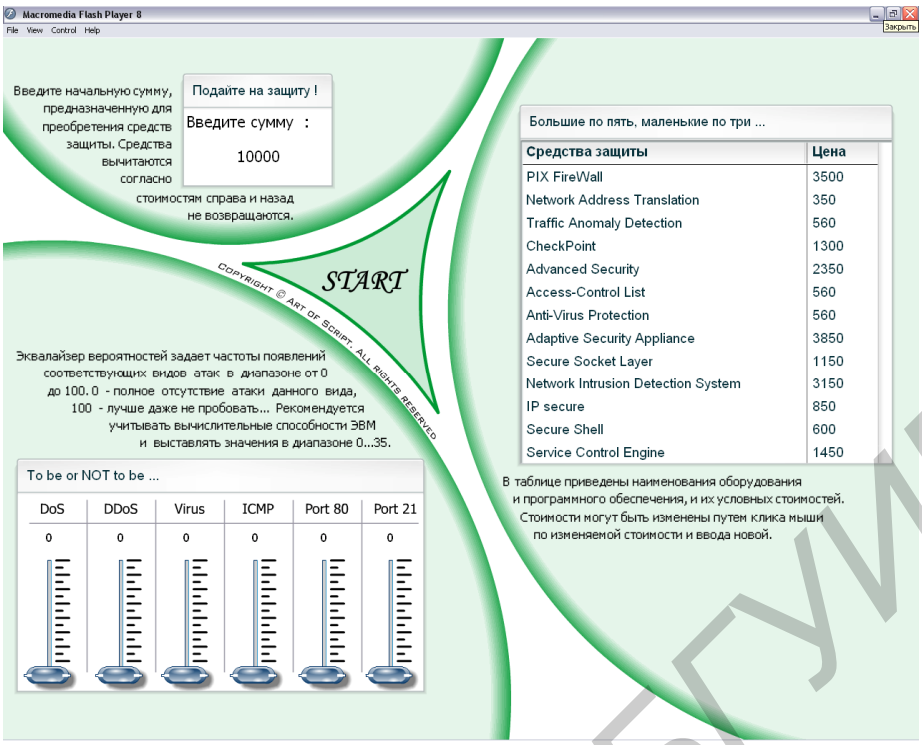

Рис. 2.2. Внешний вид главного окна программы

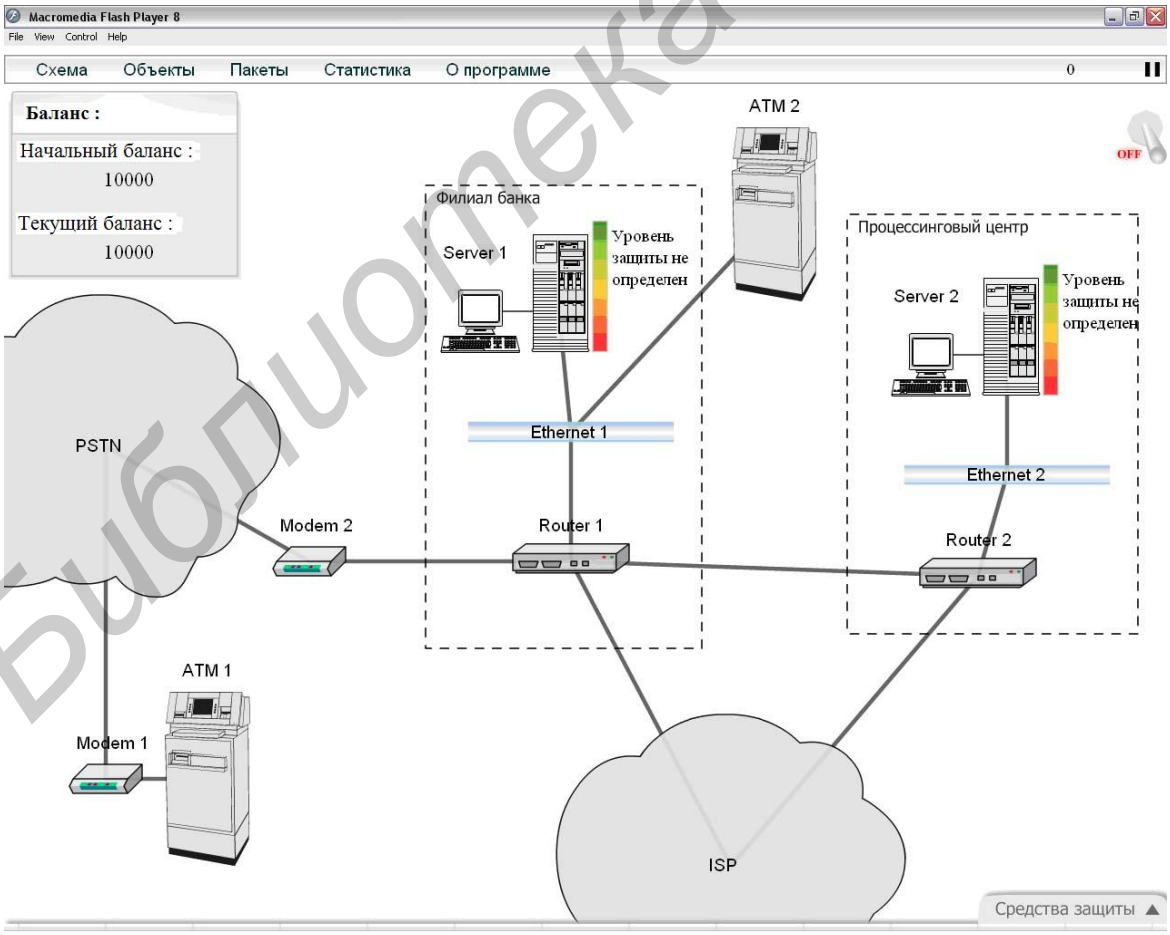

Рис. 2.3. Внешний вид рабочего окна программы

Меню «Схема»:

– пункт меню «Перемещения» включает/отключает режим перемещения объектов по схеме банковской сети (по умолчанию включен). При отключении возможно установление новых связей. Для этого необходимо подвести курсор мыши к объекту, соединение которого необходимо выполнить, и путем нажатия и удержания левой кнопки мыши подвести курсор к объекту, с которым нужно выполнить соединение, затем отпустить левую кнопку мыши;

– пункт меню «Показать связи» выводит на экран таблицу связей объектов. Символ «1» на пересечении столбца и строки, в которых указаны объекты, означает наличие связи между ними (рис. 2.4);

\	Server 1	Server 2	Router 1	Router 2	PSTN	ISP	Ethernet 1	Ethernet 2	ATM 1	ATM 2	Modem 1	Modem
Server 1	X						1					
Server 2		X						1				
Router 1			X	1		1	1					1
Router 2			1	X		1		1				
PSTN					X						1	1
ISP			1	1		X						
Ethernet 1	1		1				X			1		
Ethernet 2		1		1				X				
ATM 1									X		1	
ATM 2							1			X		
Modem 1					1				1		X	
Modem 2			1		1							X

Рис. 2.4. Внешний вид окна связей объектов банковской сети

– пункт меню «Добавить объект» вызывает окно добавления объекта (рис. 2.5).

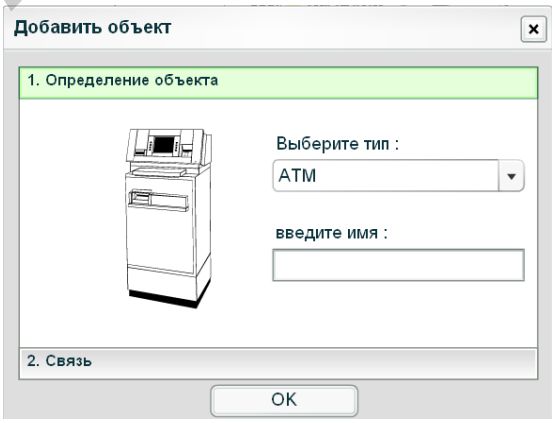

Рис. 2.5. Внешний вид окна добавления объекта банковской сети

Новые объекты могут быть добавлены при условии, что банковская сеть не функционирует, путем вызова окна добавления объектов через меню пользователя, либо нажатием правой кнопки мыши на белом фоне рабочего окна программы и выборе из контекстного меню пункта «Добавить объект».

При вызове контекстного меню объекта путем нажатия правой кнопки мыши на объекте возможно отправить пакет, выбрать окно свойств объекта или в случае выхода объекта из строя в результате атаки (объект помечается крестом красного цвета), выполнить его перезагрузку.

Меню «Объекты». Содержит перечень всех объектов банковской сети. Выбор объекта из данного перечня вызывает окно свойств данного объекта (рис. 2.6). В поле опции отображаются используемые средства защиты для выбранного объекта.

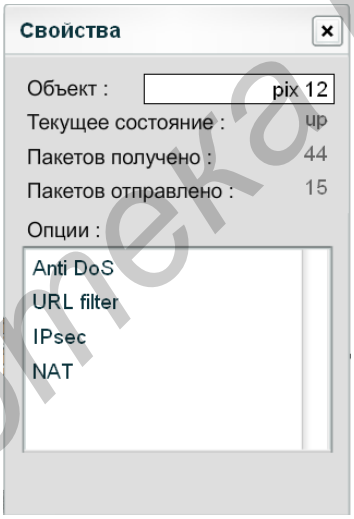

Рис. 2.6. Внешний вид окна добавления объекта банковской сети

Меню «Пакеты»:

– пункт меню «Отправить пакет» вызывает окно отправки пакета. Вначале необходимо указать объект-источник пакета, затем – получатель пакета и тип пакета (рис. 2.7);

– пункт меню «Случайность» включает/отключает режим случайной генерации пакетов объектами (работает при включенной банковской сети, по умолчанию включено).

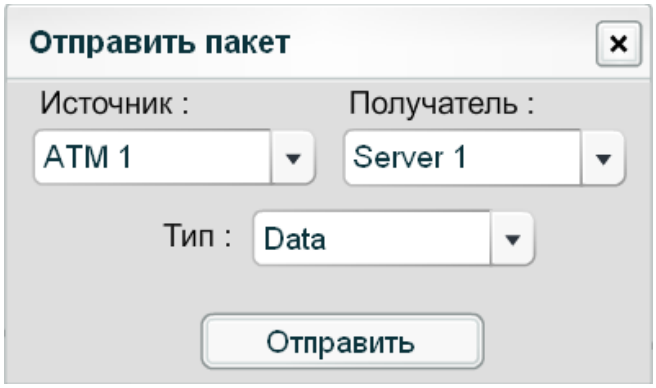

Рис. 2.7. Внешний вид окна отправки пакета

Типы используемых пакетов. В программе используются следующие типы пакетов: «Data», «Ping», «DoS», «DDoS», «Virus», «Port 80», «Port 21».

Пакеты типа «Data» используются при совершении платежей в обмене данными между банкоматом и серверами. При посылке банкоматом пакета этого типа включается тридцатисекундный таймер, по истечении которого платеж прекращается и считается не совершенным. Это происходит в случае выхода из строя сервера филиала банка. Кроме того, пакеты этого типа могут обладать двумя свойствами аутентификации и шифрования. Наличие этих свойств учитывается в общей статистике сети и определяется использованием в сети протоколов безопасности (SSH, IPsec).

Пакеты типа «Ping» используются в рамках атаки «ICMP». Данная атака имитирует сетевую разведку. Ее результаты отображаются в параметре статистики «Скрытие внутренней адресации». Ответ объекта атаки выглядит как пакет «Ping echo», не скрывающий своего адреса. При прохождении такого пакета через средства защиты с функцией «Network Address Translation – NAT» происходит скрытие адресации.

Пакеты «DoS» и «DDoS» участвуют в атаках «Отказ в обслуживании». Источник DoS-атаки генерирует некоторое случайное число пакетов, а источник DDoS-атаки выполняет «рассылку» пакетов другим объектам, которые в свою очередь выполняют уже отдельную DoS-атаку на объект. В случае успешной атаки объект выходит из строя, и дисплей центрального компьютера помечается крестом красного цвета. Для восстановления нормального режима функ-

ционирования центрального компьютера необходимо подвести указатель мыши к его системному блоку и нажать правую клавишу мыши. В выпавшем меню выбрать пункт «перезагрузка».

Атака «Virus» обладает замедленным действием, то есть при получении объектом пакета данного типа и отсутствии средства «Anti Virus Protection – AVP» включается таймер. По его истечении объект выходит из строя. Наличие таймера усложняет обнаружение и определение типа атаки на объект.

Пакеты типа «Port 80» и «Port 21» имитируют наиболее распространенный Интернет-трафик по протоколам HTTP и FTP соответственно. Данные пакеты посылаются рабочими станциями и сетями (PSTN – телефонная сеть общего пользования) и Интернет (ISP). Такие пакеты также нуждаются в шифровании и аутентификации посредством протокола SSL.

Меню «Статистика». Пункт меню «Показать статистику» вызывает окно статистики функционирования банковской сети (рис. 2.8). Нагрузка на Server 1 и Server 2, а также количество передаваемых пакетов в сети отображаются с шагом в 1 с.

Панель средств защиты. Содержит все доступные для использования средства защиты (рис. 2.9).

ACL (Access-Control list, список доступа) – программное средство, устанавливаемое на устройства третьего уровня модели OSI (маршрутизаторы, Pix, ASA, NIDS, TAD). Обеспечивает фильтрацию пакетов типов «Port 80» и «Port 21».

AVP (Anti Virus Protection, антивирусная защита) – программное средство и функция устройств седьмого уровня, препятствующее выходу из строя объекта защиты при вирусной атаке. Функция AVP включена по умолчанию на AS и SCE.

AS (Advanced Security) – аппаратное средство седьмого уровня модели OSI, имеющее следующие функции: «Anti DoS», «AVP», «SSH», «IPsec».

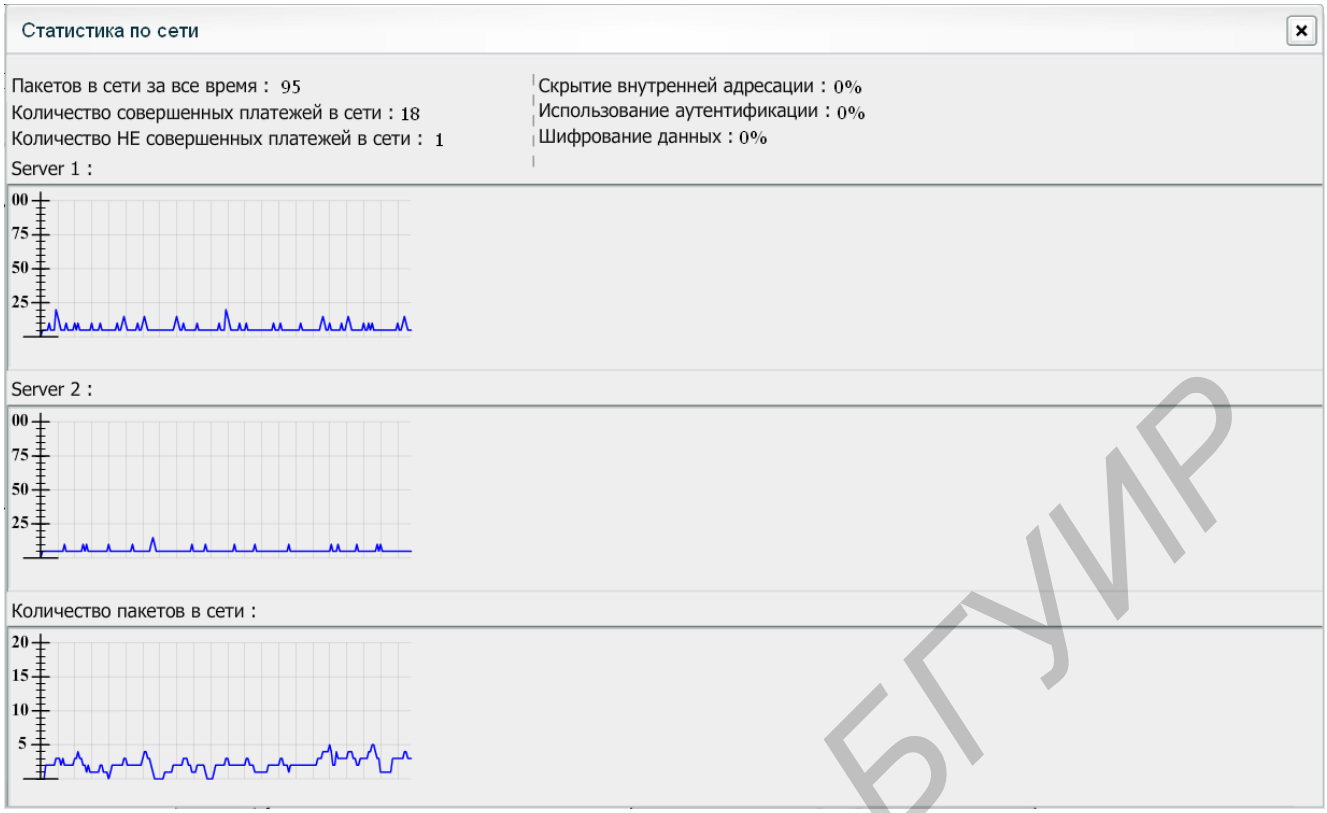

Рис. 2.8. Внешний вид окна статистики

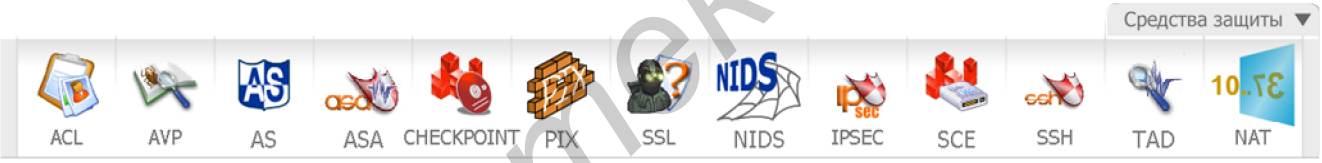

Рис. 2.9. Внешний вид панели средств защиты

ASA (Adaptive Security Appliance) – аппаратное средство третьего уровня модели OSI, имеющее следующие функции: «Anti DoS», «URL filter», «NAT». Функция «URL filter» заключается в фильтрации только пакетов типа «Port 80».

CheckPoint – программное средство, устанавливаемое на устройства седьмого уровня модели OSI и реализующее функцию «Anti DoS». Наличие этой функции на объекте защищает его от DoS-атак.

Pix (PIX FireWall, межсетевой экран) – аппаратное средство третьего уровня модели OSI, имеющее следующие функции: «Anti DoS», «URL filter», «IPsec», «NAT».

SSL – программное средство, устанавливаемое на устройства седьмого уровня модели OSI и обеспечивающее аутентификацию и шифрование пакетов, двигающихся через «облако» ISP.

NIDS (Network Intrusion Detection System, система обнаружения вторжений в сети) – аппаратное средство третьего уровня модели OSI, имеющее следующие функции: «Anti DoS», «SSH», «IPsec», «SSL».

IPsec (Secure IP) – программное средство и функция устройств третьего уровня модели OSI, обеспечивающее аутентификацию и шифрование пакетов.

SCE (Service Control Engine) – аппаратное средство седьмого уровня модели OSI, имеющее функции «Anti DoS» и «AVP».

SSH – программное средство и функция устройств седьмого уровня модели OSI, обеспечивающее аутентификацию и шифрование пакетов, исходящих от объекта.

TAD (Traffic Anomaly Detection) – аппаратное средство седьмого уровня модели OSI, имеющее функцию «Anti DoS».

NAT – функция устройств третьего уровня модели OSI, скрывающая адресацию пакетов типа «Ping».

2.3. Лабораторное задание

1. Запустить файл ZPS.exe на выполнение.

2. В соответствии с вариантом задания (см. приложение) настроить эквалайзер вероятностей и провести коррекцию начального баланса денежных средств. Подтвердить ввод данных нажатием кнопки «START».

3. Установить средства защиты в существующей конфигурации сети. Для этого открыть панель средств защиты путем позиционирования курсора мыши на закладке данных средств, которая находится в правой нижней части окна, и нажать левую кнопку мыши.

4. Выбор средства защиты осуществляется путем позиционирования курсора мыши на соответствующем средстве с последующим нажатием, и удержа-

нием левой кнопки мыши, и перетаскиванием выбранного объекта в место установки, которые отображаются на сети после нажатия левой кнопки мыши в виде прямоугольников.

5. После расстановки средств защиты активировать программу, включив переключатель, расположенный в верхнем правом углу окна, переведя его в положение «On».

6. Эффективность функционирования системы защиты определяется в соответствии с показателями, которые должны иметь следующие значения:

Показатель	Вариант		
	1	2	3
Уровень защиты процессингового центра и филиала банка	80 %	80 %	80 %
Скрытие внутренней адресации	100 %	40 %	30 %
Шифрование данных	3 %	2 %	-
Использование аутентификации	3 %	2 %	-
Количество совершенных платежей	15	15	15
Количество несовершенных платежей	1	1	1

Работа считается выполненной в том случае, если указанные показатели достигнуты.

7. Оформить отчет.

2.4. Содержание отчета

1. Цель работы.

2. Схема банковской сети с перечнем использованных средств защиты для каждого объекта.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

2.5. Контрольные вопросы

1. Что называется системой электронной коммерции?

2. Какие виды атак в данных системах наиболее вероятны?

3. Какие протоколы безопасности используют для защиты данных систем?

4. Дайте краткую характеристику каждому из протоколов.

5. Какие аппаратные средства защиты обеспечивают безопасность персональных платежей?

2.6. Приложение

Вариант	Вероятности возникновения атак						Начальный баланс
	DoS	DDoS	Virus	ICMP	Port 80	Port 21	
1	90	80	70	60	50	40	5100
2	80	70	60	50	40	30	4700
3	70	60	50	40	30	20	3000

Лабораторная работа №3

ЗАЩИТА УДАЛЕННЫХ БАНКОВСКИХ ТРАНЗАКЦИЙ

Цель работы: изучить принципы построения и функционирования электронных платежных систем, методы и способы защиты удаленных транзакций в них.

3.1. Теоретическая часть

Транзакция (англ. transaction) – группа последовательных операций, представляющая собой логическую единицу работы с данными. Транзакция может быть выполнена либо успешно при соблюдении целостности данных и вне независимости от параллельно идущих других транзакций, либо не выполнена вообще и эффект транзакции отсутствует.

3.1.1. Виды электронной коммерции

Электронная коммерция предполагает взаимодействие между партнерами с использованием информационных технологий, что существенно повышает гибкость, эффективность и масштабность бизнес-процессов. Электронная коммерция включает в себя не только операции, связанные с куплей-продажей товаров и услуг, но и операции, направленные на поддержку извлечения прибыли, создание спроса на товары и услуги, поддержку клиентов после продажи товаров и услуг и т. д.

Существуют различные приложения, которые обеспечивают новые бизнес решения, позволяющие улучшить качество товаров и предоставляемых услуг, повысить скорость обслуживания, снизить операционные издержки.

Новая методология ведения бизнеса имеет несколько сфер приложения:

– между различными видами бизнеса – сфера B2B (business-to-business);

– между бизнесом и потребителем – B2C (business-to-consumer);

– между потребителями – C2C (consumer-to-consumer);

– между бизнесом и государственными органами – B2A/B2G (business-to-administration/government);

– между государством и потребителями – A2C или G2C (administration/government-to-consumer);

– в рамках отдельного бизнеса, или Intra-business.

B2B – сфера электронной коммерции, в рамках которой компании осуществляют свою деятельность, начиная от выбора поставщика или продукта, процесса заказа товаров у поставщиков, получения счетов-фактур, до проведения платежей и других операций на основе использования сети передачи данных. Этот вид электронной коммерции характеризует взаимодействие между относительно постоянными партнерами, связанными единой цепочкой бизнес-процесса и интенсивным двухсторонним информационным обменом. Как правило, это долгосрочные отношения между крупными компаниями, а также между отдельными подразделениями компании. При этом вопрос взаимного недоверия стоит менее остро и может быть отрегулирован на начальном этапе взаимодействия обменом юридически значимыми подписанными документами. Примерами систем B2B являются международная система передачи банковской и финансовой информации (SWIFT).

B2C – данная сфера электронной коммерции является эквивалентом розничной торговли и представлена различными видами электронных магазинов с предложением спектра потребительских товаров. Этот вид электронной коммерции наиболее рискованный, поскольку деловые контакты между поставщиком и потребителем, как правило, ранее отсутствовали. Интернет-магазины, виртуальные банки – классические примеры систем B2C.

B2A – сфера электронной коммерции, которая охватывает все виды транзакций между компаниями и государственными организациями. Пока этот вид электронной коммерции находится в стадии зарождения, но имеет перспективы быстрого развития по таким направлениям, как возмещение налога на добавленную стоимость и уплата корпоративных налоговых платежей.

C2A – такая сфера существует пока только теоретически, ее рост связывают с различного рода выплатами социального назначения.

В основном электронная коммерция ассоциируется с покупкой и продажей информации, продуктов и услуг через Интернет. Концепция электронной коммерции строится не только на улучшении проведения транзакций, но и на строительстве устойчиво улучшающихся взаимоотношений с партнерами, клиентами как существующими, так и потенциальными.

3.1.2. Мобильная коммерция

Мобильная коммерция – продолжение развития сферы электронной коммерции, ее перевод в мобильные формы. С появлением электронной коммерции стало возможным совершить покупку, провести платеж, принять участие в аукционе, не отходя от компьютера, если только он подключен к Интернету. Мобильная же коммерция делает пользователя еще более независимым, не привязанным к стационарным устройствам, предоставляя все вышеперечисленные возможности при наличии одного только сотового телефона или карманного компьютера.

Мобильная коммерция способна создать немало удобств, которые будут по достоинству оценены всеми владельцами мобильных устройств. Так, телефон, сохраняя все свои прежние функции, становится еще и средством идентификации его владельца, позволяет получить доступ к банковскому карт-счету и т. д.

Наиболее распространенные устройства используемые для мобильной коммерции:

– PDA (Personal Digital Assistant) – портативный карманный компьютер. Это могут быть и умещающиеся на ладони бесклавиатурные устройства типа Palm и более дорогие устройства со встроенной клавиатурой, имеющие размеры среднего органайзера, и, наконец, средства, являющиеся уже скорее миниатюрными ноутбуками. Основные операционные системы – Palm OS, Windows CE или EPOC. Связь с Интернетом осуществляется через беспроводной модем

или посредством синхронизации с персональным компьютером, подключенным к телекоммуникационной сети;

– сотовый телефон с функцией WAP или собственным интернет-браузером;

– смартфон – устройство, выполняющее функции сотового телефона и PDA, совмещающее голосовые возможности телефона с функциями обработки и передачи данных, таких как электронная почта, выход в Интернет, работа с файлами и т. д.

Доступ в сеть Интернет может осуществляться с помощью беспроводного модема, встроенного WAP-браузера или путем синхронизации беспроводного устройства с устройством передачи данных, уже подключенным к сети Интернет.

Протокол WAP – результат совместной работы ассоциации WAP Forum, объединяющей производителей устройств и технологий мобильной связи, среди которых можно назвать Nokia, Ericsson, Motorola; телекоммуникационных операторов – Deutche Telecom, France Telecom, AT&T; компании-производителей программного обеспечения и провайдеров услуг – Microsoft, IBM, RSA, Unwired Planet, Symbian. Ассоциация объединяет более 500 членов, охватывает около 90 % рынка беспроводных устройств. Цель ассоциации – разработка единого открытого стандарта для обмена данными между беспроводными устройствами и Web-сервером.

Мобильная коммерция обладает рядом преимуществ по сравнению с классическими системами электронной коммерции:

– повсеместный доступ (в рамках сети оператора сотовой связи) к сети Интернет;

– локализация – такие технологии, как GPS (Global Positioning System), позволяют получить доступ к информации, относящейся именно к данному региону, например, предложения о покупке интересующего товара в близлежащих магазинах;

– персонализация – телефон является персональным устройством, по которому можно идентифицировать владельца.

Основным недостатком сотового телефона или смартфона является сравнительно небольшой размер экрана.

3.1.3. Интернет-коммерция

Использование торгового протокола IOTP (Internet Open Trading Protocol) в Интернет-коммерции позволило обеспечить широкий спектр услуг, начиная от торговых сделок и оплаты вплоть до доставки и послепродажного обслуживания, что сняло последние технические проблемы на пути внедрения торговли через сеть Интернет.

Открытый торговый протокол IOTP обеспечивает создание базы коммерции через Интернет и не зависит от используемой платежной системы. IOTP способен обрабатывать ситуации, когда продавец выступает в качестве покупателя, обеспечивает оформление и отслеживание доставки товаров и прохождения платежей, или совмещает некоторые или все перечисленные функции.

Использование Интернет-коммерции привносит огромные изменения в сферу бизнеса, политики, управления и в само общество. Методы, которые реализуются партнерами в торговле, обогатились и необратимо изменились. Наиболее заметные изменения характера торговли включают в себя:

– присутствие в офисе банка – операции, требующие личного контакта, становятся исключением, а не правилом;

– аутентификация. Важной частью личного присутствия является возможность партнеров использовать знакомые объекты и диалог для подтверждения того, кем они являются. Продавец демонстрирует различными способами свою способность производить кредитные и платежные операции. Покупатель предъявляет физические свидетельства своей платежеспособности, полученные от государства или финансовой организации. При этом учитывается разнообразная объективная информация: местоположение магазина, внешность, зна-

комство и поведение участников, знакомство с данной фирмой и ее торговым знаком;

– инструменты платежа. Несмотря на широкое развитие безналичных платежей, заметная часть торговых операций обеспечивается наличными деньгами или даже бартером. Существующая инфраструктура платежной системы по экономическим соображениям не может поддерживать операции с низкими суммами платежей, но и не может от них отказаться;

– стоимость операций. Новое значение низкой стоимости операции в Интернет связано с возможностью того, что продавец может предложить, например, объекты с ценой, составляющей долю денежной единицы, которой не существует при расчете наличными;

– доставка. Внедряются новые методы доставки, включая доставку с использованием сети Интернет, например, информации или программных продуктов. Возможна доставка по частям при играх, просмотре, прослушивании и некоторых других виртуальных услугах, при этом она должна быть подтверждена до осуществления платежа. Деньги в этом случае не возвращаются.

Существует несколько преимуществ использования протокола IOTP для продавцов:

– возможность предложить широкий перечень видов платежей;

– возможность быть уверенными, что покупатель будет иметь программу, необходимую для осуществления покупки;

– при получении платежа и расписки от покупателя о получении товара или услуги они смогут обеспечить клиента гарантией, что он имел дело именно с тем человеком или организацией.

Преимущества протокола IOTP для банков и финансовых организаций:

– предоставление услуг для продавцов;

– поиск новых способов для реализации услуг, сопряженных с IOTP:

– предоставление услуг клиентам продавцов;

– деньги от обработки новых платежей и депозитов;

– возможность построения отношений с новыми продавцами.

Преимущества использования протокола IOTP для покупателей:

– большой выбор продавцов, с которыми можно иметь дело;

– удобный интерфейс для осуществления покупки;

– существуют возможности уладить проблемы купли-продажи через продавца не обращаясь в банк;

– существует запись операций, которая может использоваться, для дальнейшего декларирования данной информации по купле-продаже товаров в налоговую службу.

Платежные системы, которые поддерживает IOTP, следующие: MasterCard Credit, Visa Credit, Mondex Cash, Visa Cash, GeldKarte, eCash, CyberCoin, Millicent, Proton и т. д.

Каждая система содержит некоторый обмен сообщениями, который является характерным именно для нее. Протокол IOTP не конкретизирует, какое именно следует использовать программное обеспечение или процесс для обеспечения финансового взаимодействия. Он определяет только необходимые рамки, в пределах которых реализуется торговая операция.

3.1.4. Угрозы безопасности удаленных банковских транзакций

Несанкционированный доступ (НСД) – заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности.

Способы НСД:

– преодоление системы защиты путем различных воздействий на нее;

– незаконное использование привилегий доступа к данным.

Атаки «салями» характерны для систем, обрабатывающих данные о денежных средствах. Атаки «салями» построены на том, что при обработке счета используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы.

Причинами атак «салями» являются, во-первых, погрешности вычислений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений, необходимые для обработки счетов. Успех таких атак зависит не столько от величины обрабатываемых сумм, сколько от количества счетов (для любого счета погрешность обработки одинакова). Атаки «салями» достаточно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете значительные денежные средства. Предотвратить такие атаки можно только обеспечением целостности и корректности прикладных программ, обрабатывающих счета, разграничением доступа пользователей автоматизированной банковской системы (АБС), а также контролем счетов.

«Скрытые каналы» – пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может использовать для этого обходные пути. Практически любое действие в системе каким-то образом затрагивает другие ее элементы, которые при этом могут изменять свое состояние. При достаточной наблюдательности и знании этих связей можно получить прямой или опосредованный доступ к данным. «Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»).

Атаки с использованием скрытых каналов обычно приводят к нарушениям конфиденциальности информации в АБС, по характеру воздействия являются пассивными: нарушение состоит только в передаче информации. Для организации «скрытых каналов» может использоваться как штатное программное обеспечение, так и специально разработанные «троянские» или вирусные программы.

Под ***«маскарадом»*** понимается выполнение каких-либо действий одним пользователем АБС от имени другого пользователя. При этом такие действия

другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Цель «маскарада» – сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий. «Маскарад» является способом активного нарушения защиты системы и опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей. «Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть различные, обычно они определяются ошибками и особенностями сетевых протоколов.

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к огромным убыткам. Особенно это касается платежей с помощью электронных пластиковых карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери пластиковой карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т. д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей. Кроме того, для предотвращения «маскарада» необходимо использовать надежные методы идентификации и аутентификации, блокировку попыток взлома системы, контроль входа в нее. Также необходимо фиксировать все события в системном журнале для его последующего анализа.

«Сборка мусора». После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя прочитать та-

кие данные трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс принято называть «сборкой мусора». Он может привести к утечке конфиденциальной информации.

Для защиты от «сборки мусора» используются специальные механизмы, которые могут быть реализованы в операционной системе и/или аппаратуре компьютера или в дополнительных программных (аппаратных) средствах. Примерами таких механизмов являются стирающий образец и метка полноты:

– стирающий образец – некоторая последовательность битов, записываемая на место, освобождаемое файлом;

– метка полноты – предотвращает чтение участков памяти, отведенных процессу для записи, но не использованных им. Верхняя граница адресов использованной памяти и есть метка полноты. Этот способ используется для защиты последовательных файлов исключительного доступа (результирующие файлы редакторов, компиляторов, компоновщиков т. д.). Для индексных и разделяемых последовательных файлов этот метод называется «стирание при размещении», память очищается при выделении ее процессу.

Под ***«взломом системы»*** понимают умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем (паролями).

Поскольку имя пользователя не является секретом, объектом атаки обычно становится пароль. Способы вскрытия пароля могут быть различны: перебор возможных паролей, «маскарад» с использованием пароля другого пользователя, захват привилегий. Кроме того, «взлом системы» можно осуществить, используя ошибки программы входа.

Таким образом, основную нагрузку на защиту системы от «взлома» несет программа входа. Алгоритм ввода имени и пароля, их шифрование (при необходимости), правила хранения и смены паролей не должны содержать ошибок. Противостоять «взлому системы» также поможет, например, ограничение ко-

личества попыток неправильного ввода пароля с последующей блокировкой терминала и уведомлением администратора о случае нарушения.

Кроме того, администратор должен постоянно контролировать активных пользователей системы: их имена, характер работы, время входа и выхода и т. д. Такие действия помогут своевременно установить факт «взлома» и позволят предпринять необходимые действия.

«Люк» – скрытая, недокументированная точка входа в программный модуль, которая встраивается в программу обычно на этапе отладки для облегчения работы: программный модуль можно вызывать в разных местах, что позволяет отлаживать отдельные его части независимо одна от другой. Но в дальнейшем программист может забыть удалить «люк» или некорректно его заблокировать. Кроме того, «люк» может вставляться на этапе разработки для последующей связи данного модуля с другими модулями системы, но затем в результате изменившихся условий данная точка входа оказывается ненужной. «Люк» относится к категории угроз, возникающих вследствие ошибок реализации какого-либо проекта (АБС в целом, комплекса программ и т. д.).

«Троянский конь» — программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Программы такого типа являются серьезной угрозой безопасности АБС.

По характеру угрозы «троянский конь» относится к активным угрозам, реализуемым программными средствами, работающими в пакетном режиме. Он может угрожать любому объекту АБС. Наиболее опасным является опосредованное воздействие, при котором «троянский конь» действует в рамках полномочий одного пользователя, но в интересах другого пользователя, установить личность которого порой невозможно.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователям АБС. Этот блок команд может срабатывать при наступлении некоторого усло-

вия (даты, времени и т. д. либо по команде извне). Запустивший такую программу подвергает опасности как себя и свой файлы, так и всю АБС в целом.

«Троянский конь» – одна из наиболее опасных угроз безопасности АБС. Радикальным способом защиты от этой угрозы является создание замкнутой среды исполнения программ. В особенности важно разделение внешних сетей (особенно Интернет) и внутренних сетей, по крайней мере, на уровне протоколов, а еще лучше – на физическом уровне. Желательно также, чтобы привилегированные и непривилегированные пользователи работали с разными экземплярами прикладных программ, которые должны храниться и защищаться индивидуально. При соблюдении этих мер вероятность внедрения программ подобного рода будет достаточно низкой.

Вирус – программа, которая может изменять другие программы, используемые пользователем, путем включения в них своей, возможно, модифицированной копии, причем последняя сохраняет способность к дальнейшему размножению. Вирус может быть охарактеризован двумя основными особенностями:

– способность к самовоспроизведению – за время своего существования на компьютере вирус должен хотя бы один раз воспроизвести свою копию на долговременном носителе;

– способность к вмешательству (получению управления) в вычислительный процесс. Это свойство является аналогом «паразитирования» в живой природе, которое свойственно биологическим вирусам.

Вирусы относятся к активным программным средствам. Классификация вирусов, используемые ими методы заражения, способы борьбы с ними достаточно хорошо изучены и описаны.

«Червь» – программа, распространяющаяся через локальную или глобальную сеть и (в отличие от вируса) не оставляющая своей копии на долговременном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механиз-

мов передает свое тело или его часть на этот узел и активизируется или ждет для этого подходящих условий.

Перехватчики паролей. Программы специально предназначены для несанкционированного получения паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-перехватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, воспринимая данную ситуацию как ошибку набора пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-перехватчика. Перехват пароля может осуществляться и другим способом – с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

3.1.5. Основные требования обеспечения безопасности удаленных банковских транзакций

С технической точки зрения проблемы защиты удаленных транзакций решаются с помощью нескольких механизмов, отвечающих за обеспечение адекватной безопасности АБС. Работа большинства этих механизмов обеспечивается службами сети с расширенным набором услуг (Value-Added Network – VAN). Службы, реализующие обмен электронными данными, должны выполнять следующие функции:

– защита от случайных и умышленных ошибок;

– адаптация к частым изменениям количества пользователей, типов оборудования, способов доступа, объемов трафика, топологии;

– поддержка различных типов аппаратного и программного обеспечения, поставляемого различными производителями;

– осуществление управления и поддержка сети для обеспечения непрерывности работы и быстрой диагностики нарушений;

– реализация полного спектра прикладных задач электронного обмена данными, включая электронную почту;

– реализация максимально возможного числа требований партнеров;

– включение службы резервного копирования и восстановления после аварий.

В системах обмена электронными документами должны быть реализованы следующие механизмы, обеспечивающие реализацию функций защиты на отдельных узлах системы и на уровне протоколов высокого уровня:

– равноправная аутентификация абонентов;

– невозможность отказа от авторства сообщения (приема сообщения);

– контроль целостности сообщения;

– обеспечение конфиденциальности сообщения;

– управление доступом на оконечных системах;

– гарантии доставки сообщения;

– невозможность отказа от принятия мер по сообщению;

– регистрация последовательности сообщений;

– контроль целостности и последовательности сообщений;

– обеспечение конфиденциальности потока сообщений.

Полнота решения проблем защиты обмена электронными документами сильно зависит от правильного выбора системы шифрования. Система шифрования представляет собой совокупность алгоритмов шифрования и методов распространения ключей. Правильный выбор системы шифрования помогает:

– скрыть содержание документа от посторонних лиц (обеспечение конфиденциальности документа) путем шифрования его содержимого;

– обеспечить совместное использование документа группой пользователей системы обмена электронными данными путем криптографического разделения информации и соответствующего протокола распределения ключей;

– своевременно обнаружить искажение, подделку документа (обеспечение целостности документа) путем введения криптографического контрольного признака;

– удостовериться в том, что абонент, с которым происходит взаимодействие в сети, является именно тем, за кого он себя выдает (аутентификация абонента/источника данных).

Следует отметить, что при защите систем обмена электронными данными большую роль играет не столько шифрование документа, сколько обеспечение его целостности и аутентификация абонентов (источника данных) при проведении сеанса связи. Поэтому механизмы шифрования в таких системах играют обычно вспомогательную роль.

Для предотвращения проникновения в систему безопасности используются следующие средства защиты:

– шифрование содержимого документа;

– контроль авторства документа;

– контроль целостности документа;

– нумерация документов;

– ведение сессий на уровне защиты информации;

– динамическая аутентификация;

– обеспечение сохранности секретных ключей;

– надежная процедура проверки клиента при регистрации в прикладной системе;

– использование электронного сертификата клиента;

– создание защищенного соединения клиента с сервером.

Также необходимо применять комплекс технических средств защиты Интернет-сервисов:

– брандмауэр (межсетевой экран);

– системы обнаружения атак;

– антивирусные средства;

– защищенные операционные системы, обеспечивающие уровень B2 («Оранжевая книга») и дополнительные средства контроля целостности программ и данных;

– защита на уровне приложений: протоколы безопасности, шифрования, электронно-цифровая подпись (ЭЦП), цифровые сертификаты, системы контроля целостности;

– защита средствами системы управления базами данных;

– защита передаваемых по сети компонентов программного обеспечения;

– мониторинг безопасности и выявление попыток вторжения, адаптивная защита сетей, активный аудит действий пользователей;

– обманные системы;

– корректное управление политикой безопасности.

Для проведения безопасных банковских транзакций должны выполняться:

– аутентификация документа при его создании;

– защита документа при его передаче;

– аутентификация документа при обработке, хранении и исполнении;

– защита документа при доступе к нему из внешней среды.

3.1.6. Технология удаленной банковской транзакции

Эмитент – организация, обеспечивающая выпуск пластиковых карт и гарантирующая выполнение финансовых обязательств, связанных с использованием выпущенной им пластиковой карты как платежного средства.

Эквайрер – организация, которая реализует выполнение необходимых операций по обеспечению взаимодействия участников обслуживания средствами платежной системы.

Рассмотрим механизм организации платежа при условии, что держатель пластиковой карты предварительно должен зарегистрироваться на сервере авторизации платежной системы, например CyberPlat (Россия) (рис. 3.1).

Регистрация в платежной системе требует введения следующих данных:

1. Персональные данные (фамилия, имя, отчество, паспортные данные, адрес электронной почты, телефон, почтовый адрес);

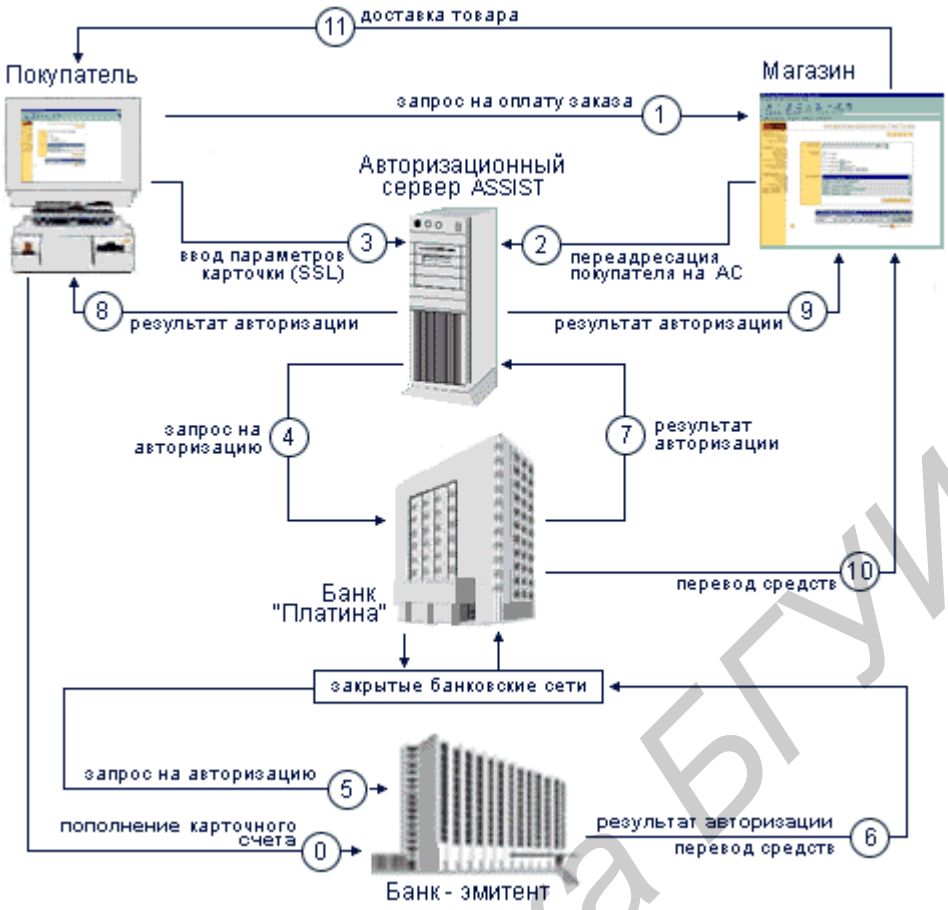

Рис. 3.1. Схема оплаты товара или услуги для пользователя, зарегистрированного на сервере авторизации

2. Параметры пластиковой карты (название платежной системы, к которой она принадлежит, номер, дата окончания действия, имя держателя в той транскрипции, как оно написано на карте).

Информация о карте передается в защищенном виде только в Банк при регистрации Покупателя и не предоставляется каким-либо иным участникам процесса.

Технология покупки товаров в Магазине Пользователем следующая:

1. Покупатель через Интернет подключается к web-серверу Магазина, формирует корзину товаров и направляет Магазину запрос на выставление счета.

2. Магазин в ответ на запрос Покупателя направляет ему подписанный своей ЭЦП счет, в котором указывает: наименование товара (услуги), стоимость товара (услуги), код магазина, время и дату совершения операции.

3. С гражданско-правовой точки зрения этот счет является предложением заключить договор (офертой).

4. Покупатель подписывает своей ЭЦП предъявленный ему счет и отправляет его обратно в Магазин, совершая тем самым акцепт. Договор считается заключенным с момента подписания Покупателем выставленного ему счета. В данной системе счет, подписанный Покупателем, становится чеком.

5. Подписанный двумя ЭЦП (Магазином и Покупателем) чек направляется Магазином в Банк для авторизации.

6. Банк производит обработку подписанного чека: проверяет наличие в Системе Магазина и Покупателя; проверяет ЭЦП Покупателя и Магазина; проверяет соответствие операции на установленные системные лимиты; сохраняет копию чека в базе данных Банка.

7. В результате проверок формируется разрешение или запрет проведения авторизации транзакции в карточную платежную систему.

8. При запрете авторизации Банк передает Магазину отказ от проведения платежа; Покупатель получает отказ с описанием причины.

9. При разрешении авторизации в соответствии с договором между Банком и Покупателем Банк увеличивает сумму оплаты на величину своей комиссии. Виды и размер комиссии определяются действующими тарифами Банка. Запрос на авторизацию передается через закрытые банковские сети банку-эмитенту карты Покупателя или процессинговому центру карточной платежной системы, уполномоченному банком-эмитентом.

10. При положительном результате авторизации, полученном от карточной платежной системы, Банк передает Магазину разрешение на оказание услуги (отпуск товара); Магазин оказывает услугу (отпускает товар). Банк осущест-

вляет перечисление средств на счет Магазина в соответствии с существующими договорными отношениями между Банком и Магазином.

11. При отказе авторизации Банк передает Магазину отказ от проведения платежа; покупатель получает отказ с описанием причины. Покупатель полностью контролирует процесс совершения покупки.

3.2. Лабораторное задание

Построить схему оплаты товара или услуги для пользователя, зарегистрированного на сервере авторизации.

Схема построения:

1. Запустить файл ZUBT.exe на выполнение.

2. Переход к изучению теоретического материала выполняется путем нажатия на кнопку «Теория», расположенную в верхнем левом углу окна (рис. 3.2). Выход из режима изучения теоретического материала осуществляется нажатием на кнопку «Выход».

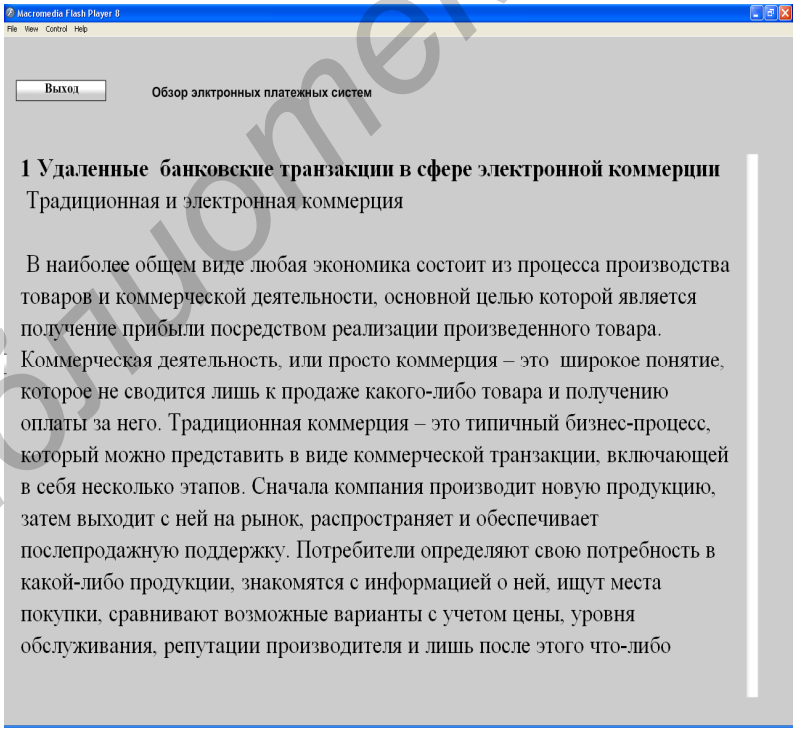

Рис. 3.2. Внешний вид окна теории

3. В работе предусмотрено пошаговое выполнение задания с проверкой правильности выполнения каждого шага. Для этого необходимо в левой части

окна на каждом шаге отметить субъектов взаимодействия путем их выбора по одному из каждой колонки и нажатием на кнопку «Проверить» (рис. 3.3). В случае ошибки – выводиться соответствующее сообщение, после чего показания счетчика ошибок будут увеличиваться на единицу.

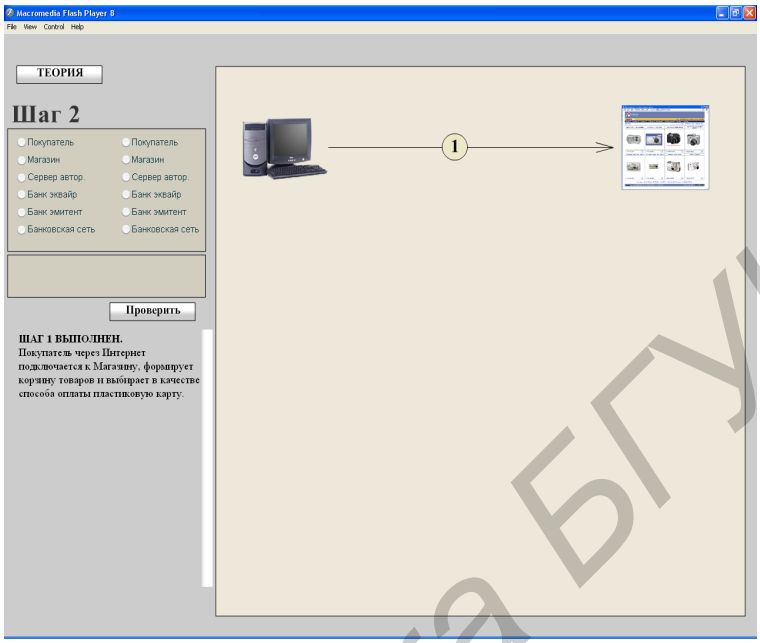

Рис. 3.3. Внешний вид рабочего окна программы

4. После того как все задание будет выполнено, необходимо ответить на вопросы теста. Для этого левой части экрана в меню выбора необходимо будет выбрать правильные варианты ответов на поставленный вопрос (рис. 3.4).

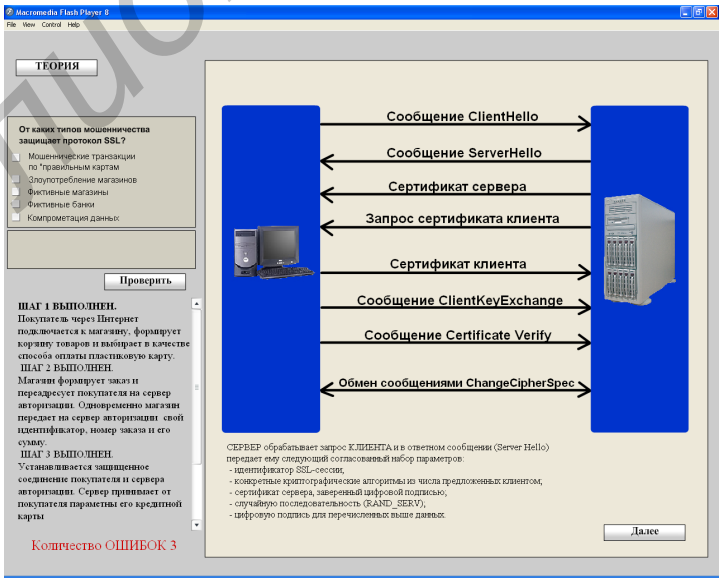

Рис. 3.4. Внешний вид окна программы с контрольными вопросами

5. Лабораторная работа считается выполненной при отсутствии допущенных ошибок.

6. Результаты выполнения работы показать преподавателю.

7. Оформить отчет.

3.3. Содержание отчета

1. Цель работы.

2. Схема оплаты товара или услуги для пользователя, зарегистрированного на сервере авторизации.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

3.4. Контрольные вопросы

1. Какие типы электронной коммерции существуют на данный момент времени?

2. Какие преимущества для продавца обеспечивает применение протокола IOTP?

3. В чем заключается особенность информационной безопасности для банковской сферы?

4. Какие угрозы информационной безопасности могут нанести максимальный ущерб банковской сфере?

5. Какие преимущества обеспечивает применение сервера авторизации в электронной платежной системе?

Лабораторная работа №4

ЗАЩИТА АВТОМАТИЧЕСКИХ КАССОВЫХ АППАРАТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Цель работы: изучить методы и средства защиты автоматических кассовых аппаратов от несанкционированного доступа.

4.1. Теоретическая часть

4.1.1. Классификация угроз

Угрозы безопасности автоматических кассовых аппаратов (банкоматов) принято классифицировать по элементам системы взаимодействия «пользователь – банкомат».

Таблица 4.1

Классификация угроз

Угрозы направленные	Ущерб
1	2
На карту и/или ее реквизиты	– кибератака; – заклинивание карты в карт-ридере с целью ее дальнейшего незаконного изъятия; – подмена или присвоение карты незаметно для держателя после выполнения операции в банкомате; – копирование магнитной полосы карты (скимминг); – фальшивые банкоматы; – запись тональных сигналов при наборе PIN-кода, которые далее расшифровываются; – скрытые видеокамеры; – увеличительные оптические приборы; – криптографические атаки; – модификация или неавторизованный доступ в систему банкоматов; – подглядывание через плечо.

Окончание табл. 4.1

1	2
На держателей карты	– ограбление держателя карты при получении или внесении денежных средств; – получение держателем карты денежных средств под принуждением со стороны злоумышленника.
На банкомат-технологию	– нарушение целостности, конфиденциальности или доступности системы (технологии) АТМ посредством несанкционированного кибервторжения; – вредоносное программное обеспечение.
На денежные средства	– хищение денежных средств путем монтажа дополнительных устройств на механизм выдачи купюр; – взлом сейфа банкомата с целью хищения денежных средств; – хищение банкомата вместе с денежными средствами; – ограбление при инкассации; – мошенничество со стороны легитимных держателей карт.

Угрозы, направленные на денежные средства. Физическое нападение – взлом, попытки разбить и достать денежные средства из банкомата – могут быть осуществлены различными способами. Наиболее распространены попытки нанести повреждения с целью проникнуть внутрь устройства и изъять кассеты с деньгами путем механического либо термического воздействия на аппарат.

Попытки протаранить либо увезти банкомат с места его расположения относятся к категории нападений с применением грубой силы и также имеют целью получение доступа к содержимому денежных ящиков. Достаточно широко известны попытки преступников сорвать банкомат с креплений посредством грузовиков, бульдозеров, экскаваторов либо погрузчиков.

Угрозы, направленные на карту и/или ее реквизиты. Основной угрозой является скимминг, которая осуществляется в несколько этапов, конечным результатом которых является получение наличных денежных средств по поддельным картам – «белому пластику». Данная угроза характерна только для магнитных карт.

Скимминг (от англ. skim – снимать) – вид мошенничества, осуществляемый при помощи электронного устройства (скиммера), устанавливаемого на банкомат для считывания информации с пластиковых карт, а также накладной клавиатуры или миниатюрной видеокамеры, с помощью которых мошенники регистрируют PIN-код, вводимый владельцем карты при его аутентификации. Скиммеры имеют внутреннюю память и могут хранить до двух тысяч реквизитов пластиковых карточек. Все считываемые данные имеют метку времени: год, месяц, день, час, минута, секунда. Считывание дорожки происходит как при захвате карты карт-ридером, так и при ее возврате. Внешний вид скиммера приведен на рис. 4.1.

а б

Рис. 4.1. Внешний вид скиммера: а – банкомат без скиммера; б – банкомат с установленным скиммером

На рис. 4.2 изображена накладная пользовательская клавиатура (PIN-PAD), с помощью которой мошенник получает PIN-код, вводимый легитимным держателем пластиковой карты. Мошенник может узнать персональный PIN-код держателя банковской карты, не прибегая к помощи накладной клавиатуры или камеры, а подглядывая из-за его плеча. Также могут использоваться специальные оптические приборы.

Рис. 4.2. Внешний вид накладного PIN-PAD

Осуществляется данное мошенничество обычно по одной схеме. Выбираются банкоматы, расположенные в местах большого скопления людей, где легко можно это устройство как установить, так и демонтировать. Устройство ставиться на непродолжительный промежуток времени (несколько часов).

С теми же целями мошенники могут устанавливать фальшивые банкоматы, которые записывают всю информацию о карточке и PIN-коде, но наличных денег не выдают.

Существует еще один метод мошенничества, направленный на карту пользователя, – «ливанская петля». В прорезь карт-ридера банкомата вставляется отрезок фотопленки, концы которого укрепляются на внешней стороне устройства считывания. Фотопленка не дает возможность карте быть возвращенной карт-ридером. Мошенник, находящийся неподалеку, предлагает владельцу карты свою помощь. Он рекомендует владельцу карты вновь ввести свой PIN-код, говоря, что такие случаи случались уже раньше и при повторном введении PIN-кода карта должна быть возвращена. Таким образом, мошенник узнает PIN-код карточки, а ее владельцу советует придти на следующий день в банк (мошенничество проводится в то время, когда отделение банка уже не работает), и карта ему будет возвращена. Затем мошенник извлекает пленку вместе с картой из банкомата и снимает со счета владельца карты все денежные средства.

Также мошенник может ставить специальное приспособление на устройство выдачи купюр, которое препятствует их выдаче. После того как владелец карты, не дождавшись запрошенной суммы, уходит, мошенник снимает устройство вместе с невыданными деньгами.

Угрозы, направленные на банкомат-технологию. Еще одной важной проблемой безопасности АКА является проблема несанкционированного подключения к линии связи между банкоматом и процессинговым центром. Данный вид угрозы весьма сложен по осуществлению: он требует определенных знаний, узкоспециального программного обеспечения и технического оборудования. Приведем схему действий преступника при такой атаке.

Преступник подключается к линии связи между банкоматом и процессинговым центром, причем делается это в разрыв кабеля так, чтобы в дальнейшем можно было не только перехватывать, но и блокировать любые проходящие пакеты. Подключение происходит с использованием электронных схем мгновенной коммутации «на ходу».

Далее злоумышленник наблюдает за пересылкой пакетов, не предпринимая никаких действий, чтобы понять логику передачи трафика. Анализируются протоколы, расшифровываются все поля заголовков пакетов для того, чтобы в дальнейшем иметь возможность генерации и отправки собственных пакетов.

Далее злоумышленник манипулирует легальной картой с тем, чтобы понять логику обмена. В частности, найти и опознать передаваемые банкоматом запросы и приходящие ему ответы. Все это сравнивается с просроченной картой, чтобы определить реакцию системы в такой ситуации, а также найти и идентифицировать коды ошибок.

На следующем шаге начинается непосредственная фальсификация передающихся сведений. В банкомат вставляется действующая карточка. Посылается запрос в процессинговый центр, который возвращает ответ, в котором содержится вся требуемая информация. Перехватывается пакет со сведениями о максимально возможной сумме для получения наличных, и взамен него посы-

лается пакет с измененной суммой. Эта сумма может присутствовать сразу в нескольких полях, кроме этого, корректируется и поле контрольной суммы.

Далее происходит получение суммы наличных денег, не превышающей измененную сумму. В это время банкомат передает банку, сколько денег было получено клиентом. Эта информация перехватывается и посылается ложный пакет, содержащий информацию о том, что полученная сумма не превышает баланс счета. Так как в банкомате ведется протоколирование всех проведенных операций, злоумышленнику необходимо обеспечить сходимость дебета и кредита.

Необходимо заметить, что предварительный этап, включающий в себя анализ трафика и кодов ошибок, весьма продолжителен по времени. Это объясняется тем, что данные шифруются.

Вредоносное программное обеспечение. Главная причина вирусных атак – человеческий фактор, то есть непрофессионализм обслуживающего и технического персонала банка. Причем стоит отметить, что вредоносное программное обеспечение не может нанести банкомату повреждения или выполнять какие-либо манипуляции со счетом владельца пластиковой карты (если, конечно, затронутыми не оказываются центральные серверы банковских систем). Они являются причиной простоев банкоматов, которые наносят убытки.

4.1.2. Обеспечение безопасности автоматических кассовых аппаратов

Физическая безопасность. Определяется прежде всего местом его расположения. Согласно своду рекомендаций по физической защите банкоматов Всемирного альянса по вопросам обеспечения безопасности банкоматов (Global ATM Security Alliance), выбор места и способа установки терминалов должен предваряться расчетами рисков с учетом следующих соображений:

– безопасность обслуживающих работников и пользователей банкоматов, а также находящихся в зоне размещения банкоматов граждан;

– криминальная обстановка в месте размещения банкоматов.

При планировании места размещения банкомата необходимо учитывать следующие возможные факторы:

– общую обстановку на объекте размещения банкомата – условия освещения, близость различных общественных служб, хорошую видимость банкоматов с подъездных путей;

– точную схему размещения банкоматов на объекте, выбранном для установки;

– имеются ли на объекте охранные службы и технические средства безопасности;

– схему пополнения запасов наличных денег – за счет торговой точки, где установлен банкомат, либо с применением централизованного инкассаторского сервиса.

Для обеспечения защиты уже установленных аппаратов предлагается разработанный специалистами отрасли набор рекомендаций по снижению риска нападения на банкоматы:

– банкоматы должны встраиваться в стену здания банка либо иного капитального дома;

– вокруг банкомата необходимо разместить различные физические препятствия для ограничения подъезда автомобилей;

– необходимо усовершенствование старых либо установка новых осветительных приборов вблизи банкомата;

– вокруг каждого банкомата должны устанавливаться сразу несколько камер видеонаблюдения таким образом, чтобы можно было наблюдать крупные планы лиц, номерные знаки, цвета, модели и особые приметы подъезжающих автомобилей;

– для отслеживания местоположения банкоматов на случай их похищения желательно на каждый из них установить маяки слежения, связанные с системой глобального позиционирования (GPS);

– в конструкцию банкоматов возможно встраивание системы нанесения меток на банкноты – к примеру, путем их окрашивания – по команде системы локальной охранной сигнализации, вызванной вибрацией, опрокидыванием банкомата и тому подобными методами воздействия; такие системы заливают купюры чернилами, делая предмет ограбления непривлекательным для присвоения;

– необходимо использовать все детали рельефа местности для ограничения подъезда к месту расположения банкомата крупногабаритной строительной техники.

Основные требования к безопасности функционирования банкоматов разделяются на две группы. Первая касается помещений, выделенных для зоны самообслуживания, вторая – зоны загрузки банкомата. Если банкомат предполагается использовать во время работы учреждения, то можно выбрать более простую модель с передней загрузкой. Если же банкомат предназначен для работы в круглосуточном режиме, то целесообразно остановиться на модели, встраиваемой в капитальную стену здания и имеющей заднюю загрузку, которая осуществляется в специально отведенном и защищенном помещении.

Требования к зоне самообслуживания банкомата, установленного в помещении с выходом на улицу, следующие:

– помещение для зоны самообслуживания выбирается таким образом, чтобы обеспечить удобство пользователя и хорошую просматриваемость подходов к банкомату;

– выступающие наружу ограждающие конструкции зоны и наружные двери выполняются, как правило, с использованием стекол, защищенных полимерными пленками, или триплекса, соответствующих классу защиты не ниже А2;

– наружная дверь для входа клиентов должна быть повышенной прочности и обеспечивать защиту от несанкционированного проникновения и взлома. Рекомендуется применять металлические двери, имеющие категорию и класс

не ниже У1, или остекленные с применением защитного остекления класса защиты не ниже Б1;

– наружная дверь должна быть оснащена: электрическим замком, открываемым снаружи с помощью пластиковой карточки, изнутри – механическим или электрическим способом (с обеспечением резервирования питания и возможности блокирования замка персоналом или охраной банка); врезным механическим замком; устройством принудительного закрывания (доводчиком), имеющим достаточно широкий диапазон рабочих температур.

Для исключения одновременного группового прохода и силового прорыва рекомендуется вход в зону самообслуживания оборудовать шлюзовой камерой. Двери, остекленные проемы, некапитальные конструкции зоны самообслуживания, смежные с помещениями банка должны быть также повышенной прочности и оборудованы техническими средствами охранной сигнализации (ТСОС). При сложной криминальной обстановке на территории расположения банкомата рекомендуется оснащать ТСОС также наружные остекленные проемы (двери) и капитальные конструкции.

Сигналы тревоги и другая информация от охранных датчиков должны поступать на пульт централизованного наблюдения ближайшего подразделения вневедомственной охраны и параллельно в службу безопасности банка или учреждения, в котором установлен банкомат.

Такой способ установки, когда банкомат устанавливается в проеме стены передней панелью на улицу, используется на оживленных, ярко освещенных проспектах и магистралях, в помещениях гостиниц, ресторанов, аэровокзалов и других учреждениях, работающих круглосуточно. Как минимум лицевая панель банкомата должна быть обеспечена эффективной защитой от вандализма.

Для записи телевизионного изображения в зоне самообслуживания и обстановки на прилегающей территории устанавливается скрытая телекамера, встроенная в банкомат или в стену над ним. При этом передняя панель банко-

мата и зона самообслуживания в темное время суток должны быть хорошо освещены и просматриваться с разных сторон.

Однако следует иметь в виду, что сама видеокамера может быть выведена из строя. Поэтому банкоматы с таким способом установки рекомендуется защищать вибрационными датчиками, которые обычно устанавливают на металлическом кожухе, закрывающем внутренние механизмы выдачи денег и расположенном в зоне загрузки.

При таком размещении датчика обеспечивается непосредственная передача вибрационных сигналов, возникающих при разрушающих (повреждающих) воздействиях на лицевую панель банкомата, и поэтому есть возможность оптимально отрегулировать дальность действия (чувствительность) датчика и обеспечить тем самым надежное обнаружение при высокой устойчивости к возникающим помехам. Настройка датчика производится путем имитации разрушающих воздействий на лицевую панель банкомата, например, нанесением серии ударов молотком (через прокладку из текстолита или гетинакса, чтобы не повредить внешнее декоративное покрытие панели).

При необходимости вибрационным датчиком может быть заблокирован и сейф банкомата, где хранятся наличные деньги. Настройка датчика в этом случае должна быть произведена в соответствии с рекомендациями для случая его установки на бронированном сейфе, изложенными в сопроводительной документации на прибор.

Требования к зоне загрузки при круглосуточном режиме работы следующие. Зоной загрузки может являться как специально выделенное внутреннее помещение банка, так и существующее служебное помещение (комната переговоров, служебный кабинет и т. п.). Не рекомендуется размещать зону загрузки банкомата в клиентской части операционного зала, если она не отгорожена соответствующими перегородками. Не допускается располагать зону загрузки в коридорах, находящихся за кассами, кабинах операционных касс, сейфовых комнатах, помещениях для пересчета денежной наличности.

Перегородки между зоной загрузки и другими помещениями должны не уступать по прочности кирпичным стенам толщиной 380 мм, а выходящие наружу здания – 510 мм.

Стены помещения, выделенного для зоны загрузки, не удовлетворяющие вышеприведенным требованиям, внутренние двери, остекленные проемы защищают решеткой, выполненной из стального прута диаметром не менее 16 мм, при этом размеры ячеек должны быть не более 150х150 мм. Допускается установка фигурной решетки, не уступающей по прочности вышеуказанной. Каждая решетка должна быть заблокирована вибрационным датчиком. При установке в остекленных проемах защитного стекла, устойчивого к взлому по классу защиты не ниже А2 или оклеивания имеющегося стекла специальной полимерной пленкой, обеспечивающей указанный класс защиты, металлические решетки допускается не устанавливать. При этом конструкция рамы (обвязки стекла) и способ ее крепления в проеме строительной конструкции должны обеспечивать ударосткойкость, равную или превышающую стойкость используемого стекла. Каждая остекленная конструкция должна быть заблокирована ударно-контактным или акустическим датчиком разрушения стекла.

Дверь помещения, выделенного для зоны загрузки, должна иметь класс защиты не ниже У1, внутренний замок, металлическую задвижку изнутри и смотровой глазок. Ограждающие конструкции зоны загрузки должны исключить ее просматриваемость снаружи.

Входную дверь следует оснастить магнито-контактным датчиком на открывание и вибрационным датчиком для защиты от взлома. Ограждающие конструкции при необходимости также могут быть защищены от преднамеренного разрушения. Если помещение, отведенное для зоны загрузки банкомата, имеет относительно небольшие размеры (менее 50 м^3), то ограждающие конструкции и дверь блокируют вибрационными датчиками. Внутренний объем помещения, отведенного для зоны загрузки банкомата, как правило, блокируют пассивным

инфракрасным или активным ультразвуковым датчиком, который реагирует на перемещение человека в охраняемом объеме.

В дополнение к датчикам в зоне самообслуживания может быть установлена система охранного телевидения (СОТ) (рис. 4.3). СОТ состоит из трех подсистем:

– видеонаблюдения;

– видеорегистрации;

– видеоконтроля.

Рис. 4.3. Базовая конфигурация для СОТ банкоматов

Система охранного телевидения должна:

– регистрировать действия клиента в зоне самообслуживания банкомата. В некоторых банкоматах устанавливают также камеры, фиксирующие момент ввода пластиковой карты;

– обеспечивать высокое качество записи. В случае необходимости восстановления событий работа идет с каждым кадром. При этом важными оказываются не только крупные планы, а мелкие объекты на заднем плане позволяют дополнить картину происшедшего;

– поддерживать настраиваемые на окружение датчики движения и физические датчики тревоги. Датчики тревоги должны инициировать запись в случаях открытия сейфа, вибрации и других подобных действий над банкоматом.

При ведении записи по детектору движения видеокамеры банкомата, установленного на улице, будут фиксировать любые перемещения людей возле него, и жесткие диски будут вскоре заполнены массой ненужной информации. Таким образом, необходимо использовать детектор движения с регулировкой чувствительности и настраивать его под каждый конкретный случай. В идеале начало записи должно инициироваться программным обеспечением банкомата в соответствии с логикой его работы;

– обеспечивать мониторинг работоспособности системы. Важный момент – возможность контроля из единого центра за работой сети банкоматов. Необходимо в режиме реального времени оценивать работоспособность элементов системы видеонаблюдения для предотвращения остановки записи, которой могут воспользоваться злоумышленники;

– определять отсутствие видеосигнала и блокировку объектива. При потере видеосигнала оператор системы наблюдения должен проинформировать группу быстрого реагирования о тревожном случае для оперативного принятия решения. Поэтому система видеонаблюдения должна фиксировать не только момент работы клиента с банкоматом, но и вести так называемую предтревожную запись, позволяющую сохранять видеоинформацию, регистрирующую события, произошедшие за заданный промежуток времени до получения сигнала «тревога»;

– обеспечивать защиту видеоархива наравне с хранимыми ценностями. Эту задачу следует разделить на две части. Во-первых, необходимо физически защитить накопитель видеоинформации от возможной кражи, располагая его или внутри самого банкомата, или в специально разработанном отсеке. Во-

вторых, сами видеоданные должны быть защищены от подделок. Для этого необходимо использовать специальные форматы оцифровки и индикацию целостности записи.

Для систем охранного телевидения чаще всего используют черно-белые видеокамеры, имеющие чувствительность не менее 0,5 лк для хорошо освещенных и не менее 0,05 лк для плохо освещенных зон. Использование цветных видеокамер нецелесообразно из-за более низкой чувствительности. Для обеспечения качественной визуализации изображений (бессрывное переключение камер на мониторы и видеомагнитофон) необходимо применять камеры с внешней синхронизацией.

Конструкция освещения должна быть вандалозащищенной, а также исключать возможность его отключения непосредственно из зоны самообслуживания. Для наблюдения в темное время суток необходимо обеспечить дежурное освещение (10–20 лк). Для повышения надежности и долговременности функционирования СОТ рекомендуется подавать напряжение питания по выделенным кабельным линиям.

Телевизионное изображение обстановки в зоне самообслуживания при входе в нее клиента должно записываться в реальном масштабе. Видеоданные, поступающие с видеокамеры, записываются в журнал синхронно при наступлении одного из трех событий:

– клиент банка вставил пластиковую карту в карт-ридер банкомата;

– клиент банка получает деньги из банкомата;

– клиент банка забирает пластиковую карту.

Таким образом, с видеоданными связывается информация об этих событиях. А именно: дата, время, идентификатор клиента банка, сумма, количество и номиналы выданных купюр.

В отсутствие клиента запись может не производиться либо вестись в замедленном режиме. С этой целью на наружной двери устанавливается датчик (например магнитный контактный), изменяющий режим записи.

При установке видеокамеры вне здания необходимо использовать герметичные термокожухи с солнцезащитным экраном, защищающие камеры от атмосферных осадков и температурных воздействий.

Внутри помещения банка целесообразно использовать видеокамеры с электронной регулировкой чувствительности (адаптация к изменению фоновой освещенности). В случае применения для освещения зоны люминесцентных ламп дневного света необходимо использовать объективы с автоматической регулировкой диафрагмы.

Для отображения поступающей информации с телекамер следует применять мониторы, способные работать круглосуточно в течение длительного времени и часто с неподвижным изображением, имеющие разрешающую способность не менее 600–700 ТВЛ.

При наличии в банке постовой охраны извещатель должен одновременно обеспечивать фиксирование (например с помощью звукового сигнала) момента входа каждого клиента в зону самообслуживания. Это делается для привлечения внимания охранника к экрану монитора. Может быть также предусмотрена акустическая связь (переговорное устройство) охранника с клиентом, находящимся в зоне самообслуживания.

Одним из лучших решений, которое позволит уменьшить риск возникновения физических угроз банкоматам, является система ограничения доступа (СОД). Она предназначена для повышения безопасности клиентов при совершении операций и ограничения доступа в помещения банкомата посторонних лиц.

Функциональные возможности СОД для банкоматов (рис. 4.4):

– предоставление доступа к банкомату владельцам пластиковых карт платежных систем, обслуживаемых данным банкоматом;

– ограничение доступа к банкомату лиц, у которых отсутствует пластиковая карта, обслуживаемая данным банкоматом;

– слежение за датчиком присутствия человека в зоне самообслуживания;

Рис. 4.4. Конфигурация СОД к банкомату

– световая индикация присутствия человека в помещении;

– управление освещением в помещении.

Принцип действия СОД к банкомату заключается в том, что на входную дверь помещения банкомата устанавливаются доводчик и электромагнитный или электромеханический замок, управляемый микропроцессорным контроллером. Контроллер СОД с помощью считывателя карт с магнитной полосой считывает и анализирует номер карты, записанный на магнитной полосе, и управляет замком. Для прохода к банкомату клиент предъявляет банковскую карту. Если контроллер запрограммирован на обслуживание карт данной платежной системы, то он открывает замок на определенное время и ждет либо срабатывания дверного контакта, либо окончания этого промежутка времени. При выполнении заданного условия замок запирается. Для выхода из помещения банкомата клиент нажимает кнопку «Выход». Таким образом ограничивается доступ в помещение банкомата лиц, не имеющих платежных карт, и обеспечивается безопасность клиента во время нахождения в зоне обслуживания банкомата.

Для повышения безопасности клиента при выполнении операций в состав СОД может включаться пассивный ИК-извещатель, блокирующий чтение маг-

нитных карт для открывания двери до тех пор, пока клиент находится в зоне обслуживания банкомата. Дополнительно в состав системы может входить информационное табло «Занято/Свободно», информирующее потенциальных посетителей о присутствии в помещении клиентов.

Контроллер СОД дает возможность применять различные типы электрических замков для организации прохода к банкомату в зависимости от требований к безопасности, особенно в нештатных и аварийных ситуациях. При этом обеспечивается возможность выполнения требований безопасности как к банкоматам, размещенным в контролируемых службой безопасности помещениях (например в вестибюле банка), так и к банкоматам, размещенным в автономных помещениях (например в специализированных киосках).

Для предотвращения угроз, связанных с установкой скимминговых устройств, существует два пути решения. Первый – технологический: оборудование банкоматов специальными техническими комплексами, противодействующими скиммингу:

– организация дискретной подачи карточки;

– установка «помехоизлучателя»;

– система IFD (англ. – Intelligent Fraud Detection – интеллектуальное выявление мошенничества).

Дискретная подача – неравномерная (рывками) подача карточки в картридер, что препятствует корректному копированию данных магнитной полосы карточки в случае наличия скимминговой устройства.

«Помехоизлучатель» – устройство, устанавливаемое внутри банкомата, которое формирует и направленно излучает в область возможного размещения скимминговой устройства электромагнитные помехи, делая невозможным корректное копирование данных магнитной полосы.

IFD представляет собой инновационное решение, препятствующее установке мошенниками устройств на лицевой панели банкомата. Система встраивается в банкомат и обнаруживает появление посторонних объектов, сделанных

из металла, дерева, пластика или других материалов. Ее срабатывание происходит в том случае, если данные изменения превышают заданные пороговые значения, установленные в соответствии с характером деятельности заказчика и параметрами транзакций. Важно отметить, что данное решение является совершенно незаметным как для клиентов, так и для мошенников.

Датчики системы реагируют на установку/удаление мошенником устройства, а также на попытки взлома банкомата. При этом датчики могут быть подключены к системе сигнализации банкомата; возможна также отправка текстового SMS-сообщения.

IFD включает в себя:

– стандартные датчики на устройстве считывания платежных карт и затворе диспенсера общим количеством до 6 шт.;

– средства обнаружения электромагнитных излучений для отслеживания видеокамер, установленных преступниками на банкомате;

– использование имеющейся в банкомате системы аварийной сигнализации;

– отправка сигналов тревоги в виде текстовых SMS-сообщений по четырем различным номерам;

– возможность обновления встроенного программного обеспечения для настройки и модернизации системы в будущем;

– полностью настраиваемая и контролируемая по времени система обнаружения.

Второй путь – организационный: регулярный осмотр банкомата и ближайшего окружающего пространства на предмет выявления установки скимминговых устройств; мониторинг операций по картам в сети банкоматов. Скорее, это не специальные, а обычные проверки (обслуживающим персоналом, сотрудниками отделений и т. п.), которые знакомы с конструкционными особенностями банкоматов и могут выявить любые изменения в его внешнем виде.

Рекомендации по обеспечению защиты автоматических кассовых аппаратов представлены в табл. 4.2.

Таблица 4.2

Рекомендации по обеспечению защиты автоматических кассовых аппаратов

Угрозы направленные	Средства защиты
На держателей карт	– установка систем охранного телевидения; – наличие «тревожной» кнопки рядом с банкоматом, сигнал от которой идет на пульт службы безопасности банка или правоохранительных органов; – организация системы контроля доступа к банкоматам.
На денежные средства	– правильный выбор места установки банкомата; – регулярный осмотр банкоматов на предмет наличия мошеннических устройств; – установка систем охранного телевидения; – наличие устройства окрашивания купюр несмываемой краской; – наличие датчиков тревожной сигнализации; – организация системы контроля доступа к банкоматам.
На карту и/или ее реквизиты	– регулярный осмотр банкоматов на предмет наличия скиммингговых устройств, скрытых видеокамер, накладных клавиатур и т. д.; – информирование пользователей банкоматов о возможных угрозах путем размещения соответствующей информации на мониторах банкоматов; – установка интеллектуальных систем выявление мошенничества; – установка систем охранного телевидения; – организация системы контроля доступа к банкоматам; – замена стандартных пользовательских клавиатур защищенными; – организация защищенных каналов связи; – применение надежных криптографических алгоритмов.
На банкомат-технологию	– организация защищенных каналов связи; – применение надежных криптографических алгоритмов; – соблюдение мер по защите от вредоносного программного обеспечения; – соблюдение правил политики информационной безопасности.

4.1.3. Защита автоматических кассовых аппаратов от несанкционированного доступа по линиям связи

Для анализа защищенности от НСД по линиям связи рассмотрим режимы работы автоматических кассовых аппаратов (АКА).

АКА может работать в одном из двух режимов:

– off-line (автономный режим);

– on-line (режим реального времени).

Автономный режим работы характерен тем, что банкомат функционирует независимо от автоматизированной системы банка. Запись информации о транзакции проводится на внутренний носитель и выводится на встроенный принтер. Достоинствами автономного режима банкомата являются его относительная дешевизна и независимость от линий связи. В то же время низкая стоимость установки напрямую обусловливает высокую стоимость эксплуатации таких банкоматов. Чтобы обновлять «черные списки» (стоп-листы) утраченных карточек, необходимо хотя бы раз в день обходить и обслуживать такие банкоматы. При большом числе таких устройств подобное обслуживание затруднительно. Отказ же от ежедневного обновления списков может привести к значительным потерям для банка в случае подделки карты или при пользовании похищенной картой.

Сложности возникают также при аутентификации клиента. Для защиты информации, хранящейся на карте с магнитной полосой, применяется ее шифрование. Для того чтобы банкоматы одного и того же банка воспринимали пластиковые карты с магнитной полосой, в них должен быть использован один ключ для шифрования (расшифрования). Компрометация его хотя бы в одном из банкоматов приведет к нарушению защиты всех банкоматов. Но так как зашифрованная информация не передается по линии связи, для получения ключа расшифрования необходимо изучение криптографических алгоритмов, применяемых в банкоматах, и анализ зашифрованных данных, что осуществляется в

течение весьма продолжительного времени и на практике является сложно реализуемым.

В режиме реального времени банкомат должен быть подключен непосредственно к автоматизированной системе банка (процессинговому центру). В этом случае регистрация транзакций осуществляется непосредственно в автоматизированной системе банка, хотя подтверждение о транзакции выдается на принтер банкомата (рис. 4.5).

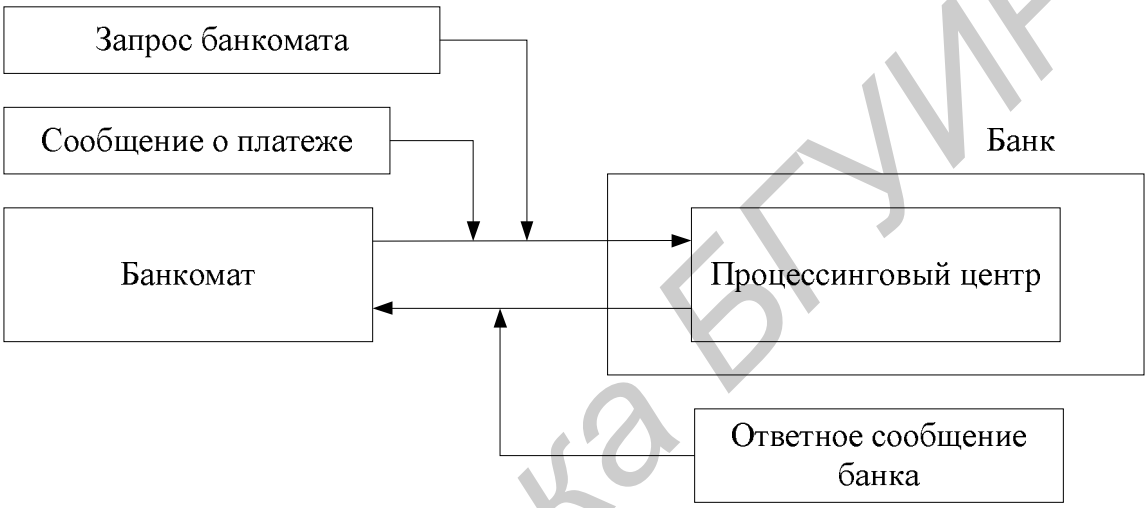

Рис. 4.5. Схема взаимодействия между банкоматом и автоматизированной системой при выполнении транзакции

Запрос банкомата включает следующие данные:

– идентификатор банкомата;

– номер счета и другая учетная информация клиента;

– номер карты;

– защитный символ;

– зашифрованный PIN клиента;

– требуемая денежная сумма;

– номер транзакции;

– проверочный код для всех данных сообщения.

Ответное сообщение банка включает следующие данные:

– идентификатор банкомата;

– разрешающий (запрещающий) код операции;

– номер транзакции;

– проверочный код для всех данных сообщения.

В этом обмене сообщениями для проверки целостности данных используется код аутентификации сообщения MAC (Message Authentication Code).

Режим реального времени имеет ряд преимуществ по сравнению с автономным режимом. Он дает возможность клиенту не только получить наличные деньги, но и осуществлять манипуляции со своим счетом. Централизованная идентификация/аутентификация позволяет существенно повысить устойчивость системы к компрометации ключей шифрования. Централизованная проверка идентификатора пользователя делает возможным оперативное обновление списков запрещенных к использованию карт, а также введение ограничений на количество наличных денег, которые может получить клиент в течение одного дня (для защиты от использования украденных карт).

Однако этот режим возможен лишь при наличии надежных каналов связи между банкоматами и банком, что делает его довольно дорогим. Кроме того, наличие канала связи порождает и другие угрозы безопасности по сравнению с автономным режимом работы. Это – анализ трафика между банкоматом и автоматизированной системой банка (АБС) и имитация работы АБС злоумышленником. При анализе трафика можно получить информацию о счетах, суммах, условиях платежей и т. п. При имитации работы АБС компьютер злоумышленника может выдавать положительный ответ на запрос банкомата о результатах идентификации/аутентификации.

Решением данной проблемы является комплексная защита, включающая в себя применение современных криптостойких алгоритмов шифрования внутренней информации обмена между банкоматом и АБС и подключение оконечных терминалов через шлюз безопасности (рис. 4.6). К данным устройствам предъявляется ряд требований:

– компактность;

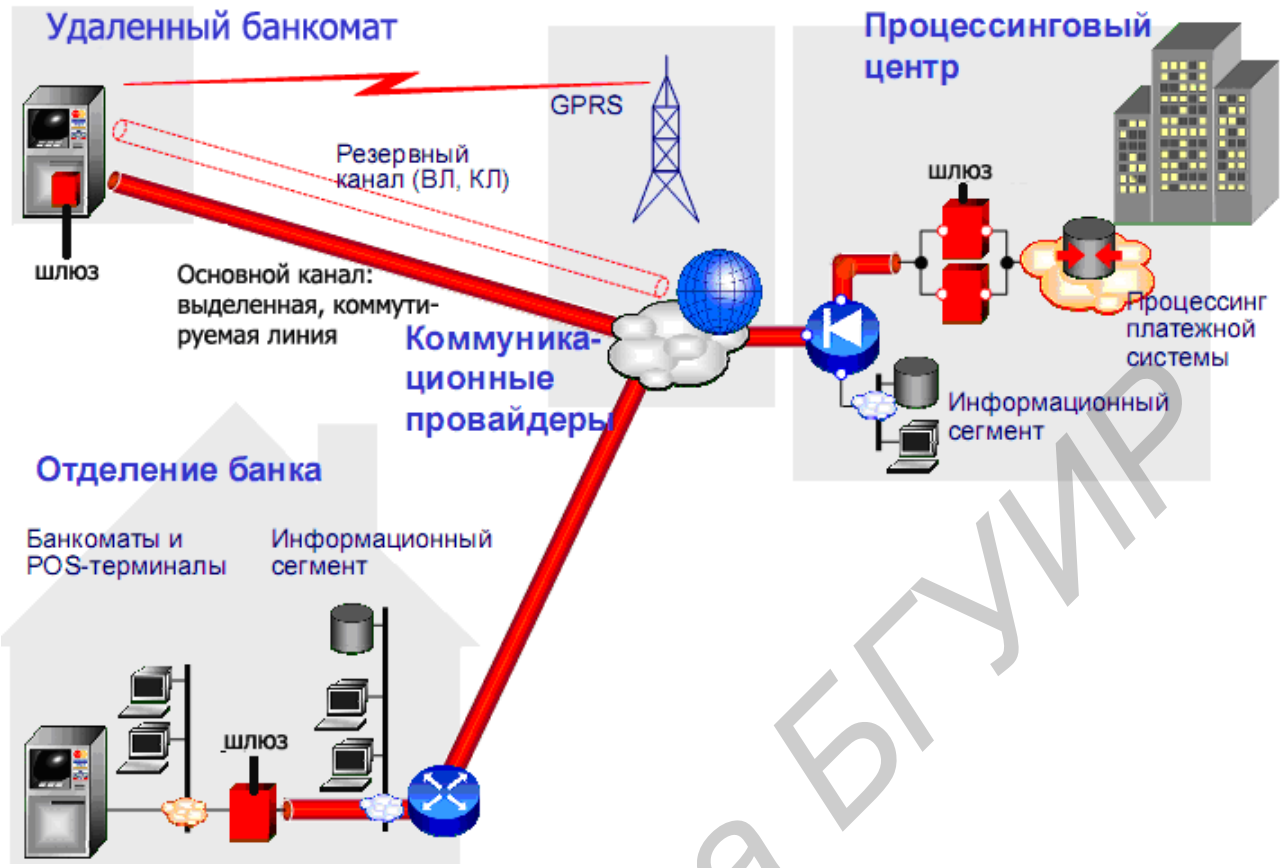

Рис. 4.6. Схема подключения АКА через шлюзы безопасности

– пылезащищенность (отсутствие механических компонент);

– поддержка коммуникационных сред платежных сетей:

– Ethernet;

– модем на внешние линии, коммутируемые линии, GPRS;

– поддержка требований надежности коммуникационной инфраструктуры;

– поддержка резервирования каналов со стороны банкомата (диверсификация доступа);

– поддержка резервирования сетевой инфраструктуры процессингового центра (работа в сети с резервированными шлюзами доступа, автоматическая обработка отказа шлюза доступа);

– стойкость защиты;

– конфиденциальность;

– контроль доступа (изоляция платежной сети);

– защищенность от несанкционированного доступа со стороны обслуживающего персонала;

– стандартизация, управляемость, совместимость с системами сетевого событийного протоколирования и мониторинга, работа с различными криптографическими и ключевыми системами.

Удаленный банкомат подключается к процессинговому центру при помощи выделенной и/или коммутируемой линии, средств мобильной телефонии. Банкомат, находящийся в отделении банка или в сети предприятия, связывается с центром через локальную сеть. Применение средств сетевой защиты позволяет безопасно подключать банкоматы или POS-терминалы через сеть Интернет. Это значительно выгоднее, чем выделенная линия IP или X.25, а также дешевле, надежнее и удобнее, чем коммутируемая линия. Подключения через Интернет легко диверсифицируются, что обеспечивает требуемый уровень надежности коммуникаций, при этом сегмент банковской сети необходимо защищать от несанкционированного доступа из сети Интернет.

Высокая стойкость системы защиты обеспечивается протоколами IKE / IPsec и использованием сертифицированных криптографических библиотек. При использовании протоколов IKE / IPsec обеспечивается устойчивость сегмента к атакам типа отказ в обслуживании (denial-of-service – DoS), повторная передача пакетов, клиппирование. Причем целостность (имитостойкость) гарантирована не только для данных, но и для заголовков пакетов (контроль целостности пакета и его заголовка не приводит к конфликту с системами трансляции IP-адресов – NAT).

Сети банкоматов являются в настоящее время распространенной формой эксплуатации банкоматов, в которой участвуют несколько банков. Банки-участники такой сети преследуют следующие цели:

– уменьшение стоимости операций для участников;

– разделение затрат и риска при внедрении новых видов услуг между участниками;

– преодоление географических ограничений и соответственно повышение субъективной ценности услуг для потребителей.

При совместном использовании несколькими банками сети банкоматов возникает серьезная проблема – защита конфиденциальной информации банков друг от друга (ключи шифрования и т. п.). Для разрешения этой проблемы предложена схема централизованной проверки PIN каждым банком в своем центре связи с банкоматами. Усложняется также система распределения ключей между всеми участниками сети.

Рассмотрим схему прохождения информации о PIN клиента между банкоматом, банком-эквайером (которому принадлежит банкомат) и банком-эмитентом (который выпустил карту клиента) (рис. 4.7).

Рис. 4.7. Схема прохождения информации о PIN клиента между участниками платежной системы

Пусть клиент Банка 2 (Эмитента) обратился к банкомату Банка 1 (Эквайера). При этом в сети банкоматов происходит следующий информационный обмен:

– карт-ридер банкомата считывает информацию, записанную на пластиковой карточке, предъявленной клиентом, и затем банкомат определяет, имеет ли этот клиент счет в Банке 1;

– если клиент не имеет счета в Банке 1, транзакция направляется в сетевой маршрутизатор, который, используя идентификационный номер Банка 2

(Bank Identification Number – BIN), направляет эту транзакцию на главный компьютер Банка 2 или производит проверку PIN для Банка 2;

– если проверка PIN производится на главном компьютере Банка 2, то этот компьютер получает полную информацию о транзакции и проверяет достоверность PIN;

– независимо от результата проверки компьютер Банка 2 пересылает сообщение с этим результатом посредством сетевого маршрутизатора компьютеру Банка 1.

Как следует из примера, к банку-эмитенту предъявляются следующие требования:

– выпускаемые пластиковые карточки должны восприниматься всеми банкоматами сети;

– банк-эмитент должен обладать технологией проверки PIN собственных клиентов.

К банку-эквайеру предъявляются следующие требования:

– в банкомате или главном компьютере банка должна быть реализована проверка принадлежности транзакции;

– если нет возможности проверить правильность чужого PIN, банк-эквайер должен передать данные о транзакции на сетевой маршрутизатор.

Для защиты взаимодействия компьютеров банков друг с другом и с банкоматами должно применяться оконечное (абонентское) шифрование информации, передаваемой по линиям связи. Обычно используется следующий подход: вся сеть банкоматов разбивается на зоны, и в каждой из них используется свой главный зональный управляющий ключ (Zone Control Master Key – **ZCMK**). Ключ **ZCMK** предназначен для шифрования ключей при обмене между сетевым маршрутизатором и главным компьютером банка. Ключ **ZCMK** индивидуален для всех участников сети. Обычно он генерируется случайным образом маршрутизатором и передается неэлектронным способом в банк. Раскрытие

ключа **ZCMK** приведет к раскрытию всех PIN, которые передаются между маршрутизатором и главным компьютером банка.

Для шифрования информации, поступающей от главного компьютера банка-эмитента на маршрутизатор, используется рабочий ключ эмитента (Issuer Working Key – **IWK**). Его сообщает главному компьютеру банка-эмитента маршрутизатор в зашифрованном на уникальном **ZCMK** виде. Ключ **IWK** может меняться по запросу пользователя в процессе работы.

Аналогичный по назначению ключ для обмена между банком-эквайером и маршрутизатором называется рабочим ключом эквайера (Acquirer Working Key – **AWK**). Для шифрования информации при передаче от банкомата к главному компьютеру банка-эквайера используется ключ связи банка-эквайера (Acquirer Communication Key – **АСК**).

При рассмотрении функционирования системы защиты введены следующие обозначения:

– $E_Y(X)$ – шифрование сообщения **X** по алгоритму DES с использованием ключа **Y**;

– $D_Y(X)$ – расшифрование сообщения **X** по алгоритму DES с использованием ключа **Y**;

– **PBL** (PIN Block Local) – локальный блок PIN, полученный из введенного клиентом PIN, дополненного до восьми символов, и представленный во внутреннем формате банкомата;

– **PBN** (PIN Block Network) – сетевой блок PIN, полученный из введенного клиентом PIN, дополненного до восьми символов, и представленный в виде, готовом для передачи в сети.

Вернемся к рассмотрению схемы на рис. 4.7:

– клиент предъявил банкомату Банка 1 банковскую карту и ввел с клавиатуры свой PIN. Банкомат формирует **PBL**, шифрует его с использованием **АСК**, то есть вычисляет криптограмму ЕАСк(PBL), и отправляет ее на главный компьютер Банка 1;

– на главном компьютере Банка 1 блок **PBL** расшифровывается и преобразуется в блок **PBN**, затем блок **PBN** шифруется с использованием **AWK** и отсылается в сетевой маршрутизатор. Процесс преобразования:

$$E_{ACK}(PBL) \rightarrow E_{AWK}(PBN)$$

называют трансляцией блока PIN с ключа **АСК** на ключ **AWK**. Основное назначение этого процесса – изменение ключа шифрования;

Если PIN проверяется на сетевом маршрутизаторе, после получения криптограммы **EAWK(PBN)** производится ее расшифрование, а затем выделение PIN с помощью преобразований:

$$D_{AWK}(E_{AWK}(PBN)) = PBN \rightarrow PIN.$$

Если PIN проверяется Банком 2, принятая криптограмма транслируется с ключа **AWK** на ключ **IWK** (оба ключа хранятся на сетевом маршрутизаторе):

$$E_{AWK}(PBN) \rightarrow E_{IWK}(PBN).$$

Затем криптограмма $E_{IWK}(PBN)$ отправляется в Банк 2;

– поступившая в Банк 2 криптограмма $E_{IWK}(PBN)$ преобразуется в зависимости от используемого способа проверки либо в открытый PIN:

$$D_{IWK}(E_{IWK}(PBN)) = PBN \rightarrow PIN,$$

либо в PIN в форме блока **PBL**, зашифрованного на ключе базы данных **DBK**:

$$E_{IWK}(PBN) \rightarrow E_{DWK}(PBL);$$

– после любого из этих преобразований осуществляется поиск принятого PIN в базе данных существующих PIN;

– в результате выполненной проверки введенный клиентом PIN либо принимается, либо отвергается. Вне зависимости от результата проверки главный компьютер Банка 2 пересылает сообщение с результатом через Сетевой маршрутизатор на компьютер Банка 1, а тот оповещает банкомат о результатах решения.

Рассмотренная схема обеспечения безопасности взаимодействия компьютеров в сети базируется на алгоритме шифрования DES. Поэтому на распро-

странение ключа **ZCMK** налагаются жесткие ограничения. Применение асимметричной системы шифрования с открытым ключом позволяет несколько упростить ключевую систему и соответственно взаимодействие между банкоматами и главными компьютерами банков.

В неразделяемой сети банкоматов достаточно использовать на всех банкоматах одинаковый открытый ключ, а на главном компьютере банка – секретный ключ. Это позволяет шифровать запрос и подтверждающее сообщение из банка, так как обеспечение конфиденциальности ответного сообщения необязательно.

4.1.4. Защита от вредоносного программного обеспечения

В целях защиты от вредоносного программного обеспечения можно использовать:

– административные меры защиты, включающие в себя разработку правил и инструкций по работе компьютерной сети предприятия и применению программного обеспечения и грамотное администрирование сети;

– профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

– технические – применение аппаратных средств – межсетевых экранов;

– специализированные программы для защиты от вирусов;

– введение четкой системы политики информационной безопасности предприятия, включающей в себя разграничение доступа, что позволит предотвратить несанкционированное использование информации, уменьшить последствия от ошибочных действий пользователей.

4.1.5. Обеспечение отказоустойчивости системы

Под отказоустойчивостью принято понимать способность сохранять работоспособность системы при воздействии на нее дестабилизирующих факторов. Основными дестабилизирующими факторами для банкоматов являются

помехи в линии связи, резкое повышение или уменьшение напряжения, импульсные помехи, а также неблагоприятные условия окружающей среды.

Приведем основные технические требования к банкоматам, при которых воздействие дестабилизирующих факторов не влияет на их работу.

Требования к максимальному току в зависимости от входного напряжения:

– 4,1 А при напряжении 240 В.

Требования к максимальному пусковому току в зависимости от входного напряжения:

– пиковое значение 150 А при напряжении 257 В.

Значение входного напряжения:

– от 198 до 257 В при частоте 50/60 Гц.

Требования к заземлению:

– если питание обеспечивается от распределительного щита общего назначения, то другие параллельные цепи с этого распределительного щита не должны использоваться для питания таких устройств, как кондиционеры, лифты и т. д.;

– в случае использования распределительного щита все заземляющие провода параллельной цепи должны быть соединены с отдельными клеммами в щите. Заземляющий провод от распределительного щита к точке заземления здания должен быть, как минимум, по диаметру равен по размеру электропроводу, который поставляется для питания банкомата.

Банкомат может функционировать при условиях окружающей среды, выходящих за указанный ниже диапазон температур и влажности. Однако следует избегать продолжительной работы устройства в условиях, близких к границам диапазона или в месте, где изменения температуры и влажности превышают ограничения, приведенные в табл. 4.3.

Таблица 4.3

Рабочий диапазон температур и влажности воздуха

Место установки	Параметр			
	Температура, °С	Скорость изменения температуры , °С в час	Относительная влажность, %	Скорость изменения относительной влажности, % в час
Банкомат, находящийся в помещении	от 10 до 40	10	от 20 до 80	10
Банкомат вне помещения	от –35 до 50	10	от 10 до 100	10

4.2. Лабораторное задание

1. Изучить теоретический материал по методам и средствам защиты АКА от НСД.

2. Включить компьютер и запустить файл Bankomat.exe на выполнение.

3. Изучить материал, представленный в медиа-галерее.

4. Выполнить тестовое задание. Ответы на вопросы теста выполняются путем выбора правильного (правильных) ответа (ответов) из предложенных вариантов. Результат выполнения теста показать преподавателю.

5. Практическая часть работы представляет собой процесс проектирования системы защиты АКА от угроз НСД.

6. В появившемся окне выбрать (рис. 4.8) место установки АКА по заданию преподавателя.

7. В соответствии с местом установки АКА выбрать соответствующие ему угрозы для АКА (рис. 4.9).

8. Для каждой отдельной выбранной угрозы выбрать соответствующее (соответствующие) средства ей противодействия путем наведения указателя мыши на выбранное средство, нажатия левой кнопки мыши и «перетаскивания» выбранного средства в область, отмеченную прямоугольником серого цве-

та (рис. 4.10). При этом максимальное количество средств защиты для одной угрозы ограничивается и не превышает 3.

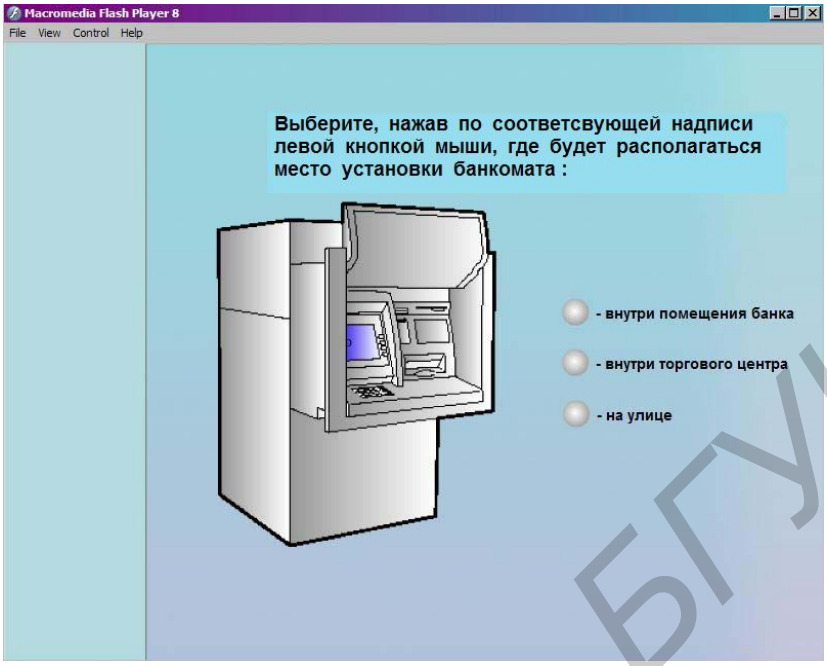

Рис. 4.8. Выбор места установки АКА

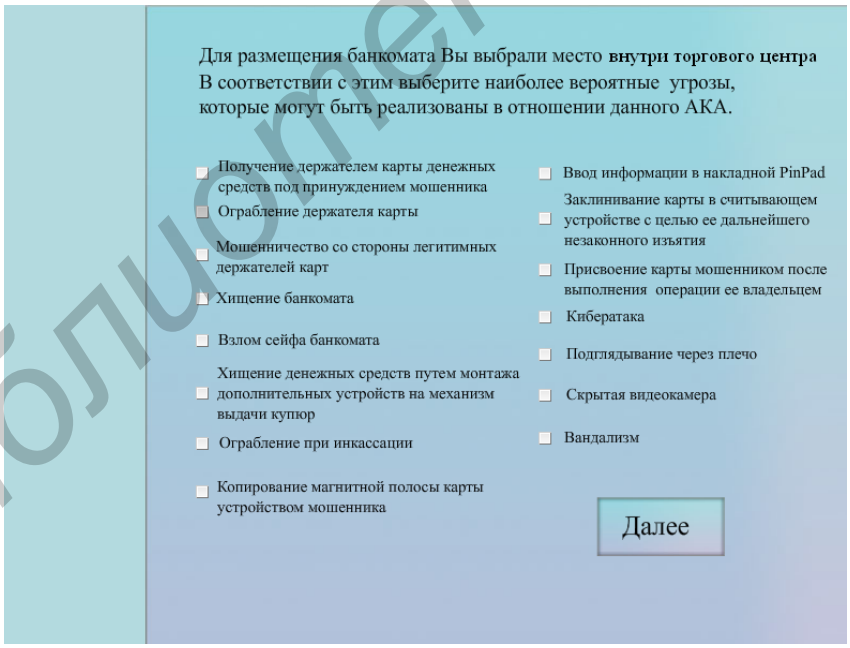

Рис. 4.9. Окно выбора угроз

9. Правильность выполнения работы будет отмечена после завершения проектирования системы защиты АКА от НСД.

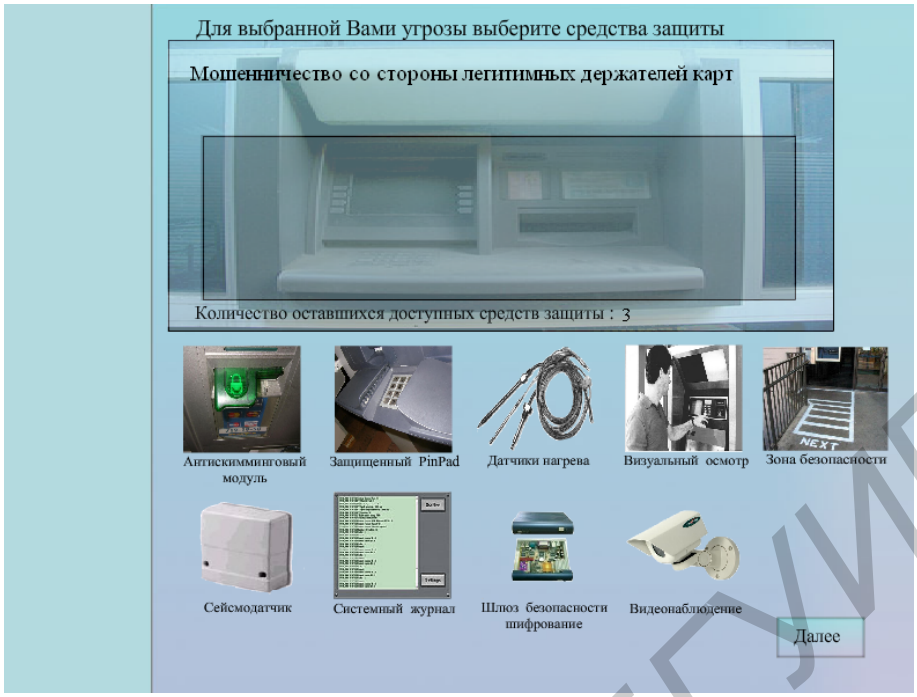

Рис. 4.10. Окно выбора средств защиты

4.3. Содержание отчета

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

4.4. Контрольные вопросы

1. Назначение автоматического кассового аппарата.
2. Что такое идентификация?
3. Что такое аутентификация?
4. Режимы работы автоматических кассовых аппаратов, их достоинства и недостатки.
5. Для чего используются разделяемые сети автоматических кассовых аппаратов.

Лабораторная работа №5

ЗАЩИТА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ В POS-СИСТЕМАХ

Цель работы: изучить принципы построения и функционирования POS-систем, методы и способы защиты электронных платежей в них.

5.1. Теоретическая часть

5.1.1. Назначение POS-систем

Системы, обеспечивающие расчеты продавца и покупателя в точке продажи (point-of-sale – POS), получили распространение в США более 20 лет назад. В основном все терминалы, подключенные к этим системам, размещены на предприятиях торговли. Большинство таких терминалов установлены в крупных магазинах, так как там совершается большое количество покупок в течение дня, а также на автозаправочных станциях.

Системы POS обеспечивают следующие услуги:

– проверку и подтверждение чеков;

– проверку и обслуживание дебетовых и кредитных карточек;

– использование системы электронных расчетов.

Использование POS-терминалов позволяет автоматизировать операции по обслуживанию держателя пластиковой карточки и существенно уменьшить время обслуживания.

POS-терминалы могут быть различными по конфигурации и выполняемым функциям. Существуют POS-терминалы, построенные на базе персонального компьютера и выполненные в виде специализированного устройства (рис. 5.1).

В комплект вышеприведенного терминала входит процессор, сенсорный дисплей, карт-ридер для считывания магнитных карт, жесткий диск как запоминающее устройство, пользовательская клавиатура для введения PIN. При необходимости данный терминал можно дополнить фискальным регистратором,

денежным ящиком, дисплеем покупателя. Кроме того, обычно POS-терминал оснащается модемом с возможностью автодозвона.

а б

Рис. 5.1. Внешний POS-терминалов: а – на базе персонального компьютера; б – выполненного в виде отдельного устройства

POS-терминал обладает интеллектуальными возможностями – его можно программировать. В качестве языков программирования используются Ассемблер, а также диалекты C и Basic'a. Все это позволяет проводить не только on-line авторизацию карт с магнитной полосой и смарт-карт, но и использовать при работе со смарт-картами режим off-line с накоплением протоколов транзакций. Последние во время сеансов связи передаются в процессинговый центр. Во время сеанса связи POS-терминал может также принимать и запоминать информацию, передаваемую персональным компьютером процессингового центра. В основном это бывают стоп-листы, но подобным же образом может осуществляться и перепрограммирование POS-терминалов.

5.1.2. Проведение транзакции и ее защита

Системы POS обеспечивают сокращение расходов по обработке бумажных денег и уменьшают риски покупателя и продавца, связанного с этой обработкой (рис. 5.2).

Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карту и для подтверждения личности вводит PIN. Продавец со своей

стороны вводит сумму, которую необходимо уплатить за покупку или за услуги.

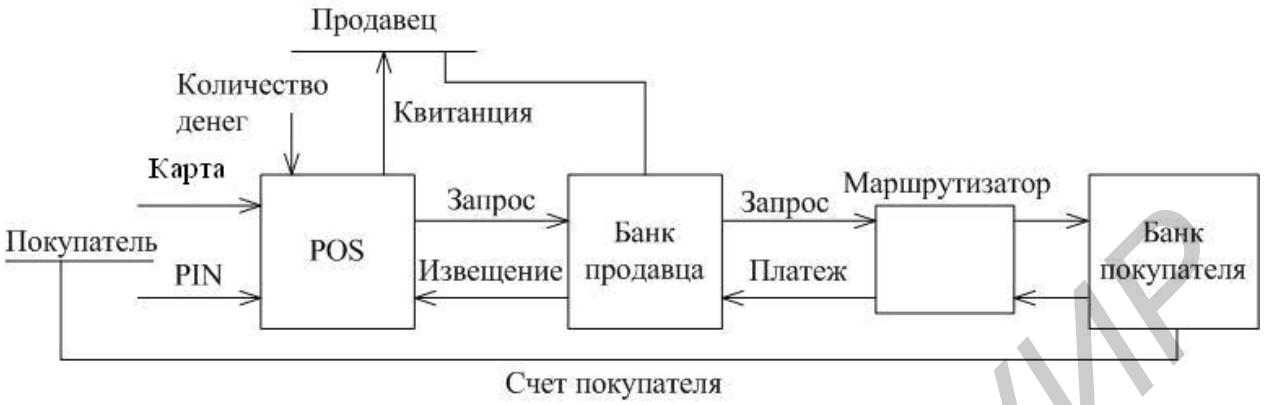

Рис. 5.2. Схема системы POS

Запрос на перевод денег направляется в банк продавца, который для проверки подлинности карточки, предъявленной покупателем, переадресует запрос в банк покупателя. Если карточка подлинная и покупатель имеет право применять ее для оплаты продуктов и услуг, банк покупателя переводит деньги в банк продавца на его счет. После перевода денег банк продавца посылает извещение на терминал POS, в котором сообщает о завершении транзакции. После этого продавец выдает покупателю извещение.

Обратим внимание на тот путь, который должна проделать информация, прежде чем будет осуществлена транзакция: во время его прохождения возможна потеря сообщений. Во избежание этого банк продавца должен повторять выдачу сообщений при обнаружении их потери.

Для защиты системы POS должны соблюдаться следующие требования:

1. Проверка PIN-кода, введенного покупателем, должна производиться системой банка покупателя. При пересылке по каналам связи PIN должнен быть зашифрован.

2. Сообщения, содержащие запрос на перевод денег (или подтверждение о переводе), должны проверяться на подлинность для защиты от внесения изменений и замены при прохождении по линиям связи к обрабатывающим процессорам.

Самым уязвимым местом системы POS являются ее терминалы. Если все построение системы охраны исходит из предположения абсолютно надежной физической защиты банкомата, то для терминалов POS это не так. Изначально предполагается, что терминал системы POS не защищен от внешнего воздействия.

В связи с этим предположением возникают новые типы угроз для терминала. Они связаны с раскрытием секретного ключа, который находится в терминале POS и служит для шифрования информации, передаваемой терминалом в банк продавца. Угроза вскрытия ключа терминала весьма реальна, так как терминал устанавливается в таких неохраняемых местах, как магазины, автозаправочные станции и пр. Эти угрозы получили следующие названия:

1. «Обратное трассирование» (back tracking). Сущность этой угрозы заключается в том, что если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, использованные в предыдущих транзакциях.

2. «Прямое трассирование» (forward tracking). Сущность этой угрозы заключается в том, что если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, используемые в транзакциях, которые произойдут после того, как он получит ключ.

Для защиты от этих угроз были предложены три метода: метод ключа транзакции, метод выведенного (полученного – derived) ключа и метод открытых ключей. Сущность первых двух заключается в том, что они предусматривают изменение ключа шифрования передаваемых данных для каждой транзакции.

Метод ключа транзакции (transaction key)

Информация, передаваемая между каждым терминалом и каждым эмитентом карточек, должна быть зашифрована на уникальном ключе, который в свою очередь должен изменяться от транзакции к транзакции. Однако применение этого метода для большого количества терминалов и эмитентов карточек

делает затруднительным управление ключами. Поэтому в подавляющем большинстве практических приложений он применяется не к связи «терминал–эмитент карт», а к связи «терминал–получатель», так как каждый получатель имеет ограниченное количество доступных терминалов.

При генерации нового ключа используются следующие составляющие: однонаправленная функция от значения предыдущего ключа; содержание транзакции и информация, полученная с карточки. При этом подразумевается, что предыдущая транзакция завершилась успешно. Такая схема обеспечивает защиту как от «обратного трассирования», так и от «прямого трассирования». Раскрытие одного ключа не дает возможности злоумышленнику вскрыть все предыдущие или все последующие транзакции.

Метод предусматривает также раздельную генерацию двух ключей – одного для шифрования PIN, другого – для получения MAC. Это необходимо для разделения функций банков продавца и получателя. Недостатком схемы является ее сложность.

Метод выведенного ключа (derived key)

Этот метод более прост в использовании, однако менее надежен. Он обеспечивает смену ключа при каждой транзакции независимо от ее содержания. Для генерации ключа здесь используется однонаправленная функция от текущего значения ключа и некоторое случайное значение. Метод обеспечивает защиту только от «обратного трассирования». Процесс получения ключа для шифрования транзакции показан на рис. 5.3. Вершиной дерева является некое начальное значение ключа. Для того чтобы получить ключ с номером S, число S представляется в двоичном виде. Затем, начиная со старшего разряда, идет анализ двоичного представления числа S. Если разряд равен единице, то к текущему значению ключа применяется односторонняя функция $F_X(K)$, где $\boldsymbol{X}$ – номер рассматриваемого разряда. В противном случае переходят к рассмотрению следующего разряда без применения односторонней функции. Последняя реализована на основе алгоритма DES. Для увеличения скорости обычно огра-

ничивают количество единиц в двоичном представлении числа S (не более десяти).

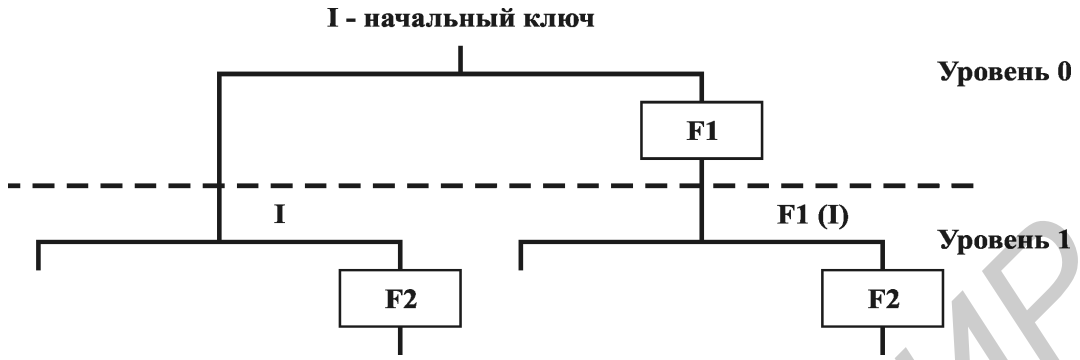

Рис. 5.3. Процесс получения ключа шифрования транзакции

Применение открытых ключей

Применение открытых ключей позволяет надежно защититься от любых видов трассирования и обеспечить надежное шифрование передаваемой информации. В этом методе терминал POS снабжается секретным ключом, на котором шифруется запрос к банку продавца.

Этот ключ генерируется при инициализации терминала. После генерации секретного ключа терминал посылает связанный с ним открытый ключ на компьютер продавца. Обмен между участниками взаимодействия осуществляется с использованием открытого ключа каждого из них. Подтверждение подлинности участников осуществляется специальным центром регистрации ключей с использованием своей пары открытого и закрытого ключей. Недостатком метода является его сравнительно малое быстродействие.

5.1.3. Механизмы защиты POS-систем

Задачи, решаемые протоколами обмена данными, аналогичны задачам, решаемым при защите локальных систем: обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети. Реализация этих функций осуществляется с помощью специальных механизмов.

Механизмы шифрования, которые обеспечивают конфиденциальность передаваемых данных и/или информации о потоках данных. Используемый алгоритм шифрования может использовать секретный или открытый ключи. В первом случае предполагается наличие механизмов управления и распределения ключей. Различают два способа шифрования: канальное (link encryption), реализуемое с помощью протоколов канального уровня, и оконечное (абонентское, end-to-end encryption), реализуемое с помощью протоколов прикладного или, в некоторых случаях, представительного уровня.

В случае канального шифрования защищается вся передаваемая по каналу связи информация, включая служебную. Этот способ имеет следующие особенности:

– вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;

– вся передаваемая информация, включая служебные сообщения, служебные поля сообщений с данными, надежно защищена;

– вся информация оказывается открытой на узлах – ретрансляторах, шлюзах и т. д.;

– пользователь не принимает участия в выполняемых операциях шифрования;

– для каждой пары узлов требуется свой ключ;

– алгоритм шифрования должен быть криптостойким и обеспечивать скорость шифрования на уровне пропускной способности канала связи (иначе возникнет задержка сообщений, которая может привести к блокировке системы или существенному снижению ее производительности);

– предыдущая особенность приводит к необходимости реализации алгоритма шифрования аппаратными средствами, что увеличивает расходы на создание и обслуживание системы.

Оконечное (абонентское) шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами.

Другими словами, отправитель зашифровывает данные, получатель – расшифровывает. Такой способ имеет следующие особенности (сравните с канальным шифрованием):

– защищенным оказывается только содержание сообщения: вся служебная информация остается открытой;

– никто, кроме отправителя и получателя, восстановить информацию не может (если используемый алгоритм шифрования криптостойкий);

– маршрут передачи не существенен – в любом канале информация останется защищенной;

– для каждой пары пользователей требуется уникальный ключ;

– пользователь должен знать процедуры шифрования и распределения ключей.

Выбор того или иного способа шифрования или их комбинации зависит от результатов анализа риска. Вопрос стоит следующим образом: что более уязвимо – непосредственно отдельный канал связи или содержание сообщения, передаваемого по различным каналам. Канальное шифрование быстрее (применяются другие, более быстрые, алгоритмы), прозрачно для пользователя, требует меньше ключей. Оконечное шифрование более гибко, может использоваться выборочно, однако требует участия пользователя. В каждом конкретном случае вопрос должен решаться индивидуально.

Механизмы цифровой подписи, которые включают процедуры закрытия блоков данных и проверки закрытого блока данных. Первый процесс использует секретную ключевую информацию, второй – открытую, не позволяющую восстановить секретные данные. С помощью секретной информации отправитель формирует служебный блок данных (например, на основе односторонней функции), получатель на основе общедоступной информации проверяет принятый блок и определяет подлинность отправителя. Сформировать подлинный блок может только пользователь, имеющий соответствующий ключ.

Механизмы контроля доступа. Осуществляют проверку полномочий сетевого объекта на доступ к ресурсам. Проверка полномочий производится в соответствии с правилами разработанной политики безопасности (избирательной, полномочной или любой другой) и реализующих ее механизмов.

Механизмы обеспечения целостности передаваемых данных. Эти механизмы обеспечивают как целостность отдельного блока или поля данных, так и потока данных. Целостность блока данных обеспечивается передающим и принимающим объектами. Передающий объект добавляет к блоку данных признак, значение которого является функцией от самих данных. Принимающий объект также вычисляет эту функцию и сравнивает ее с полученной. В случае несовпадения выносится решение о нарушении целостности. Обнаружение изменений может повлечь за собой действия по восстановлению данных.

В случае умышленного нарушения целостности может быть соответствующим образом изменено и значение контрольного признака (если алгоритм его формирования известен), в этом случае получатель не сможет установить нарушение целостности. Тогда необходимо использовать алгоритм формирования контрольного признака как функцию данных и секретного ключа. В этом случае правильное изменение контрольного признака без знания ключа будет невозможно и получатель сможет установить, подвергались ли данные модификации.

Защита целостности потоков данных (от переупорядочивания, добавления, повторов или удаления сообщений) осуществляется с использованием дополнительных форм нумерации (контроль номеров сообщений в потоке), меток времени и т. д.

Механизмы аутентификации объектов сети. Для обеспечения аутентификации используются пароли, проверка характеристик объекта, криптографические методы (аналогичные цифровой подписи). Эти механизмы обычно применяются для аутентификации одноуровневых сетевых объектов. Используемые методы могут совмещаться с процедурой «троекратного рукопожатия»

(троекратный обмен сообщениями между отправителем и получателем с параметрами аутентификации и подтверждениями).

Механизмы заполнения текста. Используются для обеспечения защиты от анализа трафика. В качестве такого механизма может использоваться, например, генерация фиктивных сообщений. В этом случае трафик имеет постоянную интенсивность во времени.

Механизмы управления маршрутом. Маршруты могут выбираться динамически или быть заранее заданы с тем, чтобы использовать физически безопасные подсети, ретрансляторы, каналы. Оконечные системы при установлении попыток навязывания могут потребовать установления соединения по другому маршруту. Кроме того, может использоваться выборочная маршрутизация (то есть часть маршрута задается отправителем явно – в обход опасных участков).

Механизмы освидетельствования. Характеристики данных, передаваемые между двумя и более объектами (целостность, источник, время, получатель), могут подтверждаться с помощью механизмов освидетельствования. Подтверждение обеспечивается третьей стороной (арбитром), которой доверяют все заинтересованные стороны, поскольку она обладает необходимой информацией.

Помимо перечисленных выше механизмов защиты, реализуемых протоколами различных уровней, существует еще два, не относящихся к определенному уровню. Они по своему назначению аналогичны механизмам контроля в локальных системах.

Обнаружение и обработка событий (аналог средств контроля опасных событий). Предназначены для обнаружения событий, которые приводят или могут привести к нарушению политики безопасности сети. Список этих событий соответствует списку для отдельных систем. Кроме того, в него могут быть включены события, свидетельствующие о нарушениях в работе перечисленных выше механизмов защиты. Предпринимаемые в этой ситуации действия могут включать различные процедуры восстановления, регистрацию событий, одно-

стороннее разъединение, местный или периферийный отчеты о событии (запись в журнал) и т. д.

Отчет о проверке безопасности (аналог проверки с использованием системного журнала). Проверка безопасности представляет собой независимую проверку системных записей и деятельности на соответствие заданной политике безопасности.

5.2. Лабораторное задание

1. Включить персональный компьютер.

2. Запустить файл act.exe на выполнение.

3. В появившемся окне ввести личные данные. После нажатия кнопки «ОК» карточка будет зарегистрирована (рис. 5.4).

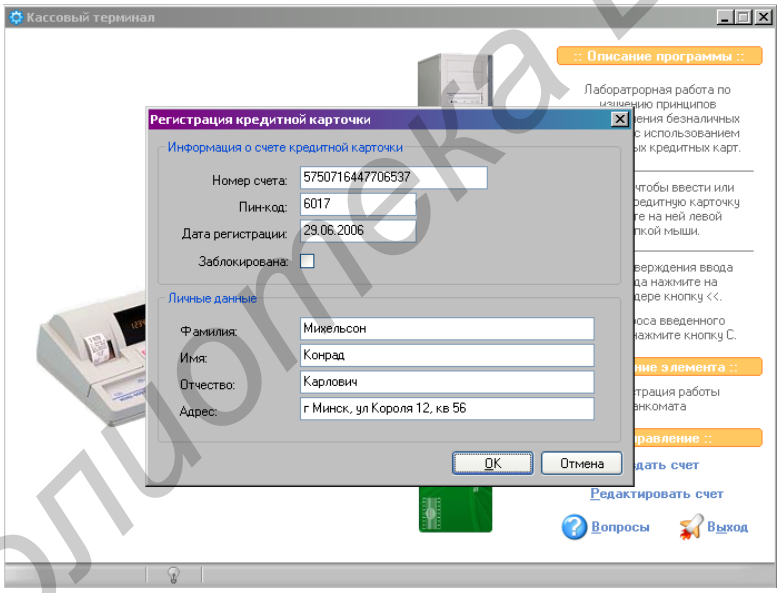

Рис. 5.4. Окно регистрации пластиковой карты

4. Оплата товаров и услуг в АКА производится за счет безналичных средств. Для этого нужно вставить карту в карт-ридер (кликните по карте мышью).

5. Введите PIN-карты. Подтверждение набранного PIN осуществляется нажатием кнопки «<<». При вводе PIN-кода нужно помнить, что неправильный

ввод PIN три раза подряд вызовет блокировку карточки. Просмотр PIN выполняется выбором пункта «Редактировать счет».

6. После подтверждения введенного PIN АКА обращается в процессинговый центр для аутентификации карточки и если результат этой процедуры положителен, то производится расчет.

7. Введите неправильный PIN три раза подряд и убедитесь, что карта действительно блокируется. Разблокировку карты можно выполнить, выбрав пункт «Редактировать счет», где необходимо убрать метку в пункте «Заблокирована», после чего карта может использоваться в дальнейшем для оплаты товаров и услуг.

5.3. Содержание отчета

1. Цель работы.
2. Вывод по работе.
3. Схема POS-системы.
4. Ответы на контрольные вопросы.

5.4. Контрольные вопросы

1. Назначение автоматического кассового аппарата.
2. Что такое идентификация?
3. Что такое аутентификация?
4. Какие существуют режимы работы автоматических кассовых аппаратов, их достоинства и недостатки.
5. Для чего используются разделяемые сети автоматических кассовых аппаратов?

Лабораторная работа №6

ЗАЩИТА ТРАНЗАКЦИЙ В СИСТЕМАХ МИКРОПЛАТЕЖЕЙ

Цель работы: изучить принципы построения и функционирования систем микроплатежей, методы и способы защиты транзакций в них.

6.1. Теоретическая часть

6.1.1. Категории электронных платежей

Электронные платежные системы предназначены для обеспечения платежных операций в сети Интернет. С помощью этих систем можно оплатить домен или хостинг для сайта, коммунальные услуги, услуги сотовой связи и т. д.

Существует несколько категорий электронных платежей. Для Интернета установлены три типа платежей в зависимости от объема заказа. ***Микроплатежи*** – транзакции стоимостью товара или услуги до пяти евро (долларов). Данного типа системы принимают к оплате электронные наличные (e-cash) ввиду малых затрат на осуществление транзакции. ***Потребительские платежи*** – стоимостью товара или услуги от 5 до 500 евро (долларов). В данном случае оплата выполняется с использованием пластиковой карточки. ***Промышленные платежи*** – транзакции с объемом свыше 500 евро (долларов), выполняемые путем перечисления средств или посредством счет-фактур.

В Интернете существует три типа систем оплаты: с предоплатой, оплатой в момент совершения сделки и оплатой по факту получения товара. Система ***с предоплатой*** предполагает, что сначала осуществляется платеж, а затем покупатель получает товар или услугу. Системы с предоплатой обычно работают с сохранением электронных денег на жестком диске персонального компьютера или на смарт-карте. В этом случае электронные деньги можно считать цифровым эквивалентом наличных денег, а содержащий электронные деньги файл называется электронным кошельком. Электронные деньги можно использовать в любой момент для оплаты приобретаемых товаров или услуг в онлайновом ре-

жиме. Преимущество электронных наличных денег – анонимность. Нельзя установить личность покупателя, который заплатил за услуги или товары. Правда, если заказанный товар нужно доставить на определенный адрес, анонимность теряется. Недостаток электронного кошелька – хранение файла на жестком диске или смарт-карте. Утрата файла означает пропажу денег. Кроме того, существует и проблема несанкционированного доступа к файлам пользователя.

6.1.2. Оплата с помощью пластиковых карт

Оплата по пластиковым карточкам – один из самых распространенных и удобных методов оплаты через Интернет. Пластиковые карточки просты в использовании и принимаются к оплате во всем мире. Клиент просматривает предлагаемые на Web-сайте товары и услуги, выбирает то, что ему нужно, и вводит данные своей карточки в соответствующее поле HTML-формы. Заполненная форма передается на Web-сайт, где данная информация накапливается и один раз в день передается в банк; либо, если владелец Web-сайта имеет прямую связь с банком, проверка кредитоспособности клиента проводится немедленно, в режиме реального времени.

Система оплаты с помощью пластиковых карточек обладает определенными преимуществами по сравнению с другими системами оплаты. Пластиковые карточки выпускаются и принимаются к оплате во всем мире, так что клиент может накапливать счета и оплачивать их позже (например в конце месяца). Система пластиковых карточек обеспечивает хорошую защиту потребителя, поскольку позволяет клиентам вернуть товар в течение определенного времени и оспорить выплаты, поскольку сумма не сразу перечисляется с банковского счета клиента. Пластиковые карточки не привязаны к национальным валютам. Независимо от места покупки товаров конвертация валюты осуществляется для клиента автоматически.

Для защиты владельца карточки в платежных системах Visa и MasterCard используются дополнительные идентификаторы карточки CVC2 (Control Verification Code), CVV2 (Control Verification Value). Узнать это число можно,

только имея физический доступ к карте в момент совершения сделки (предполагается, что эту возможность имеет только владелец). В настоящее время эти дополнительные идентификаторы входят в стандартный формат авторизационных сообщений, проверка которых осуществляется в банках-эмитентах.

6.1.3. Технология WebMoney Transfer

Эта технология реализует мгновенные расчеты, для проведения которых не требуется открывать банковский счет. Действующий в системе порядок идентификации позволяет однозначно определять и фиксировать все проводимые операции, а специальный комплекс мер безопасности полностью исключает несанкционированный доступ к средствам и информации. С помощью встроенной службы конфиденциальных сообщений можно вести защищенную переписку с другими участниками, обсуждать детали сделок, комментировать проведение платежей.

Все процессы, совершаемые в системе, – хранение электронной наличности в кошельках, выписка счетов, расчеты между участниками системы, обмен сообщениями – выполняются с использованием алгоритма шифрования, аналогичного RSA, с длиной ключей не менее 1024 бит. Для каждой транзакции назначаются уникальные сеансовые ключи. Если та или иная операция не была успешно завершена, она не учитывается системой.

Средством расчетов в системе служат титульные знаки WebMoney (WM) нескольких типов, хранящиеся в кошельках (электронных счетах) их владельцев: WM-R – эквивалент рублю России – в R-кошельках, WM-Z – эквивалент доллару США – в Z-кошельках, WM-B – эквивалент рублю Республики Беларусь – в B-кошельках. При переводе средств используются однотипные кошельки, а обмен WM-R на WM-Z производится в обменном пункте. WebMoney – полностью закрытая система, обслуживаемая только одним банком. Алгоритмы работы программного обеспечения являются секретом. Несмотря на заявления руководства WebMoney о реализованной анонимности расчетов, это заявление подвергается сомнению, поскольку все транзакции

проходят через единственный процессинговый центр WebMoney, где их легко отследить.

6.1.4. Проблемы безопасности в электронной коммерции

В соответствии с данными международных платежных систем все конфликты, связанные с электронной коммерцией (ЭК), делятся в основном на три класса:

– владелец карты утверждает, что никогда не проводил транзакцию через Интернет;

– владелец карты утверждает, что заказ ЭК не был выполнен;

– владелец карты оспаривает размер транзакции.

Наиболее многочисленным является первый класс отказов от платежей. Как показывают исследования, проведенные специалистами международных платежных систем, в подавляющем большинстве случаев причиной возникновения конфликта, относящегося к первому классу, является использование мошенниками похищенных реквизитов карт.

Иногда случается так, что некоторые торговые предприятия (ТП) по разным причинам не способны выполнить принятый заказ. Одна из таких причин состоит в том, что только крупные торговые предприятия имеют в своем арсенале системы управления складами, позволяющие им в любой момент времени точно определить наличие того или иного товара на складе. В результате только после приема заказа выясняется, что интересующий клиента товар в ТП отсутствует.

Третий класс конфликтов связан со случаями, когда ТП к согласованной с покупателем цене вдруг неожиданно для последнего добавляет дополнительную стоимость (налоги, плату за доставку и т. д.).

6.1.5. Классификация типов мошенничества в системах микроплатежей

Классификация возможных типов мошенничества, приводимая международными платежными системами:

– внедрение на клиентский компьютер вредоносной программы, которая несанкционированно расходует средства с электронного кошелька;

– перехват данных в канале связи между плательщиком и получателем платежа;

– внедрение ложного эмитента. Во многих платежных системах предусмотрена авторизация клиента сервером, но отсутствует авторизация сервера клиентом;

– атака на эмитент;

– транзакции, выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т. п.);

– компрометация данных (получение данных о клиенте через несанкционированный доступ к базам данных ТП или путем перехвата сообщений покупателя, содержащих его персональные данные) с целью их использования в мошеннических целях;

– интернет-магазины, возникающие, как правило, на непродолжительное время, для получения от покупателей средств за несуществующие услуги или товары;

– злоупотребления ТП, связанные с увеличением стоимости товара по отношению к предлагавшейся покупателю цене или повтором дебетирования счета клиента;

– интернет-магазины и торговые агенты, предназначенные для сбора информации о реквизитах карт и других персональных данных покупателей.

6.1.6. Протоколы защиты электронных платежей

Протокол SSL. Протокол SSL предоставляет «безопасный канал» со следующими характеристиками:

– является частным (шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа);

– аутентифицирован (серверная сторона диалога всегда аутентифицируется, в то время как клиентская – аутентифицируется опционно);

– надежен (транспортировка сообщений включает в себя проверку целостности с привлечением MAC-адресов).

Безопасность проводимой транзакции также зависит от правильности настройки безопасности Интернет-соединения. Для обеспечения безопасного соединения с Интернетом в диалоговом окне «Internet Options» интернет-браузера необходимо включить следующие параметры безопасности:

– Check for publisher's certificate revocations;

– Check for server's certificate revocations;

– Check for signature on downloaded programs;

– Enable Integrated Windows Authentication;

– Enable Profile Assistant;

– Use SSL 3.0;

– Warn about invalid site certificate;

– Warn if changing between secure and not secure mode.

Протокол SET. Используется для операций с кредитными карточками (Secure Electronic Transactions – SET). В отличие от SSL протокол SET узко специализирован. Целью SET является обеспечение безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция реализуется через Интернет.

Рассмотрим функции, которые осуществляет SET на различных уровнях:

– аутентификация. Все участники кредитных операций идентифицируются с помощью электронных подписей. Это касается покупателя, продавца, банка-эмитента и банка-эквайера;

– конфиденциальность. Все операции производятся в зашифрованном виде;

– целостность сообщений. Информация не может быть подвергнута модификации по дороге – в противном случае это будет сразу известно;

– присоединение. SET позволяет подключить к базовому сообщению дополнительный текст и послать его одному из партнеров;

– безопасность. Протокол должен обеспечить максимально возможную безопасность операции, достижимую в имеющихся условиях;

– совместимость. Должна быть предусмотрена с любыми программными продуктами и с любыми сервис-провайдерами;

– независимость от транспортного протокола. Безопасность операций не должна зависеть от уровня безопасности транспортного протокола. Такие гарантии особенно важны, так как протокол SET ориентирован для работы в Интернете.

На более высоком уровне протокол SET поддерживает все возможности, предоставляемые современными кредитными карточками: регистрация держателя карточки, регистрация продавца, запрос покупки, авторизация платежа, перевод денег, кредитные операции, возврат денег, отмена кредита, дебитные операции.

Таблица 6.1

Основной набор команд протокола SET

Команда	Действие	Примечание
PReq	Генерируется после принятия решения о покупке	Является предшествием заказа какого-либо товара или услуги
CredReq	Соответствует выдачи кредита	
CredRevReq	Возврат кредита	
AuthReq	Авторизация клиента	
AuthRevReq	Отказ в авторизации	
CapReq	Генерируется в случае приобретения товара	

Необходимым условием создания глобальной системы аутентификации, основанной на использовании асимметричных алгоритмов шифрования, является наличие иерархической однокорневой системы центров сертификации, которая отсутствует в протоколе SSL. Основные функции системы центра сертификации – генерация и распределение сертификатов открытых ключей, обнов-

ление сертификатов, а также генерация и распределение списков отозванных ключей (Certificate Revocation Lists – CRL).

6.2. Лабораторное задание

Совершить покупку ноутбука стоимостью 1 200 000 белорусских рублей или оплатить услуги по написанию реферата стоимостью 2000 белорусских рублей (в соответствии с предложенным заданием) посредством сети Интернет.

1. Запустить файл ZSMP.exe на выполнение.

2. Зарегистрироваться. Для этого необходимо нажать кнопку «Регистрация» и в выпадающем меню заполнить поля «Имя, Фамилия» «№ группы». После чего необходимо закрыть выпадающее меню.

Рис. 6.1. Окно регистрации

3. Изучить теоретический материал. Для этого необходимо нажать кнопку «Теория». Управление перемещением текста в данном окне выполняется путем перемещения указателя положения страницы на полосе прокрутки в правой части окна. Выход из раздела теории выполняется нажатием на кнопку «Выход».

4. Для выполнения задания необходимо нажать кнопку «Задание». Исходя из условия задания, необходимо выбрать способ оплаты, при помощи которого возможно произвести платеж (рис. 6.1). Правильность выбора сообщается по окончании работы.

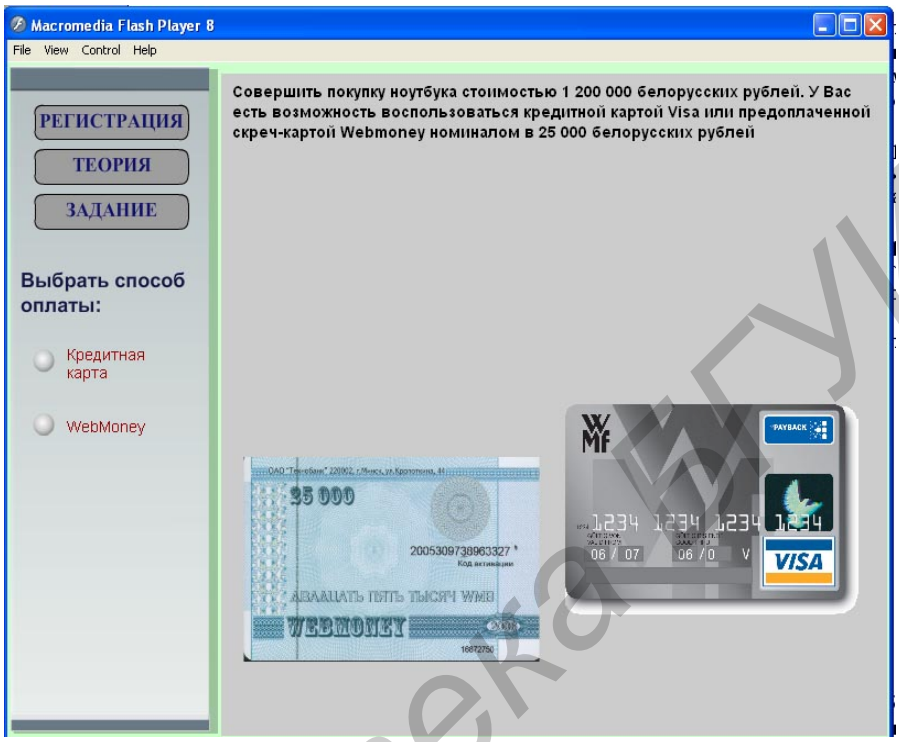

Рис. 6.2. Окно выбора способа оплаты товара или услуги

5. В случае выбора способа оплаты с помощью кредитной карты в следующей форме необходимо будет отметить поля, которые заполняются при осуществлении покупки. Подтверждение выбора осуществляется нажатием на значок в виде сферы под перечнем полей. Правильность выбора контролируется программой.

6. Следующий шаг – выбор протокола защиты выполняемой транзакции (SSL или SET).

7. В случае выбора протокола SSL – в следующем окне будет предложено правильно настроить параметры безопасности Интернет-соединения.

8. В случае выбора протокола SET – в следующем окне необходимо правильно заполнить диаграмму конечных состояний системы, использующей протокол SET.

9. В случае выбора способа оплаты с помощью системы WebMoney – в последующих окнах будут предложены деморолики, иллюстрирующие регистрацию, зачисление средств и оплату товара или услуги. Их просмотр осуществляется путем нажатия одноименных кнопок («1. Регистрация», «2. Зачисление», «3. Оплата») в верхней части окна. Управление каждым демороликом в отдельности выполняется с помощью панели, аналогичной панели проигрывателя Windows Media Player управления в нижней части окна, в котором воспроизводится ролик. По окончании просмотра демороликов необходимо нажать на кнопку «Подтвердить». В появившемся окне выбирают один из протоколов защиты и далее выполняют работу в соответствии с пунктами 7 и 8 данного руководства.

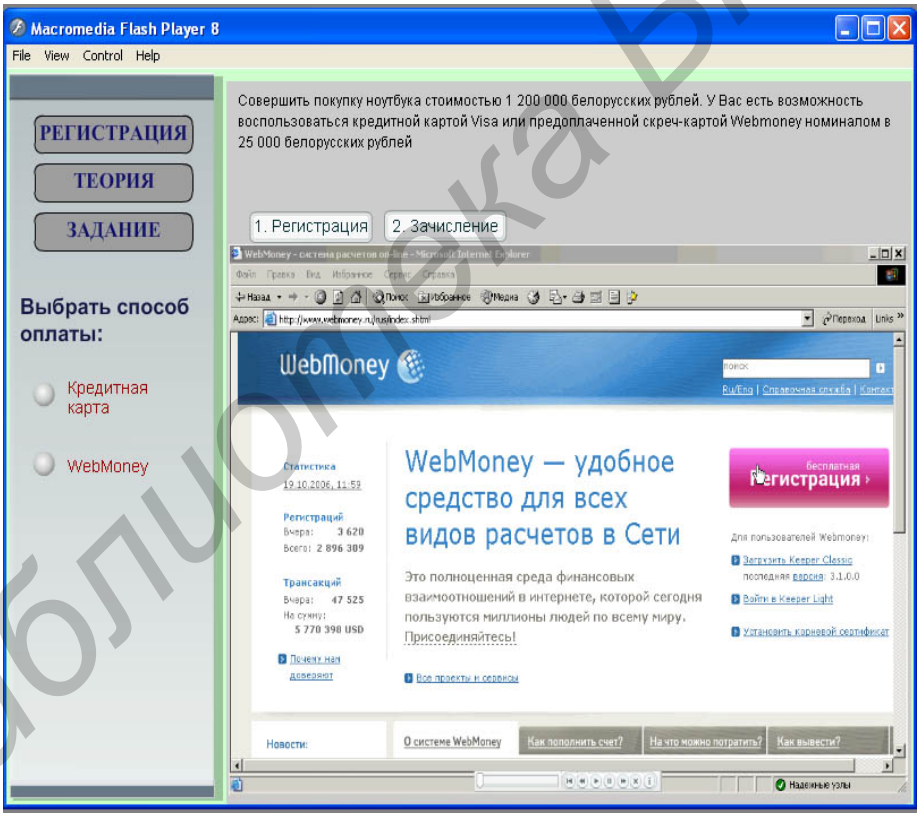

Рис. 6.3. Окно демонстрации процессов регистрации, зачисления, оплаты в системе WebMoney

10. Работа считается выполненной, в случае если в конце выполнения программы в окне отображается соответствующее сообщение о выполнении.

11. Оформить отчет.

6.3. Содержание отчета

1. Цель работы.

2. Вывод по работе.

3. Построить схему платежа в соответствии с выполненным заданием.

4. Ответы на контрольные вопросы.

6.4. Контрольные вопросы

1. Что называется электронными деньгами?

2. Какое преимущество имеют системы с оплатой товаров или услуг с помощью кредитной карты?

3. Какое преимущество имеет система с WebMoney?

4. К какой категории платежей относятся платежи в системе WebMoney?

5. К какой категории платежей относятся платежи в системах с кредитными картами?

ЛИТЕРАТУРА

1. Деднев, М. А. Защита информации в банковском деле и электронном бизнесе / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. – М. : Кудиц-образ, 2004. – 512 с.

2. Пярин, В. Безопасность электронного бизнеса / В. Пярин. – М. : Гелиос АРВ, 2002. – 432 с.

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

4. Курило, А. П. Обеспечение информационной безопасности бизнеса / А. П. Курило [и др.]. – М. : БДЦ-пресс, 2005. – 512 с.

5. Олифер, В. Г. Компьютерные сети / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2007. – 960 с.

Учебное издание

Беляев Борис Илларионович
Борботько Тимофей Валентинович
Гасенкова Ирина Владимировна и др.

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ:

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Редактор *Т. П. Андрейченко*
Корректор *А. В. Тюхай*

Подписано в печать Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. Уч.-изд. л. 8,0. Тираж 100 экз. Заказ 440.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6