ЭЛЕКТРОННАЯ @ КОММЕРЦИЯ

И. Голдовский

БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ В ИНТЕРНЕТЕ

ПИТЕР®

ЭЛЕКТРОННАЯ @ КОММЕРЦИЯ

ЭЛЕКТРОННАЯ @ КОММЕРЦИЯ

И. Голдовский

БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ В ИНТЕРНЕТЕ

ПИТЕР®

Санкт-Петербург
Москва • Харьков • Минск
2001

И. Голдовский

Безопасность платежей в Интернете

Серия «Электронная комерция»

Главный редактор	*Е. Строганова*
Заведующий редакцией	*И. Корнеев*
Руководитель проекта	*А. Васильев*
Литературный редактор	*Н. Дубнова*
Художник	*С. Маликова*
Подготовка иллюстраций	*В. Шендерова*
Корректоры	*С Беляева, Н. Лукина*
Верстка	*А. Попов*

ББК 65.262.6+32.988.02
УДК 658.8:681.324

И. Голдовский

Г60 Безопасность платежей в Интернете — СПб: Питер, 2001. — 240 с: ил.

ISBN 5-318-00562-4

Книга содержит практически полную информацию о способах безналичных расчетов в системах электронной коммерции. В ней представлен обзор рынка электронной коммерции: оценка его объема и сегментация, тенденции развития, обзор технологий, оказывающих на него существенное влияние, а также российское и зарубежное законодательство в области электронной коммерции.

Приводится подробный анализ функциональности и архитектуры протокола SET, предложения по решению проблем миграции на протокол SET с существующих протоколов (в частности, с SSL). Рассмотрены вопросы, выходящие за рамки конкретных протоколов электронной коммерции, но весьма важные для обеспечения скорейшего и эффективного внедрения безопасной системы расчетов через Интернет (Remote Server Wallet, смарт-карты и SET и т. п.).

Книга рассчитана на специалистов банков, технологических и телекоммуникационных компаний, торговых и промышленных предприятий, изучающих возможность внедрения средств электронной коммерции.

ISBN5-318-00562-4

ЗАО «Питер Бук». 196105, Санкт-Петербург, Благодатная ул.. д. 67.
Лицензия ИД № 01940 от 05.06.00.
Налоговая льгота— общероссийский классификатор продукции ОК 005-93, том 2; 95 3000 —книги и брошюры.
Подписано в печать 17.08.01. Формат 60x90/16. Усл. п. л. 15. Тираж 5000 экз.
Заказ № 2103.
Отпечатано с готовых диапозитивов в АООТ «Типография „Правда"».
191119, С.-Петербург, Социалистическая ул., 14.

Краткое содержание

Содержание

Предисловие

Эта книга была написана благодаря спонсорской поддержке одной из крупнейших международных платежных систем Europay International (сегодня компания Europay International объединяется с другим мировым лидером в области безналичных платежей — компанией MasterCard).

Компания Europay International вносит значительный вклад в дело развития электронной коммерции, и потому роль компании в качестве генерального спонсора данной книги, пропагандирующей надежные средства защиты от мошенничества при проведении расчетов по транзакциям электронной коммерции, понятна и естественна.

Автор книги в течение нескольких лет являлся членом рабочего комитета Europay Operations Advisory Committee и потому имел возможность изнутри компании Europay убедиться в том, какое внимание она уделяла развитию надежных технологий безналичных платежей.

Несмотря на то, что компания не принимала непосредственного участия в разработке спецификаций Secure Electronic Transaction (SET), ее роль в распространении и развитии этого стандарта переоценить трудно. Не случайно именно европейские банки более всех продвинулись в вопросе внедрения стандарта SET в своих системах электронных платежей.

Став одним из учредителей SETCo (компания, занимающаяся развитием стандарта, сертификацией программных продуктов на соответствие стандарту SET, а также являющаяся корневым центром сертификации в инфраструктуре центров сертификации SET), Europay немало сделала для развития SET, в частности, для утверждения одного из основных расширений протокола SET, связанного с использованием микропроцессорных карт стандарта EMV.

Фактически модель «трех доменов», введенная другим лидером электронной коммерции компанией VISA, была впервые «нащупана» Europay в форме пропагандировавшейся компанией технологии Issuer Remote Wallet. В соответствии с этой технологией функции электронного бумажника покупателя «переносились» на отдельный сервер эмитента.

Значителен вклад Europay и в развитии мобильной коммерции и в использовании карт EMV для совершения транзакций мобильной коммерции.

Для уменьшения расходов банков на внедрение дорогостоящей технологии SET компания Europay предоставляет на условиях аутсорсинга сервисы платежного шлюза, сервера эмитента и центров сертификации торговых точек, шлюзов и покупателей.

Кроме того, Europay добивается от поставщиков решений для SET скидок на их программное обеспечение для некоторых европейских банков.

С участием Europay было запущено несколько пилотных проектов по внедрению SET. В частности, в России такой пилотный проект был запущен для банка «Олимпийский».

Много усилий было предпринято Europay и в области распространения технологии виртуальных карт. В Европе было реализовано несколько десятков подобных проектов. Один из них связан с российским «Альфабанком» — первым в России эмитентом виртуальных карт MasterCard.

Весной 2001 года вместе с Maestro компания Europay представила на рынок новое оригинальное решение для эмитентов по использованию для транзакций электронной коммерции виртуальных номеров карт. Технология не только практически сводит к нулю вероятность компрометации реквизитов платежной карты во время проведения транзакции электронной коммерции, но и предоставляет дополнительные возможности по обеспечению целостности некоторой информации, связанной с транзакцией.

С 1 апреля 2001 года для повышения безопасности транзакций электронной коммерции все банки-участники платежной системы Europay используют значение CVC2 при проведении транзакций электронной коммерции.

Компания Europay предложила и целый ряд организационных инициатив, связанных с электронной коммерцией. В частности, заслуживает упоминания программа Shop Smart!, идентифицирующая наиболее надежные Интернет-магазины.

Таким образом, можно уверенно говорить о серьезном вкладе Europay International в дело развития защищенной электронной коммерции.

Компания проводит многочисленные семинары для своих банков с целью разъяснения и популяризации наиболее передовых технологий электронной коммерции. Хочется верить, что и книга внесет свой вклад в это дело.

Введение

Новые представления о пространстве и времени, рожденные теорией относительности Эйнштейна, развитие наших представлений о материи (квантовая теория поля, элементарные частицы, полупроводники, сверхтекучесть, сверхпроводимость и т. п.), появление ядерной физики (от первых представлений об атоме Резерфорда и Бора, до расщепления и синтеза атомного ядра и управляемых термоядерных реакций), полеты человека в космос и развитие космонавтики, компьютеризация общества — все это символы прошедшего XX века. За одно столетие человечество совершило в своем развитии беспрецедентный по значимости шаг вперед.

Успехи в науке привели к тому, что XX век стал веком автоматизации в самых разных областях человеческой деятельности (наука, промышленность, финансовая активность, быт и т. п.). Примером внедрения автоматизации могут служить разнообразные системы управления, созданные человеком для обеспечения надежного контроля и управления функционированием как отдельных технических устройств, так и целых отраслей промышленности.

Автоматизация коснулась широких слоев населения планеты. Сегодня на многих предприятиях для повышения эффективности работы сотрудников внедрены локальные сети персональных компьютеров, позволяющие широко использовать системы электронной почты, электронного документооборота, юридические и бухгалтерские консультационные системы и многое, многое другое.

Успешное широкомасштабное внедрение средств автоматизации стало возможным только благодаря появлению электронных вычислительных машин (ЭВМ). Компьютер наряду с ядерной физикой и космонавтикой стал одним из главных символов прошедшего века. Влияние последствий появления вычислительных машин на развитие человеческого общества переоценить невозможно.

Компьютер впервые позволил человеку обрабатывать колоссальные объемы информации в течение коротких интервалов времени. Переход «количества» в «качество» не заставил себя долго ждать. На страницах этой книги невозможно даже перечислить всего, что стало возможным благодаря появлению ЭВМ.

Не ставя себе задачу рассказать о всех победах, одержанных человеком благодаря появлению компьютера, отметим лишь два достаточно экзотических открытия — расшифровку генома человека и доказательство великой теоремы Ферма (проблемы теории чисел, стоявшей перед математиками в течение нескольких веков), — сделать которые без использования компьютера было бы весьма затруднительно.

Бурное развитие вычислительной техники, вылившееся в появление компьютеров различной производительности и назначения (от высокопроизводительных мэйнфреймов до микропроцессоров на пластиковых картах), в свою очередь стимулировало развитие систем передачи цифровой информации, объединяющих различные вычислительные средства в мощные комплексы обработки информации. Системы передачи информации прошли эволюцию от специализированных систем, позволяющих с помощью специальных протоколов подключить к центральному компьютеру его удаленные терминалы до распределенных высокопроизводительных сетей, использующих для подключения пользователей самые разнообразные, но стандартные технологии и протоколы передачи информации. По своему назначению это были сети общего доступа или корпоративные сети. Кульминацией развития сетей общего доступа стал Интернет.

Обмен информацией по каналам связи в коллективных многопользовательских системах в свою очередь потребовал решения задачи обеспечения защиты информации от несанкционированного доступа. Это стимулировало развитие криптографических методов. В 70-е годы человечество взяло на вооружение открытые стандарты шифрования информации, что было единственно возможным решением проблемы обеспечения защиты информации в больших информационных системах.

Развитие перечисленных ранее технологий происходило разными способами и разными темпами. В то же время оно имело общие черты, отражающие общие для всех технологий тенденции. О двух тенденциях хочется сказать особо.

Первая — это стандартизация используемых технических средств (аппаратных и программных). Наличие общепринятых стандартов является единственным известным человечеству способом обеспечения совместимости средств различных производителей. Нужно сказать, что люди неплохо научились решать эту задачу, придерживаясь простого правила — сначала стандарт, а потом на его основе производство.

Вторая тенденция — индивидуализация или, иначе, персонализация различных технических средств. Технологии развиваются таким образом, чтобы новые технические средства могли войти в арсенал каждого

человека. Персональные компьютеры, мобильные телефоны, Интернет — все это средства, предназначенные для индивидуального применения.

Среди достижений ушедшего века Интернет является одним из наиболее значимых. Широкое внедрение Интернета не могло не отразиться на развитии электронных форм бизнеса (e-business), одной из которых является электронная коммерция. Таким образом, электронная коммерция стала порождением самых современных технологий прошедшего столетия.

Многие крупные компании уже давно прибегают к помощи электронной коммерции (electronic commerce, или e-commerce) при проведении деловых операций. Электронный обмен данными (electronic data interchange, EDI) по частным компьютерным сетям начался в 60-х годах. Почти с того же времени банки начали успешно использовать телекоммуникационные сети для электронного перевода денежных средств (electronic funds transfer, EFT).

Системы электронной коммерции на базе протоколов EDI (ANSI X.12, EDIFACT) использовались крупными компаниями (например, такими, как General Electric, General Motors) для организации закупок комплектующих, запчастей, сырья у своих партнеров-поставщиков (системы e-procurement, или электронного снабжения). При этом обмен информацией производился через корпоративные телекоммуникационные сети этих компаний.

Системы, построенные на основе протоколов EDI, не получили широкого распространения в силу своей дороговизны. Они оказались доступными для использования только крупным компаниям.

С появлением Интернета ситуация в электронной коммерции изменилась коренным образом. У каждого пользователя персонального компьютера появилась возможность за относительно небольшие деньги получить доступ к практически любому информационному ресурсу, что полностью изменило представление об электронной коммерции. С ростом популярности Интернета и появлением новых технологий электронная коммерция вошла в жизнь многих больших и малых торговых фирм, а также частных лиц.

Электронная коммерция знаменует собой третий этап развития Интернета (бизнес в Интернете начинался с услуг Internet Service Provider, далее сменился обеспечением информационного наполнения Интернета и сегодня в значительной степени представлен различными системами электронной коммерции). При этом ее развитие не является

монотонно возрастающей функцией времени. Бум в электронной коммерции, отмеченный летом 2000 г., уже к концу того же года сменился массой пессимистических сообщений, связанных с закрытием или сокращением персонала целого ряда Интернет-магазинов и Интернет-компаний.

Такое развитие событий не следует драматизировать, вынося электронной коммерции смертный приговор, как это иногда делается в прессе. Оно характерно для начального этапа развития любого бизнеса, когда новая технология берется на вооружение, и в тех случаях, когда она бизнесу не очень нужна. В результате часть пионеров, не продумавших до конца необходимость использования электронной коммерции для решения своих задач, была вынуждена сойти с дистанции.

Электронная коммерция считается одним из видов электронного бизнеса. В соответствии с документами ООН, бизнес признается электронным, если хотя бы две его составляющие из четырех (производство товара или услуги, маркетинг, доставка товаров и расчеты) осуществляются с помощью Интернета. Поэтому в такой интерпретации обычно полагают, что покупка относится к электронной коммерции, если как минимум маркетинг (организация спроса) и расчеты производятся средствами Интернета.

Более узкая трактовка понятия «электронная коммерция» характеризует системы безналичных расчетов на основе пластиковых карт. В этом случае операция покупки считается электронной, если реквизиты карты передаются торговому предприятию или его агенту через Интернет. При этом товар может предлагаться на продажу без помощи Интернета, например через журнальные каталоги.

И все-таки наиболее популярная трактовка электронной коммерции состоит в следующем. Под электронной коммерцией подразумевается продажа товаров, при которой как минимум организация спроса на товары осуществляется через Интернет. При этом способ оплаты не имеет значения: расчеты за покупку могут совершаться даже наличными.

В настоящей книге будут использоваться два последних определения платежных систем. При этом, когда речь идет о безопасности расчетов, используется определение, введенное международными платежными системами, а в случаях, когда приводится статистика по объемам электронного бизнеса, — последнее определение.

Сегодня рынок электронной коммерции в зависимости от того, кем являются покупатель и продавец, принято делить по нескольким секторам:

- Business-to-Business (когда покупателем и продавцом являются юридические лица); сегодня это наиболее крупный сектор электронной коммерции, занимающий около 80 % всего рынка;
- Business-to-Consumer (в отличие от предыдущей схемы покупателем в этом случае является физическое лицо); на этот сектор приходится практически вся оставшаяся часть ЭК;
- Consumer-to-Consumer (покупателем и продавцом в этом случае являются физические лица; типичный пример — аукционы);
- Business-within-Business (когда роль покупателя и продавца играют различные подразделения одной и той же компании);
- Business-to-Government (выполнение заказов для правительственных учреждений).

Электронная коммерция начиналась с операций купли-продажи и перечисления денежных средств по компьютерным сетям. В ее основе лежала традиционная коммерция. При этом использование электронных сетей добавляло электронной коммерции гибкости в решении задач организации спроса и расчетов, а также в отдельных случаях и доставки товаров.

Сегодня цели электронной коммерции с точки зрения бизнеса расширились. Они включают в себя не только деловые операции, прямо связанные с куплей-продажей товаров и услуг для непосредственного извлечения прибыли. Электронная коммерция подразумевает и поддержку извлечения прибыли: например, создание спроса на товары и услуги, организацию послепродажной поддержки и обслуживания клиентов, а также повышение эффективности взаимодействия между деловыми партнерами.

Оперируя цифровой информацией в компьютерных сетях, электронная коммерция предлагает бизнесу принципиально новые возможности: например облегчает сотрудничество деловых групп. Если такие группы представляют собой подразделения одной компании, то они могут обмениваться информацией при планировании маркетинговой стратегии. Электронная коммерция поможет в совместной работе над новыми товарами или услугами, даст возможность фирмам улучшить связи с потребителями.

Коммерческая деятельность через электронные сети снимает ряд физических ограничений, естественных для работы обычных предприятий торговли и сервиса. Компьютерные системы в Интернете способны обеспечивать поддержку клиентов 24 часа в сутки, семь дней в неделю.

Заказы на продукцию могут приниматься в любое время и из любого места нашей планеты.

Развитию электронной коммерции в немалой степени способствовало отсутствие таможенных ограничений. Еще в 1996 г. специализированная комиссия ООН опубликовала «Акт о беспошлинной электронной торговле и международном торговом праве». С 1998 г. беспошлинную электронную торговлю ведут страны Европейского Союза и США. В мае того же года решение о введении беспошлинной торговли приняла Всемирная Торговая Организация, членом которой готовится стать Россия.

Электронная коммерция предлагает новые формы организации предприятия и ведения бизнеса. Примером может служить фактически символ электронного бизнеса — книготорговая фирма Amazon из Сиэтла. Не имея традиционных магазинов с прилавками, она продает всю продукцию через Интернет и напрямую координирует доставку товаров от издателей к покупателям.

Другой пример новой формы организации бизнеса — компания Software.net. Вся продукция этой компании — коммерческое программное обеспечение, находится на том же компьютере, который используется для приема заказов через Интернет.

В результате оборотные фонды компаний Amazon и Software.net полностью цифровые.

Ключевым вопросом любой коммерческой сделки является способ ее оплаты. При широком разнообразии механизмов оплаты, как существующих, так и разрабатываемых, эта часть электронной коммерции наиболее подвижна и чувствительна к изменениям. Покупатели могут использовать пластиковые карты, электронные чеки, цифровую наличность, смарт-карты и т. п.

В настоящей книге в основном рассматривается способ оплаты по пластиковым картам, являющийся на сегодняшний день наиболее универсальным и хорошо апробированным методом безналичной оплаты товаров и услуг.

Ожидается, что позиции этого способа оплаты только укрепятся по мере распространения микропроцессорных карт, осуществляемого сегодня всеми крупнейшими международными платежными системами. Микропроцессорные карты обладают рядом существенных преимуществ по сравнению с другими средствами оплаты. К числу таких преимуществ в первую очередь следует отнести высокую защищенность операций от мошенничества благодаря применению криптографических методов,

реализуемых картой, а также наличие широкого набора терминальных устройств, в которых покупатель может совершить операцию электронной коммерции с помощью микропроцессорной карты (персональный компьютер, GSM-телефон, приставка для телевизионного приемника Set-Top-Box).

Значение микропроцессорных карт для развития электронной коммерции возрастает с ростом рынка этих карт. Крупнейшие платежные системы еще в 1996 г. признали стандарт EMV и объявили о миграции всех своих карточных продуктов с магнитной полосой на смарт-карты, поддерживающие этот стандарт. Протоколы, разработанные для электронной коммерции, учитывают этот факт и позволяют эффективно использовать EMV-карты в электронной коммерции.

В свою очередь и стандарты в области микропроцессорных карт развиваются в направлении учета требований электронной коммерции. Так в 1999 г. в версии v.3.1.1 стандарта EMV были опубликованы спецификации Chip Electronic Commerce, а в последней версии 4.0 того же стандарта, принятой в июне 2000 г., приводится определение процедуры, позволяющей объединить выполнение команды Generate AC (команда генерации криптограммы) и динамической аутентификации карты (Dynamic Data Authentication). Новая процедура весьма полезна для реализации мобильной и телевизионной коммерции.

На конгрессе GSM World Congress, прошедшем в феврале 2001 г. в Каннах, впервые была продемонстрирована транзакция мобильной коммерции, выполненная по карте, поддерживающей стандарт EMV. Карта была создана компанией Oberthur и содержала два приложения: M/Chip Lite (версия стандарта EMV международных платежных систем Europay/MasterCard) и приложение SIM GSM. Транзакция была выполнена с помощью телефона Motorola Timeport GSM. EMV-приложение использовалось для расчетов за электронную покупку, а приложение SIM GSM — для выполнения стандартных функций, оговоренных в протоколе мобильной связи GSM.

Относительно недавно появился международный стандарт на электронный кошелек CEPS (Common Electronic Purse Standard). Электронные кошельки, поддерживающие этот стандарт, а также уже получившие распространение электронные кошельки Mondex, GeldKarte, Proton, VISA Cash, несомненно, со временем займут свою нишу в электронной коммерции.

Вполне возможно, что уже в ближайшие годы появятся новые методы оплаты. В частности, весьма перспективным представляется быстро развивающийся способ оплаты товаров небольшой стоимости с помощью

микроденег (microcash) или электронной наличности. Сегодня на слуху системы электронной наличности eCash, DigiCash, Web Money Transfer, PayCash, CyberCash и другие.

Электронная коммерция развивается на наших глазах. Хотя еще не исчерпаны все возможности, обеспечиваемые текущим уровнем технологического развития, новые сетевые технологии и прикладные программы могут появиться уже завтра. Здесь в первую очередь следует отметить появление новых средств доступа в Интернет, повышающих возможности клиентов. К таким средствам доступа относятся устройства Set-Top-Box, предназначенные для организации интерактивного телевидения, мобильные телефоны стандарта GSM, карманные персональные компьютеры (Personal Digital Assistant).

Ожидается, что в ближайшем будущем мобильный телефон станет самым распространенным средством проведения операции покупки в электронной коммерции. По данным некоторых исследований уже в 2004 г. с помощью мобильной коммерции (часто для обозначения мобильной коммерции используется термин m-comrnerce) будет совершаться около 40 % электронных покупок.

Значительное внимание уделяется и развитию телевизионной коммерции (t-commerce). Телевизор остается самым массовым и привычным электронным устройством, находящимся в распоряжении человека. Новые формы цифрового телевидения позволяют эффективно использовать его и для решения задач финансового рынка, в частности, электронного бэнкинга и электронной коммерции. Сегодня устройства управления Set-Top-Box от компаний Pace, Philips, Pioneer и Sony уже прошли сертификацию на совместимость со стандартом EMV по уровню Type Approval Level I. Об использовании микропроцессорных карт в электронной коммерции в этой книге будет рассказано подробно.

Настоящая книга посвящена главным образом одному аспекту электронной коммерции — расчетам. Эта часть электронной коммерции является наиболее сложной и фундаментальной. От качества организации расчетов (особенно от обеспечения их безопасности) зависит успех любого бизнеса, основанного на технологии электронной коммерции в целом.

Первоначально в планы автора входило дополнительно рассказать о построении Интернет-магазинов и организации Интернет-коммерции в целом. По мере работы над книгой стало понятно, что перечисленные аспекты должны стать темой отдельной книги. Слишком обширной и специфической по содержанию оказалась главная тема — безопасность электронной коммерции.

В книге рассмотрены все известные на сегодняшний день протоколы электронной коммерции, включая SET, 3D SET, SSL, 3D SSL, 3D Secure, технологию виртуальных номеров карт (Proxy Numbers). Обсуждаются достоинства и недостатки рассмотренных протоколов. Проводится их сравнение.

Несмотря на то что спецификации протокола Secure Electronic Transaction общедоступны, в книге, пожалуй, впервые на русском языке приводится достаточно подробное описание процедур получения сертификатов и совершения электронных покупок с комментариями, поясняющими необходимость тех или иных шагов алгоритмов протокола.

Для того чтобы читатель смог полностью разобраться с основными принципами, лежащими в основе протоколов безопасной коммерции, автор в отдельной главе постарался дать общее представление о современной прикладной криптографии. Автор надеется, что это поможет читателю оценить качество отдельных протоколов с точки зрения обеспечиваемой ими безопасности и экономии потребляемых вычислительных ресурсов.

Помимо описания протоколов Интернет-коммерции и обсуждения их достоинств и недостатков, читатель сможет познакомиться с правилами международных платежных систем, относящимися к электронной коммерции. Не остались без внимания и вопросы стандартизации в области электронной коммерции, а также правовые аспекты этого бизнеса.

Автор также посчитал необходимым дать в начале книги краткий обзор рынка Интернет-коммерции, а также рассказал о главных факторах, оказывающих влияние на эту технологию. Это было важно сделать не только для того, чтобы дать представление читателю о текущем состоянии дел в электронной коммерции. Необходимо также понять, в каком направлении будет развиваться эта технология. От правильного понимания тенденций развития электронной коммерции зависит успех технического и технологического обеспечения этой новой формы ведения бизнеса.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу электронной почты comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

Подробную информацию о наших книгах вы найдете на Web-сайте издательства http://www.piter.com.

Глава 1. Краткий обзор рынка электронной коммерции

Базовые понятия и определения

На сегодняшний день банки-участники крупнейших международных платежных систем VISA, MasterCard, Europay и American Express эмитировали (выдали своим клиентам) более 2 млрд карт. Поэтому многим жителям нашей планеты хотя бы в общих чертах известно о том, что собой представляют пластиковые карты. И все-таки для того, чтобы в дальнейшем в этой книге придерживаться общей и понятной всем терминологии, коротко опишем, каким образом функционируют системы безналичных расчетов, основанные на использовании пластиковых карт.

В первую очередь необходимо отметить, что платежная система представляет собой ассоциацию банков, называемых банками-участниками этой платежной системы. Когда банк присоединяется к ассоциации (вступает в нее), он тем самым подтверждает свою готовность и берет на себя обязательство следовать правилам этой ассоциации (платежной системы), определяющим технические, юридические и финансовые аспекты функционирования банка в системе. Такое признание банком правил системы является основой для взаимного доверия между неизвестными друг другу банками при организации ими безналичных расчетов для своих клиентов.

В платежной системе банк может выступать в двух ипостасях: во-первых, в качестве банка-эмитента и, во-вторых, в качестве обслуживающего банка. Каждый банк может быть одновременно и эмитентом и обслуживающим банком.

В качестве эмитента банк выдает своему клиенту (физическому и/или юридическому лицу, имеющему в данном банке счет) специальное удостоверение (пластиковую карту), обеспечивающее удаленный доступ клиента к своему счету с целью получения различных услуг: безналич-

ная покупка в торговом предприятии (ТП), получение наличных в банкомате или отделении банка и т. п. Таким образом, пластиковая карта связана со счетом (счетами) клиента в банке.

Пластиковая карта содержит логотипы платежной системы и банка-эмитента, голограмму платежной системы и специальные символы, повышающие устойчивость карты к возможным ее подделкам, а также информацию, называемую реквизитами карты (номер карты, срок ее действия, имя владельца карты, код обслуживания, специальную информацию, генерируемую эмитентом и используемую им для проверки подлинности карты). Часть этой информации наносится на пластик карты с помощью специальной печати и считывается в процессе совершения транзакции визуально. Эта информация используется продавцом ТП для проведения так называемой голосовой авторизации. Другая часть информации наносится на магнитную полосу и/или микропроцессор (чип), расположенные на карте. Информация с магнитной полосы или чипа считывается с помощью специальных устройств, называемых считывателями карты или карт-ридерами. Электронные терминалы в ТП (Point-of-Sale, или POS-терминалы), а также автоматические устройства выдачи наличных (банкоматы) оснащены подобными карт-ридерами.

Обслуживающий банк обеспечивает поддержку инфраструктуры приема пластиковых карт, к которой в общем случае относятся банкоматы, пункты выдачи наличных и предприятия торговли и сервиса (в мире насчитывается около 21 млн торговых предприятий, принимающих в качестве средства оплаты своих товаров пластиковые карты). Обслуживающий банк заключает договоры с торговыми предприятиями на обслуживание в них пластиковых карт, гарантируя торговому предприятию возврат средств за операцию, совершенную в нем по карте любого банка-участника платежной системы.

Когда клиент банка А собирается совершить покупку в ТП обслуживающего банка В, то торговое предприятие в первую очередь должно убедиться в том, что в соответствии с договором с обслуживающим банком В операция по предъявляемой для оплаты карте будет возмещена. Другими словами, ТП должно убедиться в том, что банк-эмитент А и обслуживающий банк В являются участниками одной платежной системы. Это устанавливается по логотипу платежной системы, нанесенному на пластиковой карте клиента.

Процесс оплаты услуги в общем случае состоит из двух частей. Первая часть — авторизация транзакции. Схематично она показана на рис. 1.1.

Рис. 1.1. Авторизация транзакции

ТП «считывает» с предъявляемой клиентом для оплаты покупки пластиковой карты необходимую информацию, а также, возможно, получает некоторую идентифицирующую клиента информацию непосредственно от самого клиента (например, персональный идентификационный номер владельца карты). Полученная от клиента и считанная с карты информация, а также информация о покупке (сумма покупки, валюта транзакции и т. п.) и торговом предприятии (идентификаторы ТП и устройства приема карты) передается торговым предприятием своему обслуживающему банку в форме авторизационного запроса. С помощью авторизационного запроса ТП спрашивает у обслуживающего банка, может ли оно предоставить данному клиенту запрашиваемую им услугу. В свою очередь обслуживающий банк обращается за разрешением на оказание услуги к банку-эмитенту А. При этом банки А и В обмениваются сообщениями в соответствии с правилами, установленными платежной системой. Поэтому синтаксис и семантика сообщений понятна обоим банкам.

Эмитент А, получив запрос от обслуживающего банка В, проверяет достоверность информации о карте и ее владельце: правильность реквизитов карты и идентификатора владельца карты. После этого банк А определяет достаточность средств на счете клиента для оплаты запрашиваемой им услуги. Если все проверки завершились успешно, банк А отвечает на запрос банка В разрешением на совершение покупки, предварительно списав (или только «заморозив») со счета клиента стоимость покупки вместе с некоторыми установленными им комиссиями.

Получив разрешение от банка А, обслуживающий банк в свою очередь разрешает операцию покупки своему ТП, тем самым гарантируя последнему возмещение средств за совершаемую торговым предприятием продажу товара/услуг. В большинстве случаев, если обслуживающий банк представил эмитенту правильную и достаточную (по правилам системы) для авторизации информацию, ответственность за транзакцию в случае возникновения спора (диспута) ложится на эмитента.

Вторая часть безналичной оплаты товаров/услуг заключается в расчетах между всеми участниками транзакции. Как уже отмечалось, ТП получает возмещение за операцию покупки от своего обслуживающе-

го банка. Обслуживающий банк в свою очередь получает возмещение с банка-эмитента. Гарантом расчетов между банками выступает платежная система. В этом состоит ее важнейшая функция. Расчеты, как правило, производятся безакцептно (то есть без получения специального разрешения) через специальные счета, открываемые банками в расчетных банках платежной системы.

Наконец, банк-эмитент списывает средства со счета своего клиента. Таким образом, при участии и гарантии платежной системы реализуется передача средств со счета клиента на счет ТП.

Основанием для расчетов между участниками транзакции могут быть авторизационные сообщения, которыми обменялись в процессе совершения транзакции обслуживающий банк и банк-эмитент. В этом случае по окончании бизнес-дня платежная система на основе имеющейся у нее информации осуществляет расчеты между всеми своими банками-участниками за прошедший бизнес-день. Системы, в которых расчеты производятся на основании авторизационного трафика, называются Single Message System (SMS).

Иногда правила платежной системы таковы, что для инициализации расчетов между участниками транзакции обслуживающий банк должен отправить в платежную систему специальное сообщение, которое далее передается банку-эмитенту. Только на основании этого сообщения платежная система осуществит расчеты между всеми ее банками-участниками. Специальное сообщение называется презентментом (presentment), а системы, производящие расчеты на основе презентментов, — Dual Message System. Сегодня большинство международных платежных систем относятся именно к этому классу систем.

Несмотря на то что системы Dual Message System являются функционально более гибкими, их техническая поддержка является более сложной. В результате общая тенденция состоит в переходе всех систем на режим SMS.

В платежной системе время от времени по различным причинам могут возникать споры (диспуты) между банком-эмитентом и обслуживающим банком, связанные с некоторой транзакцией, имевшей место в системе. Например, владелец карты может утверждать, что никогда не совершал транзакции, за которую с его счета были списаны деньги, или совершал транзакцию, но на другую сумму. Жизнь многогранна и подобных «или» может быть очень много. Для разрешения возникающих споров платежные системы разрабатывают правила, предусматривающие использование специальных сообщений, которыми обмениваются банки-участники системы.

В частности, если банк-эмитент считает, что некоторая транзакция, выполненная по карте его клиента, является по каким-то причинам неверной (например, клиент не совершал данной транзакции, сумма транзакции является неправильной, транзакция является дубликатом транзакции, по которой безналичные расчеты уже были совершены и т. п.), он направляет обслуживающему банку специальное сообщение, называемое chargeback (отказ от платежа). На основании этого сообщения платежная сеть возвращает на счет банка-эмитента средства, связанные с транзакцией, на которую пришел chargeback. Возвращаемые средства списываются со счета обслуживающего банка. Далее банк-эмитент возвращает списанные средства на счет клиента.

Операции безналичных расчетов в платежных системах называют транзакциями. Платежные системы поддерживают транзакции различных видов: покупка, снятие наличных в отделении банка, снятие наличных в банкомате, получение информации об остатке на счете клиента и другие.

Транзакции различаются также по способу представления информации о карте в платежную систему. Существуют электронные транзакции (информация о карте считывается с магнитной полосы/чипа) и транзакции голосовой авторизации (paper-based).

По определению CNP-транзакция (Cardholder Not Present) представляет собой операцию покупки по пластиковой карте, в момент совершения которой клиент не присутствует лично в предприятии торговли/сервиса, а сообщает торговому предприятию (ТП) реквизиты своей карты (обычно номер карты и ее срок годности), необходимые для проведения авторизации, заочно (письмом, по телефону, сети передачи данных и т. д.).

В этой книге всякий раз, когда речь идет о расчетах с помощью пластиковой карты, под транзакцией электронной коммерции (ЭК) понимается CNP-транзакция, при совершении которой обмен данными между владельцем пластиковой карты и ТП о реквизитах карты происходит через Интернет.

Обычно процесс покупки в ЭК выглядит следующим образом. Клиент с помощью персонального компьютера (или другого устройства, например GSM-телефона), подключенного к сети Интернет, выбирает интересующие его товары в виртуальной витрине (Storefront) товаров Web-сайта торгового предприятия. Подтвердив выбор товаров и согласие с их стоимостью, клиент сообщает ТП о желании заплатить за покупку с помощью пластиковой карты.

Далее происходит диалог между ТП и владельцем карты, целью которого является получение реквизитов карты покупателя для их пред-

ставления в сеть в виде стандартного авторизационного запроса. В течение этого диалога ТП и покупатель иногда имеют возможность аутентифицировать друг друга, что обеспечивает безопасность транзакции ЭК.

Полученные от клиента данные о реквизитах карты (кстати, ТП может и «не видеть» эти данные) торговое предприятие передает своему обслуживающему банку, который на основе этих данных формирует и представляет в сеть авторизационный запрос. Начиная с этого момента, транзакция обрабатывается по тем же правилам, что и обычная операция покупки по пластиковой карте. Авторизационный запрос обслуживающего банка в виде сообщения в формате, принятом в соответствующей платежной системе, передается банку-эмитенту клиента, который авторизует транзакцию и о результате авторизации сообщает обслуживающему банку. Обслуживающий банк передает ТП решение эмитента, которое сообщается владельцу карты. В случае успешного завершения транзакции клиент получает электронный чек, содержащий адрес ТП в Интернете, название ТП, сумму покупки и т. п.

На этом обработка транзакции ЭК может завершиться, и тогда между всеми участниками транзакции будут произведены расчеты. Иногда транзакция считается завершенной только после того, как ТП передаст обслуживающему банку специальное сообщение, подтверждающее факт выполнения торговым предприятием заказа, связанного с покупкой.

Возможность совершить покупку заочно (без присутствия покупателя в ТП) всегда являлась привлекательной как для покупателя, так и для продавца. Для покупателя — из-за удобства способа (не выходя из дома, в любое время суток, в спокойном режиме без очереди и т. п.), для продавца — благодаря, главным образом, возможности снижения накладных расходов на организацию торговли и возможности круглосуточно рекламировать свой товар широкой аудитории потенциальных покупателей.

На первом этапе развития «заочной» торговли наиболее распространенным способом проведения такой покупки был заказ товара по почте, телеграфу и телефону. Поэтому подобные транзакции получили название MO/TO-транзакций (Mail Order/Telephone Order). Единственная проблема в то время состояла в организации расчетов за такие покупки. Продавцу хотелось заранее идентифицировать покупателя и убедиться в его кредитоспособности. С распространением пластиковых карт эта проблема частично решилась — у торгового предприятия появилась возможность получить относительно надежные **гарантии** кредитоспособности покупателя.

Относительность гарантии заключалась в том, что при заочных покупках вероятность мошенничества по кредитным картам все-таки оставалась высокой. Для успешного выполнения операции заочной покупки достаточно было знать всего лишь номер карты и ее срок действия.

Основные предпосылки к развитию электронной коммерции

Ситуация в области «заочных» покупок стала качественно меняться по мере распространения Интернета как глобальной среды информационного взаимодействия пользователей друг с другом. Быстрому развитию электронной коммерции через Интернет способствуют:

- быстрый рост продаж персональных компьютеров (оценка скорости роста числа проданных PC, сделанная в 1998 г., показала увеличение в 10 раз за 10 лет);
- стремительный рост производительности процессоров, памяти и каналов передачи данных (в соответствии с законом Мура время удваивания перечисленных выше показателей составляет соответственно, 18, 12 и 9 месяцев);
- отсутствие таможенных налогов, связанных с электронными продажами;
- быстрое распространение альтернативных средств доступа в Интернете, прежде всего — мобильных телефонов и интерактивного телевидения;
- относительно низкая стоимость доступа в Интернет, а также постоянная тенденция к уменьшению платы за доступ в Интернет и пользование его ресурсами;
- повышение безопасности обработки транзакций в Интернете благодаря появлению новых технологий и стандартов, связанных с ЭК;
- удобство и простота технологии электронных покупок через Интернет для покупателя: интересующий его товар можно приобрести не выходя из дома, в любое время суток, без очереди и т. п.;
- возможность для покупателя получить предложение на покупку интересующего его товара сразу от многих ТП;
- доступность информации о товарах и услугах в Интернет-магазинах в режиме реального времени;
- возможность для ТП дать предложение по продаже своих товаров большой аудитории потенциальных покупателей;

- привлекательность ЭК для ТП в связи с уменьшением накладных расходов на организацию бизнеса.

В основе развития ЭК лежат бурный рост сети Интернет и компьютеризация населения. К концу 1996 г. число пользователей Интернета по разным оценкам насчитывало 50-60 млн человек. По данным исследования, проведенного компанией Nua, в начале 2001 г. Интернетом пользуются 407,1 млн, что более чем в два раза превышает количество пользователей в сентябре 1999 г. В частности, быстрый рост числа пользователей наблюдался в Азиатско-Тихоокеанском регионе: в настоящее время количество пользователей Интернета здесь превышает 100 млн человек. При этом на регион приходится 26 % всего населения мира. Лидером по количеству пользователей Интернета продолжает оставаться Северная Америка. На нее приходится 41 % всех пользователей. Однако в 2000 г. наблюдалось снижение темпов роста количества пользователей Сети в этом регионе, что во многом объясняется близостью рынка к насыщению. В Европе проживает 27,8 % всех пользователей Интернета, в Латинской Америке — 4 %, в Африке — 0,8 %, а на Среднем Востоке — 0,6 %.

В США, которые являются мировым лидером по числу пользователей Интернета, в 2001 г. зарегистрировано 110,83 млн пользователей (около 41 % населения страны).

Другими лидерами по критерию «доля пользователей Интернета среди всех жителей страны» являются Швеция (44 %), Великобритания (24 %), Голландия (19 %), Германия (15 %), Франция (10 %), Италия (8 %), Испания (7 %).

Сегодняшние темпы роста числа пользователей Интернета составляют 92 % в год.

По данным monitoring.ru, размер аудитории российской части Интернета (Рунет) на конец 2000 г. равнялся 11,4 млн человек, что составляло 10,3 % от взрослого населения страны (110,5 млн человек). Аудитория Рунета продолжает увеличиваться. В целом, за год (с ноября 1999 г. по ноябрь-декабрь 2000 г.) рост составил ПО % (примерно на 20 % выше, чем в среднем в мире). Нерегулярная аудитория, включающая всех посетителей, кроме тех, кто имеет только единичный опыт пользования Интернетом, выросла в среднем на 0,9 млн человек (5,1 млн в мае-июне, 6,0 млн в ноябре-декабре). Недельная аудитория Рунета (те, кто регулярно посещает Интернет примерно раз в неделю) за год практически не изменилась, ее численность стабилизировалась на уровне, зафиксированном в третьем квартале 2000 г. Наиболее активная аудитория

(те, кто регулярно посещает Интернет и проводит там не менее одного часа в неделю) с ноября 1999 г. по ноябрь-декабрь 2000 г. практически не выросла. Численность активной аудитории составляет 1,8 млн человек. Ядро аудитории образуют посетители, которые проводят в Интернете не менее 3 часов в неделю. В Рунете их 900 тыс. человек.

Основной рост аудитории Рунета происходит за счет тех, кто только-только приобрел первый опыт, но не стал пока регулярным пользователем. С мая-июня по ноябрь-декабрь 2000 г. такие пользователи обеспечили рост максимальной аудитории Рунета (все посетители Интернета, включая тех, кто имел хотя бы единичный опыт посещения Сети) в среднем на 2,2 млн человек (9,2 млн в мае-июне, 11,4 млн в ноябре-декабре).

Данные monitoring.ru отличаются от прогнозов специалистов компании A. T. Kearney, оценивающих среднегодовые темпы роста числа тех, кто регулярно пользуется Рунетом, примерно на 50-70 %.

Рост аудитории Рунета сказывается и на изменении других ее характеристик. На начало 2000 г. поисковая система «Апорт» зарегистрировала в русскоязычном секторе Интернета около 70 тыс. серверов и более 6,2 млн Web-страниц, на которых размещено 54 Гбайт документов.

Сегодня 95 % всех транзакций ЭК совершается с помощью персональных компьютеров. Однако все большее распространение получают новые виды терминальных устройств, предназначенных для организации ЭК. К ним в первую очередь следует отнести мобильные телефоны стандарта GSM и устройства доступа к инте^ктивному телевидению Set-Top-box (STB-устройства). Уже в 2005 г. предсказывается следующее распределение объемов ЭК между тремя основными каналами:

- персональные компьютеры — 29 %;
- мобильные телефоны — 35 %;
- интерактивное телевидение — 36 %.

По данным VISA International наиболее перспективным средством доступа в Интернет является мобильный телефон. В частности, компания прогнозирует, что объем покупок ЭК, осуществляемых в мире в 2003 г. через мобильные телефоны, составит около $66 млрд.

Более скромные оценки предлагает компания Jupiter Media Metrix. По данным Jupiter, уже в 2001 г. владельцы сотовых телефонов потратят в Интернете около $260 млн. К 2005 году пользователями мобильного Интернета станут уже 171 млн человек, а объем продаж поднимется до $10,8 млрд.

Мобильная телефония

Остановимся коротко на мобильной телефонии и интерактивном телевидении.

В 1998 г. в Европе насчитывалось 120 млн владельцев GSM-телефонов, а к концу 1999 г. их количество достигло 170 млн. Для сравнения — число персональных компьютеров в Европе на тот же момент времени (конец 1999 г.) составляло 42 млн.

По данным различных агентств, к началу 2000 г. в мире было зарегистрировано около 470 млн абонентов сотовой связи (8 % от всего населения планеты), доля цифровых стандартов достигла 83 %, а доля стандарта GSM превысила 54 %.

Рост числа владельцев GSM-телефонов в мире происходит с космической скоростью. В соответствии с прогнозами компании Ericsson, в 2004 г. число мобильных телефонов в мире превысит 1 млрд аппаратов. Еще более оптимистичный прогноз предлагает компания Nokia. Согласно ее прогнозу планка в 1 млрд сотовых телефонов будет превышена до конца 2002 г.

Интернет-технологии и мобильная связь в настоящее время представляют собой два наиболее быстро развивающихся телекоммуникационных рынка. По прогнозу исследовательской группы Strategies Group of Washington в 2001 г. будет уже около 15,6 млн мобильных пользователей Интернета, число которых в любой стране зависит только от скорости развития сетей и возможностей оборудования передачи данных.

Сегодня мало кто сомневается в том, что мобильный Интернет в недалеком будущем станет частью нашей повседневной жизни. Основные производители средств передачи сообщений по электронной почте (IBM/Lotus Notes, MS Mail и Da Vinci eMail) уже включили возможности мобильных Интернет-коммуникаций в свои продукты. Все большее число операторов сотовой связи вместе с ISP-провайдерами предлагают услуги мобильного Интернета.

Позиции GSM-телефонов в качестве средства доступа в Интернет упрочились после появления открытого глобального стандарта WAP (Wireless Access Protocol), описывающего защищенный протокол обмена данными GSM-телефона с сервером.

Необходимость создания специального стандарта для доступа к ресурсам Интернета через мобильный телефон объяснятся двумя причинами. Во-первых, файлы, передающиеся по протоколу HTTP, трудно было бы смотреть на маленьком экране сотового телефона (минимальный размер Web-страницы — 640 x 480 пикселов, а максимальный размер

сотового телефона — 96 x 65 пикселов). Во-вторых, объемы информации, передаваемые во время проведения транзакции ЭК, совершенно не рассчитаны на те скорости связи, которые сегодня доступны владельцам мобильных телефонов (9,6 Кбит/с для телефонов в стандарте GSM и 14,4 Кбит/с для телефонов в стандарте CDMA). При этом стоит отметить, что более скоростной стандарт CDMA в России продвигается с большим трудом. В 2000 г. в стране насчитывалось не более 30 тыс. владельцев телефонов, работающих в этом стандарте.

Стандарт WAP (последняя версия 1.2) определяет полный стек протоколов, начиная с физического и заканчивая прикладным уровнем эталонной модели взаимодействия открытых систем. Он использует двоичный формат представления данных, что позволяет эффективно сжимать пакеты передаваемой информации. Кроме того, протокол адаптирован под большой период ожидания и низкую пропускную способность каналов. Специальный язык WML (производное от XML), с помощью которого создаются WAP-совместимые Web-страницы, позволяет оптимально использовать малые дисплеи сотовых телефонов, включая двухстрочные текстовые и полностью графические. Благодаря встроенному в мобильный телефон WAP-браузеру, пользователи смогут запускать различные приложения без помощи компьютера прямо на своих телефонах. Еще одно преимущество WAP — поддержка различных транспортных протоколов. Кроме того, предусматривается его совместимость с домашними радиосетями стандарта Bluetooth.

Стандарт WAP 1.2 включает в себя технологию WIM (Wireless Identity Module), обеспечивающую шифрование и цифровую подпись данных на основе алгоритмов симметричного шифрования. Это позволяет использовать WAP 1.2 для реализации проектов мобильной коммерции и банковских операций, гарантируя приемлемую безопасность этих приложений. При этом WIM-модуль находится в памяти SIM-карт (такие карты уже производятся компаниями Gemplus и Schlumberger).

В начале 2001 г. компании Nokia, KPN Mobile и голландский процессор Interpay провели успешное испытание системы m-commerce с использованием протокола WAP 1.2.

До конца 2001 г. ожидается появление версии 1.3 стандарта WAP, которая должна существенно повысить уровень безопасности приложений, функционирующих на основе беспроводной связи. Протокол WAP 1.3 будет поддерживать асимметричные алгоритмы шифрования и динамическую прокси-навигацию. Динамическая прокси-навигация является методом переадресации, поддерживающим соединение между телефонной трубкой и Web-сервером без промежуточной расшиф-

ровки данных. В настоящее время информация при ее передаче от оператора мобильной связи до сервера на разных участках передачи защищается протоколами WTLS и SSL. При переходе от одного протокола к другому данные расшифровываются и оказываются подверженными риску быть перехваченными мошенниками. В протоколе WAP 1.3 обеспечивается сквозное шифрование данных с помощью протокола WTLS.

По данным различных аналитических агентств в 1999 г. из 80 млн проданных в США и Европе радиотелефонов менее четверти были снабжены возможностями WAP-протокола. В 2001 г. их доля должна была достигнуть 95 %. Однако уже сегодня понятно, что столь массового распространения телефонов, поддерживающих WAP, не произойдет.

По мнению экспертов, срок жизни протокола WAP ограничен появлением скоростных протоколов передачи данных в мобильной телефонии, позволяющих передавать за разумное время полноценную графику. Протокол WAP для этого совершенно не приспособлен. Ожидается, что с появлением GPRS (скорость передачи данных до 115 Кбит/с) через 1-1,5 года время протокола WAP пройдет.

Таким образом, следует признать, что протокол WAP не до конца оправдал возложенные на него надежды. Это произошло по различным причинам, включая дороговизну WAP-совместимых телефонов и стоимости услуг, а также низкую скорость передачи данных в режиме коммутации каналов CSD (Circuit Switch Data).

В России получили распространение модели WAP-телефонов от компаний Motorola, Nokia и Siemens. На сегодняшний день все крупнейшие операторы сотовой связи, включая Би Лайн, МТС, North-West GSM, запустили WAP-сервисы, и абоненты этих компаний уже сейчас могут воспользоваться доступом к Интернету через мобильный телефон. При этом стоимость доступа остается высокой — от 5 до 30 центов за минуту.

В условиях относительно низкого распространения WAP операторы GSM начали поиск альтернативных вариантов доступа к уже готовым WML-сайтам с помощью существующей широкой базы аппаратов GSM фазы 2+. Идея состояла в том, чтобы средствами SIM Application Toolkit (STK) встроить в SIM-карту минибраузер, который бы формировал SMS-запросы, а также обрабатывал ответы и выводил на дисплей телефона содержащуюся в них информацию. В качестве языка представления данных рассматривался язык WML. Использование канала SMS с одной стороны уменьшает стоимость передачи данных, а с другой — позволяет обеспечить скорость работы, сравнимую с CSD.

Изложенный здесь подход получил название WML/STK-браузинга, а для его стандартизации было создано сообщество SIM Alliance (www.simalliance.org), в которое вошли ведущие производители SIM-карт: компании Bull, Gemplus, Giesike&Devrient, Graphium Denmark, Oberthur Card Systems, ORGA, Schlumberger.

Итогом работы сообщества SIM Alliance стали новые спецификации S@T (SIMAlliance Application Toolbox), определяющие функциональность минибраузера в SIM-карточке, а также уровни передачи информации в канале связи SMS и их соответствие уровням WAP-запросов.

Таким образом, решение S@T обеспечивает канал доступа к информации в формате WML на основе недорогой сетевой инфраструктуры SMS. Подключенная к любому мобильному телефону GSM фазы 2+, 5@T-совместимая карточка обеспечивает доступ к WML-услугам через сервер S@T Gateway, связанный с центром коротких сообщений.

Архитектура S@T обеспечивает встроенную сквозную безопасность между приложениями на сервере и браузером S@T, тем самым позволяя осуществлять безопасные транзакции мобильной коммерции. Обеспечение безопасности S@T пока базируется на технологиях шифрования и электронной подписи с использованием симметричных алгоритмов, хотя уже сегодня ведутся разработки спецификаций браузера с асимметричным шифрованием.

Определенный интерес для развития электронной коммерции представляют также инициативы организации Mobile Electronic Transactions Initiative (MeT) (http://www.mobiletransaction.org), сформированной несколькими лидерами индустрии сотовой связи. Эта организация выпустила спецификации в области безопасной мобильной коммерции.

Организация MeT была основана рядом лидеров телекоммуникационной индустрии, включая таких гигантов, как Nokia, Ericsson, Sony и Matsushita, с целью скорейшей разработки технологий мобильной коммерции. В дополнение к спецификациям организация прилагает несколько вариантов их использования. Спецификации можно бесплатно скачать с Web-сайта MeT.

Согласно концепции MeT, разрабатываемые технологии должны работать в рамках любых сетей, со всеми службами и любыми устройствами. В частности, спецификации обеспечивают совместимость с существующими стандартами и технологиями, такими как WAP, WTLS (протокол безопасной передачи данных), WIM, инфраструктурой открытого ключа и технологией беспроводной связи Bluetooth. Спецификации MeT обеспечивают аутентификацию владельца сотового те-

лефона, а также обеспечивают конфиденциальность и целостность информации, которой клиент обменивается с платежной системой.

Продукты, созданные с использованием спецификаций МеТ, должны появиться уже в 2001 г.

Удобным средством инициализации транзакции электронной коммерции через GSM-телефон является банковская микропроцессорная карта. Сегодня на рынке присутствуют две основные концепции организации систем мобильной коммерции. Первая основана на применении двухслотовых (dual slot) телефонов, имеющих встроенный ридер, способный считывать информацию с двух стандартных (ISO 7816-1,2,3) микропроцессорных карт. GSM-телефоны с двумя слотами (один слот для SIM-карты телекоммуникационного оператора, а второй — для платежной смарт-карты) уже демонстрировались компаниями Alcatel, Motorola, Gemplus.

Ряд банковских приложений, таких как пополнение электронного кошелька, предоставление выписок по счетам, а также иные виды мобильного банковского обслуживания и программ лояльности могут предоставляться через двухслотовые мобильные телефоны с использованием SIM-карточек, реализующих ЭЦП, уже сегодня. Подобные услуги предоставляются в ряде европейских (Германия, Швеция, Чехия), а также азиатских (Гонконг, Сингапур) стран. При этом SIM-карта обменивается информацией с чиповой картой, реализующей то или иное банковское приложение, с помощью команд, определенных стандартом GSM SIM Application Toolkit Commands GSM 11.14.

Вторая концепция основана на все возрастающих возможностях SIM-карточек, способных выполнять не только свою основную функцию модуля идентификации абонента, но и обеспечивать функционирование других приложений, например финансовых. Хорошей иллюстрацией этой концепции является недавно продемонстрированная компанией Oberthur Card Systems SIM-карта SIMphonic 3G, обеспечивающая наряду со стандартной функциональностью GSM SIM функциональность платежного приложения стандарта EMV. Вставляя эту карту в платежный POS-терминал, поддерживающий стандарт EMV, можно выполнить безналичный платеж по EMV-карте.

Важнейшую роль в развитии концепции использования SIM-карты как универсального средства для реализации доступа к сети мобильной связи и других приложений (в том числе финансовых) сыграло появление спецификаций SIM Application Toolkit (STK). Стандарт STK позволяет хранить и выполнять на SIM-карточке разнообразные прикладные программы, а также предусматривает возможность удаленного

программирования или обновления хранимой на SIM-карточке информации. При этом обеспечивается защита информации при ее передаче по радиоканалам. SIM-карты в сочетании со стандартом STK позволяют аутентифицировать абонентов на основе технологии электронной цифровой подписи, а также шифровать конфиденциальную информацию. При этом уровень безопасности, обеспечиваемый ими, выше, чем предоставляемый другими технологиями, в частности протоколом WAP.

Технология STK позволяет разрабатывать разнообразные финансовые приложения на SIM-карте. Однако на сегодняшний день не существует многофункциональной SIM-карты с полностью решенными проблемами разграничения доступа между приложениями. Поэтому несомненное достоинство концепции dual slot состоит в разделении финансовых и коммуникационных приложений с обеспечением для каждого из них независимого контроля доступа и полным исключением возможности их интерференции.

Другое достоинство этой концепции заключается в возможности построения более гибких отношений между операторами коммуникационных услуг и банками, а также в использовании различных приложений для организации безналичных расчетов в мобильной коммерции. В то же время очевидным недостатком концепции dual slot является необходимость обеспечения пользователей двухслотовыми телефонами, выбор которых невелик, а функциональные возможности и эргономика в лучшем случае средние.

Активными сторонниками концепции dual slot является банковское сообщество и платежные системы на основе пластиковых карт. Эта концепция позволяет банкам обеспечить контроль над своими приложениями.

Сотовые операторы в своем большинстве не поддерживают концепцию dual slot, являясь сторонниками концепции универсальной SIM-карты. Тем самым коммуникационные операторы пытаются сохранить имеющееся у них преимущество, связанное с тем, что GSM SIM-карта разрабатывалась прежде всего как приложение для мобильной связи. Эмиссия SIM-карт всегда контролировалась и продолжает контролироваться сотовыми операторами, которым бы очень хотелось оставить существующее положение дел как можно дольше.

Кроме того, концепция dual slot предоставляет возможность пользователю сотового телефона использовать SIM-карты различных операторов сотовой связи, что также не соответствует интересам операторов сотовой связи.

Таким образом, на сегодняшний день банковское сообщество предпочитает решения на базе двухслотовых аппаратов, в то время как телекоммуникационные операторы, а также производители мобильных телефонов идею двухслотового телефона «SIM+банковская карта» не принимают. При этом финансовые возможности многих таких операторов значительно превосходят имеющийся потенциал банковских структур. В результате отмечается борьба за клиента телекоммуникационных операторов с банковскими организациями. Причем сегодня эта борьба ведется на поле банковских услуг.

Контролируя эмиссию SIM-карт, операторы сотовой связи активно предлагают внедрение на рынке многофункциональных SIM-карт или в крайнем случае — двухслотовых SIM-карт (один слот — для GSM SIM-карты, а другой — для SIM-карты с банковским приложением).

Наиболее серьезные аргументы банковского сообщества в пользу принятия концепции двухслотового «SIM+банковская карта» телефона состоят в том, что банки на сегодняшний день обладают по крайней мере двумя проработанными финансовыми технологиями в области смарт-карт (EMV, CEPS), а также построили мощную распределенную инфраструктуру приема пластиковых карт, обработки платежных транзакций и межбанковских расчетов за транзакции. Очень многое будет зависеть от того, как быстро банки будут внедрять эти приложения на рынке платежных средств (особенно это касается скорости распространения EMV-карт). Наличие на рынке большого количества банковских микропроцессорных карт может заставить телекоммуникационных операторов принять концепцию двухслотовых телефонов.

Дополнительным аргументом в пользу банков является тот факт, что сотовые операторы в основном поддерживают замкнутые системы, в которых пользователь может выполнить транзакцию электронной коммерции, только если и продавец подключен к тому же оператору сотовой связи. В условиях конкуренции между операторами сотовой связи вряд ли стоит надеяться, что в ближайшее время получится построить единую систему мобильной связи на базе нескольких операторов, не говоря уже о платежных системах с глобальным географическим покрытием. Кроме того, операторы сотовой связи понимают, что платежи по картам дадут весьма незначительный в относительном выражении доход как с точки зрения платы за трафик, так и с точки зрения комиссий за обработку транзакций.

Чтобы как можно скорее закрепить свои позиции в области мобильной связи, банки предпринимают попытки сделать обязательным для производителей оборудования для мобильной связи внедрение стандарта

FINREAD, находящегося сегодня в процессе разработки CEN/ISSS (www.cenorm.be/ under ISSS). В разработке проекта принимают участие отдельные заинтересованные банки, а также European Committee for Banking Standards.

Серьезные изменения в области мобильной коммерции могут произойти после появления на рынке смарт-карт, поддерживающих многофункциональные операционные системы. На сегодняшний день существует три основные многофункциональные операционные системы (ОС):

- MULTOS, поддерживается консорциумом MAOSCO, основным участником которого является MasterCard;
- Java Card, поддерживается VISA International и Sun Microsystems;
- Windows for Smart Cards, поддерживается Microsoft.

Из перечисленных операционных систем большой интерес на сегодняшний день представляет ОС MULTOS. Это объясняется следующими причинами:

- MULTOS является наиболее стабильной спецификацией, не подверженной, в отличие от других перечисленных выше ОС, частым изменениям.
- MULTOS обеспечивает высокий уровень безопасности для приложений, функционирующих под ее управлением, что подтверждается сертификацией этой ОС по высшему уровню безопасности ITSEC Еб (примерно соответствует уровню А1 Оранжевой книги США).
- MULTOS действительно ясно специфицирует операции загрузки-удаления приложений в отличие от других ОС, которые только заявляют подобную функциональность, но не определяют ее с необходимой для реализации степенью детальности.

MULTOS является наиболее эффективной ОС с точки зрения своих операционных показателей. Сравнения многофункциональных ОС проводились специалистами компании Consult Hyperion. Методика анализа базировалась на сравнении характеристик выполнения некоторого фиксированного набора приложений, написанных на различных языках высокого уровня (MEL, C, Java). С точки зрения размера кода выяснилось, что лидером является MULTOS. Приложения, написанные на языке MEL под MULTOS, требовали наименьших затрат памяти. Более того, было установлено, что размер кода приложения, написанного на языке С под MULTOS, меньше размера кода того же приложения, написанного на языке Java под Java Card. Что касается такого показателя эффективности ОС, как время исполнения кода приложения,

то исследования показали, что приложение под управлением ОС MULTOS выполняется на 50 % быстрее по сравнению с ОС Java Card.

Как уже отмечалось, ОС MULTOS является высокозащищенным решением. Карты, поддерживающие эту ОС, обязательно содержат сопроцессор RSA. Таким образом, решение задачи динамической аутентификации владельца карты при использовании этой карты является обеспеченным. Это особенно важно для приложений EMV, CEPS, digital ID, Windows 2000 logon, GSM SIM и т. п.

В самом конце 2000 г. компания MasterCard объявила о запуске многофункциональной смарт-карты на базе ОС MULTOS, стоимость которой на больших тиражах составляет $3. При этом карта имеет размер EEPROM, равный 16 K, сопроцессор RSA, реализующий шифрование на ключах длиной 1024 бита. Последняя версия ОС MULTOS для карты разработана австралийской компанией Keycorp Ltd. При этом в ПЗУ карточки прошиты приложения M/Chip Lite (EMV-приложение системы MasterCard) и Public Key Infrastructure.

До конца 2001 г. появятся карточки нескольких производителей на базе MULTOS с EEPROM, равным 32 K. Микропроцессор будет поставляться компаниями Infineon Technologies AG и Philips Semiconductors NV. Ожидается, что стоимость такой карты также не будет превышать $3.

В самом начале апреля 2001 г. компания Keycorp уже объявила о запуске на рынок карточки MULTOS с объемом EEPROM, равным 32 K. Решение Keycorp базируется на применении криптоконтроллера 66Plus (SLE66CX320P) компании Infineon Technologies AG. Микроконтроллер был сертифицирован по наивысшему для микропроцессоров уровню безопасности ITSEC E4. Производительность криптоконтроллера в три раза выше производительности микропроцессоров, имевшихся на рынке до его появления. Карта, наряду с приложениями EMV, может поддерживать такие электронные кошельки, как Mondex, Proton, а также приложение аутентификации клиента.

Необходимо остановиться на очень важном свойстве карты MULTOS — возможности загружать новые приложения в удаленном режиме. Фактически это означает возможность существования нескольких различных центров эмиссии приложений. Например, эмитент приложения GSM SIM — сотовый оператор, эмитент приложений EMV и CEPS — кредитная организация и т. п. В этом случае могут представлять интерес однослотовые модели мобильных телефонов. Возможно, это и является серьезным опасением для телекоммуникационных операторов,

понимающих, что если принять концепцию двухслотового «SIM+ банковская карта» телефона, то наличие банковской многофункциональной карты приведет со временем к тому, что SIM-карта будет заменена банковской, поддерживающей функциональность GSM SIM.

Повторим, что на сегодняшний день существенным ограничением для использования мобильных телефонов в качестве инструмента проведения транзакций ЭК являются два фактора: низкая скорость передачи данных в сетях, основанных на использовании стандарта GSM, и маленький дисплей телефона, ограничивающий возможности отображения на нем информации, необходимой клиенту в процессе совершения электронной покупки.

Проблема повышения скорости передачи данных между мобильным телефоном и сервером решается внедрением стандарта для средств мобильной связи третьего поколения Universal Mobile Telecommunications System (UMTS), предложенного Европейским институтом электросвязи (ETSI). Стандарт UMTS открывает новые возможности для мобильной связи. Ширина полосы частот и скорость передачи данных в нем во много раз выше, чем в стандарте GSM (до 2 Мбит/с вместо 9,6 Кбит/с). Таким образом, мобильный телефон в скором времени превратится в мультимедиа-терминал со встроенным телевизионным экраном. Это позволит передавать и принимать не только обычный разговор, но и видеоизображение (то есть аппарат будет функционировать как видеотелефон), работать с Интернетом и электронной почтой, даст возможность владельцу заниматься телешопингом, а также заказывать и просматривать телепрограммы прямо на мобильном аппарате.

В России планируется развернуть три опытные сети сотовой связи третьего поколения. Разработан план создания опытных зон UMTS в Москве и Санкт-Петербурге. Заявки на их создание уже подали North-West GSM, Delta Telecom (обе компании — из Санкт-Петербурга) и конструкторское бюро «Импульс» от оператора «Вымпелком» (Москва). Заявки на тестирование технологии UMTS поступили также от московских компаний МТС и МСС.

С помощью UMTS можно будет решить проблему телефонизации в РФ, поскольку возможности стационарных аналоговых сетей связи очень ограничены. По оценке аналитиков, к 2005 г. число абонентов сотовой связи в России составит около 10-15 млн человек.

Массовое использование технологии UMTS в мире начнется не раньше 2003 г., а по некоторым прогнозам — в 2009 г. Первая сеть мобильной связи третьего поколения вступила в действие в мае 2001 г. на ост-

рове Мэн. Владельцы 3О-телефонов производства компании NEC получили возможность пользоваться услугами видеотелефонии, играть в масштабе реального времени в компьютерные игры, а также получать информацию обо всех услугах, которые они могут получить в той точке острова Мэн, где они находятся.

Наконец, в заключение необходимо сказать несколько слов о системах GPRS, реализующих переходный этап от технологии GSM к стандарту UMTS. Система GPRS (General Packet Radio Services) представляет собой новый стандарт для пакетного обмена данными в сетях мобильной связи стандарта GSM. На первом этапе обеспечивается пропускная способность 13,4 Кбит/с, в будущем возможно увеличение до 115 Кбит/с. Массовое коммерческое внедрение GPRS во всем мире ожидается через 1-1,5 года, когда в широкой продаже появятся GPRS-совместимые телефоны. На выставке CeBIT 2000 компании Motorola и Sagem демонстрировали образцы GPRS-трубок.

При производстве GPRS-трубок производители столкнулись с серьезными техническими проблемами. Увеличение скорости передачи данных в GPRS происходит за счет одновременного использования нескольких временных слотов в GSM-канале. Это приводит к значительному повышению нагрузки на аккумуляторы и микросхемы телефона. Как результат, первые образцы GPRS-трубок обходились без подзарядки источника питания очень ограниченное время. К тому же существовала проблема с перегревом трубки. Сейчас конструкторы решили отмеченные проблемы, и массовый выпуск надежных трубок ожидается уже в 2001 г.

Все ведущие операторы (назовем хотя бы Vodafone Airtouch, T-Mobile, Sonera, Telnor Mobile) модернизировали свои узлы до поддержки пакетной передачи данных по протоколу GPRS уже к середине лета 2000 г. Основное преимущество GPRS в том, что эта технология обеспечивает пакетную передачу данных: абонент не резервирует за собой канал, а занимает его только при передаче информации. По сути дела, при использовании протокола GPRS абонент может быть все время подключен к Интернету, но при этом его телефонная линия свободна. В этом случае плата берется только за объем переданной информации. По данным сотрудников Nokia, передача 1,8 Мбайт данных аналогична разговору продолжительностью 30 минут, а предложенный компанией Nokia тариф — $1 за передачу мегабайта данных — гораздо дешевле современных тарифов на передачу голоса.

Сегодня стандарт GPRS поддерживается и крупнейшими российскими операторами сотовой связи — МТС и «Би Лайн».

Интерактивное телевидение

Интерактивное телевидение, как и мобильная телефония, приобретает все большее распространение. В мире насчитывается 1,5 млрд телевизионных приемников, что значительно превышает количество телефонных абонентов, равное примерно 1 млрд.

Наиболее распространенными услугами, получаемыми клиентом с использованием STB-устройств, являются:

- программирование широковещательных телевизионных передач под конкретных пользователей;
- получение информационных сервисов: прогноз погоды, новости, биржевая информация и т. п.;
- покупка товаров и услуг;
- заказ и оплата индивидуальных телевизионных программ (Video-on-Demand, Pay-Per-View);
- доступ в Интернет;
- игры и т. п.

Организация платежей через интерактивное телевидение (сегодня для обозначения этого вида ЭК часто используется термин t-commerce) требуется для оплаты:

- покупок товаров и услуг;
- избирательно для оплаты услуг Video-on-Demand и Pay-Per-View («плати и смотри»);
- игр;
- доступа к информационным услугам.

Наиболее оптимистичные прогнозы утверждают, что уже к 2003 г. через интерактивное телевидение будет производиться около 30 % всех удаленных платежей.

Рассматриваются две модели ввода платежных данных при применении интерактивного телевидения:

- ввод данных с помощью микропроцессорной карты через картридер, подключенный к отдельному второму слоту STB-устройства;
- ввод данных из программы электронного бумажника (electronic wallet), хранящейся в устройстве управления телевизора.

Сегодня мало примеров использования TV для проведения транзакций ЭК. Предоставляемый каналом Sky Digital интерактивный телевизионный сервис Open позволяет потребителям совершать покупки,

не выходя из дома, пользоваться электронной почтой и играть в некоторые несложные игры.

Похожие услуги (включая ЭК) начала оказывать российская компания Телеком Рикор.

Известен также пример сотрудничества компаний Future TV и Mondex International в области использования электронных кошельков Mondex. По технологии Future TV зрители могут теперь выбирать, какие программы им смотреть и когда. Оплата услуг производится с помощью карт Mondex. В результате телевизор пользователя со временем узнает о предпочтениях своего хозяина и сам предлагает ему программы, которые он может захотеть увидеть.

Существующая ситуация, видимо, связана с тем, что некоторые телевизионщики считают новые информационные технологии опасными для себя. До последнего времени основу могущества телевизионных магнатов составляло владение содержанием передаваемой информации и контроль над ним, а также «право собственности» на аудиторию. Появление технологий, осуществляющих «распаковывание» содержания передач (каждый зритель выбирает передачу, а не канал), а также поддерживающих принцип «плати и смотри», угрожают привычной власти телемагнатов и устоявшейся схеме получения доходов.

Тем не менее, переход к «распаковыванию» и «плате за просмотр» неизбежен, поскольку оба эти принципа чрезвычайно привлекательны для потребителя. Недавние исследования показали, что 57 % потребителей предпочли бы оплачивать телевидение по принципу «плати и смотри».

Как уже отмечалось, ЭК с помощью TV должна стать наиболее распространенным способом проведения заочной торговли. По данным опроса, проведенного Gallup по заказу Pace Micro Technology (Pace Micro Technology является крупнейшим в Европе производителем телевизионных цифровых декодеров и устройств Set-top-Box; компания выпустила 2 500 000 приставок digital set-top box), 42 % респондентов ответили, что предпочитают использовать телевизионные приемники для проведения операций ЭК. При этом примерно 25 % респондентов ответили, что не будут использовать технологию ЭК ни при каких обстоятельствах. Среди тех опрошенных, кто собирается когда-нибудь использовать ЭК, 59 % склоняются в пользу интерактивного телевидения, а 37 % — в пользу персональных компьютеров. При этом, как это ни покажется странным, среди компьютерного поколения (молодые люди от 16 до 24 лет) доля людей, предпочитающих интерактивное телевидение персональным компьютерам в качестве средства проведения ЭК, составляет 65 %.

Краткое описание состояния рынка электронной коммерции

Состояние рынка в мире

Объемы операций через Интернет постоянно растут. В 1995 г. оборот продаж/покупок по Интернету составлял около $300 млн (Coopers&Lybrand). По данным компании ActiveMedia общий объем сделок в рамках систем электронной коммерции в мире в 1996 г. составил $2,7 млрд, а в 1998 г. достиг $73,8 млрд. По данным отчета исследовательской компании eMarketer, в 2000 г. мировые обороты по электронной коммерции составили $185 млрд, в 2001 г. они увеличатся до $336,2 млрд, в 2002 г. — составят $684,3 млрд, а в 2003 г. достигнут $1,26 трлн.

Похожая оценка для 2003 г. дается компанией IDC. По прогнозам IDC к 2003 г. объем операций ЭК достигнет уровня $1,3 трлн. Ожидается, что к 2005 г. более 10 % всех торговых операций в мире будет производиться с использованием средств электронной коммерции.

Аналитики eMarketer утверждают, что в общих доходах электронной коммерции в 2000 г. доля B2B составляла 79,2 %. В дальнейшем эта доля будет только увеличиваться: в 2001 г. она составит 82,5 %, а к 2003 г. достигнет 87 %.

По оценкам компании Forrester Research в 2004 г. обороты электронной коммерции в корпоративном секторе составят $2,7 трлн. По мнению аналитиков рост объемов будет происходить в основном за счет рынков Европы и Азиатско-Тихоокеанского региона. Более половины транзакций ЭК (около 51 %) будет осуществляться в Северной Америке. Объем второго по величине, Азиатско-Тихоокеанского рынка, составит 23 % от всего объема ЭК. Лидером в этом регионе останется Япония. Объем европейского рынка оценивается в 22 % от всего объема ЭК.

По прогнозам исследовательского центра IDC, доходы европейских B2B-компаний, составившие в 2000 г. 61 млрд евро ($57,3 млрд), к 2005 г. взлетят до 1,5 трлн евро. Самым динамично развивающимся направлением европейского B2B-бизнеса в следующие четыре года будут торговые площадки в Интернете (emarketplaces). В течение периода до 2005 г. эти площадки будут приносить наиболее высокий доход, который будет складываться преимущественно из поступлений от электронных сделок, заключения партнерств и дополнительных услуг, таких как, например, электронный консалтинг.

Лидером рынка B2B-коммерции в ближайшие годы останутся США — в 2003 г. их доля на этом рынке составит 59 % ($ 747 млрд). По прогнозам eMarketer, до 2003 г. будет наблюдаться рост популярности онлайновых торговых площадок и бирж. Будут усложняться и совершенствоваться предлагаемые ими услуги. Причем основными игроками на этом рынке станут небольшие компании. Сейчас в онлайновой торговле принимают участие только 8 % малых компаний, но к 2003 г. их доля возрастет до 72 % и их доходы от этой деятельности достигнут $230 млрд.

По данным компании Boston Consulting Group (BCG) в 1999 г. скорость роста годового объема операций, выполненных через системы электронной коммерции (ЭК), составила около 200 % для Европы и 145 % для США.

В четвертом квартале 2000 г. американцы потратили $ 8,562 млрд в секторе B2C и впервые в истории перешагнули рубеж в 1 % от общего объема розничных продаж в США.

В отчете Департамента Коммерции США говорится, что за период с октября по декабрь 2000 г. американцы купили на 35,9 % больше товаров, чем за предыдущий квартал, что свидетельствует о неослабевающем интересе к покупкам через Интернет в Америке, даже несмотря на общее замедление развития экономики. Лидерство в Европе по числу любителей делать покупки через Интернет принадлежит Швеции, где таким способом покупают товары 2,5 % населения страны. Как показало исследование компании Jupiter Media Metrix, число интернет-пользователей в Швеции достигло рекордного уровня. Согласно этому исследованию, в феврале 2001 г. 4,23 млн шведов выходили в Интернет. В общей сложности Интернет использует 59 % всего населения страны в возрасте от 12 до 79 лет, что составляет максимальный показатель среди европейских стран. 65 % мужчин и 54 % женщин хотя бы один раз в месяц выходят в Интернет.

«Несмотря на более низкую степень развития электронной коммерции, Германия и Великобритания являются наиболее важными рынками благодаря размерам их экономики. Вместе они составляют 60 % европейского рынка и отвечают за большую часть роста в абсолютном значении (в том числе трехкратного роста в течение одного года)», — говорится в отчете Boston Consulting Group.

Небольшая доля продаж через Интернет во Франции объясняется национальной спецификой. Уже 20 лет во Франции распространены дешевые устройства Minitel, позволяющие входить в некий национальный аналог Интернета и делать там покупки. Оборот в этой сети превы-

шает оборот Интернет-торговли в любой другой европейской стране — $1,32 млрд.

Значительно отличаются методы платежей. В Германии и скандинавских странах менее 20 % покупок через Интернет оплачивается кредитными картами, а в Британии, Франции и Италии кредитки используются очень широко. Более 90 % онлайновых платежей Великобритании оплачивается карточками.

К 2003 г. по прогнозу Jupiter Communications покупки через Интернет в Европе будут совершать 40,2 млн человек.

Структура электронных покупок в 1998 г. имела следующий вид:

- компьютеры и комплектующие к ним — 44 %;
- продажа авиабилетов — 23 %;
- книги - 14 %;
- музыкальные записи — 5 %;
- программы — 5 %;
- прочее-9%.

Ожидается, что доля продаж авиабилетов в ближайшие годы увеличится до 35 %, в то время как доля продаж компьютеров, наоборот, уменьшится до 16%.

Согласно отчету, проведенному компанией Census Bureau, пользователи Интернета в 2000 г. потратили на покупки $28 млрд, что превысило аналогичные показатели за 1999 ($17,3 млрд) и 1998 годы ($7,7 млрд). Пользователи потратили больше всего денег на покупку авиабилетов — $7,8 млрд (27,9 %). На покупку ПК в Интернете было потрачено $5,1 млрд (18,2 %), а на бронирование номеров в отелях $2,1 млрд (7,5 %). При этом через Интернет производилось 24 % всех продаж компьютерного оборудования. На покупку программного обеспечения пользователи потратили $1,3 млрд (4,6 %), что составило 21 % от всего объема данного рынка. По прогнозам этой же компании объем продаж в секторе B2C в 2001 г. составит $ 65 млрд. Таким образом, рост этого сектора электронной коммерции составляет 46 % в год.

Согласно последнему отчету компании Boston Consulting Group объем продаж в секторе B2C в 2000 г. равнялся $44,5 млрд, что составило 1,7 % от всего объема в розничном секторе.

Набирают обороты и новые виды электронных покупок. Все более популярной становится торговля через Интернет ценными бумагами. Так, по итогам первого квартала 2000 г. объем торгов ценными бумагами

вырос на 69 %, а размер активов счетов пользователей впервые перевалил за $1 трлн. Лидером рынка является онлайновый брокер Charles Schwab. На втором месте E-Trade.

Интернет меняет и формы торговли. Большой популярностью пользуются электронные аукционы, превращающиеся из увлекательной экзотики в основной способ торговли в виртуальной экономике. По мнению экспертов, объем продаж через потребительские аукционы будет стремительно расти от $1,4 млрд в 1998 г. до $19 млрд в 2003 г. Интересно, что в 1998 г. 75 % всего объема продаж на аукционах составляли компьютеры и все, что с ними связано. К 2003 г. эта цифра упадет до 27 %. Наиболее крупные известные компьютерные аукционы: OnSale, uBid и Cyberian Outpost.

Среди аукционов для потребителей можно выделить две крупные категории — продажа остатков и торговля коллекционными предметами. OnSale, Cybershop, Sharper Image и Cyberian Outpost продают остатки, а недавно запущенный компанией Amazon аукцион Auctions, с которым подписали договор о сотрудничестве уже около 170 торговцев, ориентированы на коллекционеров антиквариата, марок, монет, комиксов и старых пластинок.

Аукционы распространяют свое влияние на самые разные области торговли. Эксперты компании Forrester предсказывают, что очень скоро все — от маек до автомобилей — будет продаваться через Интернет по договорным ценам. Меняться будет и структура аукционов. В 1998 г. 70 % всех аукционных продаж составили продажи «от одного человека другому», а остальные 30 % были продажи в секторе B2C. В 2003 г. доля последних возрастет до 66 %.

В заключение, говоря об аукционах, нельзя не упомянуть крупнейший аукцион eBay. На начало 2000 г. рыночная стоимость акций этого аукциона составляла $18 млрд. На аукционе eBay зарегистрировано 4 млн клиентов. Аукцион поддерживает около 90 тематических групп, что привлекает к нему продавцов — продавца интересует не общее число клиентов какого-либо аукциона, а число клиентов, интересующихся его товаром (находящихся в его тематической группе).

Рассказывая об электронных аукционах и биржах, нельзя не упомянуть и таких монстров, как MetalSite (торговля металлом), World Chemical Exchange (работает с 4000 химических компаний, продающих и покупающих на ее Web-узле излишки продукции), Ariba и Commerce One.

Состояние российского рынка

В настоящее время в России существует рынок товаров и услуг, для оплаты которых средства электронной коммерции являются удобным платежным инструментом. К числу таких товаров и услуг относятся:

- бронирование и продажа билетов (авиабилетов, билетов на другие виды транспорта, билеты в театры, кино и т. п.);
- продажа компьютеров, ноутбуков, принтеров, мониторов, сканеров, программного обеспечения, сетевого оборудования, комплектующих и т. д.;
- продажа книг и изданий, компакт-дисков, аудио- и видеоаппаратуры;
- резервирование и оплата проживания в гостиницах;
- оплата пользователями Интернета услуг своих операторов доступа к Интернет-провайдеру (Internet Service Provider, ISP); сегодня в России насчитывается около 150 активных ISP;
- оплата пользователями услуг коммуникационных систем общего пользования (сотовых сетей, пейджинговых систем и других);
- продажа туристических путевок;
- подписка на различные услуги (например, газеты и журналы);
- продажа продуктов питания;
- продажа медикаментов;
- оплата коммунальных услуг;
- продажа программного обеспечения.

По самым грубым оценкам в 1999 г. годовой объем операций по электронной коммерции в России составлял $1 млн (на фоне примерно $ 130 млрд в мире). По данным компании eTopS, объем рынка ЭК в 1999 г. составлял примерно $1,5 млн. В соответствии с различными оценками в 2000 г. обороты ЭК составляли $10—45 млн. В частности, по данным инвестиционной компании RuNet Holding совокупный объем ЭК составлял в 2000 г. $12 млн. По данным A. T. Kearney, суммарный оборот российского рынка электронной торговли в 2000 г. равнялся $40 млн.

В России доля операций ЭК от общего товарооборота находится на уровне сотых долей процента. Представители российского офиса Boston Consulting Group прогнозируют рост объема электронной коммерции в России в 2003 г. до $400-600 млн. При этом соотношение электронной коммерции к общему товарообороту должно достигнуть 0,25 %, что будет соответствовать уровню США в 1998 г. Таким обра-

зом, по этому критерию отставание России от Северной Америки в области ЭК составляет примерно пять лет.

Boston Consulting Group прогнозирует в 2003 г. средний оборот российской онлайновой торговли в $50—60 в год на каждого пользователя Интернета, что составит около 1 % от его дохода. Доход этот, заметим, будет вдвое выше, чем у среднего гражданина России. Сейчас же доходы пользователей, имеющих доступ из дома (25 % от общего числа), в 5—6 раз выше средних доходов по стране. К 2003 г. количество пользователей Интернета с низкой платежеспособностью, входящих в Интернет через образовательные и научные учреждения, сократится с нынешних 25 % до 10 %, а количество домашних пользователей возрастет до 40 %.

Тем не менее, аналитики Boston Consulting Group не предрекают до 2003 г. массового проникновения на российский рынок американских онлайновых продавцов. В отличие от европейского рынка в России не развита необходимая для этого инфраструктура. Скорее ожидается появление Интернет-компаний 2-3-го уровня, например скандинавов и турок. Наглядным примером служит их экспансия на традиционном рынке — достаточно взглянуть на магазины IKEA и «Рамстор».

В отношении прогнозов развития в России рынка B2B интерес представляют выводы аналитиков рейтингового агентства «Эксперт РА», сделанные в завершенном в начале 2001 г. отчете-исследовании «Перспективы развития межкорпоративного электронного бизнеса в промышленности России». В соответствии с этим отчетом к 2005 г. общий объем операций между российскими предприятиями через Интернет может составить $2,8 млрд. Данный показатель рассчитан при условии сохранения тех позитивных тенденций, которые наблюдаются в российской промышленности в последнее время. По прогнозам аналитиков рейтингового агентства «Эксперт РА» через три-четыре года российские компании могут вступить в фазу активного освоения межкорпоративного электронного бизнеса и взаимоотношения между участниками рынка примут более цивилизованный характер. Тем не менее, по оценкам авторов отчета, в ближайшем будущем лавинообразный рост продаж промышленной продукции в России через Интернет маловероятен. Скорее всего, до 2003 г. российский B2B-рынок будет проходить этап структурной организации, при котором стоимостные показатели объема рынка будут невелики.

Аналитический доклад «Перспективы развития межкорпоративного электронного бизнеса в промышленности России» составлен на основе базы данных рейтингового агентства «Эксперт РА», материалов официальных статистических органов (Госкомстата РФ, ГТК РФ) и сведе-

ний ведомственной отчетности. Также для получения дополнительной информации было проведено анкетирование 200 ведущих компаний России и серия интервью с топ-менеджерами крупнейших отечественных корпораций. Консультантом исследования была компания PricewaterhouseCoopers.

В России сегодня насчитывается полтора десятка систем ЭК и около 600 виртуальных магазинов. В области розничной торговли только половина Интернет-магазинов реально ведет бизнес, а ощутимый ежемесячный доход (более $5 тысяч) имеют два-три десятка. Среди них известна торговая система eMatrix (www.ematrix.ru), принадлежащая холдингу eHouse. В систему входят такие известные магазины, как Dostavka.ru, Megashop.ru, Wsore.ru, Aromat.ru, Kenga.ru. Суммарный оборот этих магазинов за первую половину 2000 г. составил $5,7 млн, а в сентябре того же года — $1,79 млн.

Российским пионером в области продаж через Интернет явился Мост-банк. В 1997 г. Мост-банк совместно с фирмой «Формоза Софт» и процессинговой компанией «Мультикарта» реализовал технологию электронных платежей с использованием карточек Мост-Банка EC/MC, VISA, MostCard. Подключившись через Интернет к Web-сайту компании «Формоза», можно было совершить покупку компьютеров, ноутбуков, принтеров, мониторов, сканеров, программного обеспечения, сетевого оборудования, комплектующих и т. д. (всего более 1000 видов техники). Интернет-магазин позволял в режиме реального времени получить доступ к информации о наличии товаров, ценах, предоставляемых скидках и льготах. Кроме того, для каждого товара имелось его изображение и краткое описание основных характеристик.

Процесс оплаты покупки в Интернет-магазине Мост-банка с использованием пластиковых карточек происходил следующим образом. Для авторизации операции покупки Интернет-магазин автоматически связывается с процессинговой компанией. После успешной авторизации сумма покупки холдировалась (замораживалась, но не списывалась) на счете клиента. Завершалась операция покупки передачей заказа и оформлением в момент доставки товаров слипа (специального банковского документа, оформляемого торговым предприятием и подтверждающего обслуживающему банку факт совершения покупки в торговой точке), на котором производился оттиск карточки и проставлялась подпись клиента. Только после этого банк списывал заблокированную ранее сумму.

Вслед за Мост-банком на рынке появились другие игроки. Сегодня в России продажами через Интернет активнее других занимаются такие банки, как Альфа-банк, Росбанк (через компанию UCS), «Первое

общество взаимного кредита» (через процессинговую компанию STB CARD), «Менатеп (С.-Петербург)», «Петровский», «Платина».

Для захвата транзакции от Интернет-магазина и ее доставки в платежную систему банки чаще всего используют технологию виртуального POS-сервера. Основная функция такого сервера состоит в подключении ТП к платежной системе на основе нескольких заранее оговоренных интерфейсов, а также в получении данных от владельца карты. Таким образом, для ТП облегчается задача начала безналичных расчетов по пластиковой карте. Кроме того, реквизиты карты не известны ТП, что является важным фактором при обеспечении безопасности в Интернет-торговле.

Сервер Assist (разработка и собственность петербургской компании «Рексофт») является на сегодняшний день самым известным виртуальным POS-сервером в России. Сервер начал свою работу в марте 1999 г. и сегодня через него работают несколько десятков ТП. Схема расчетов с помощью пластиковых карт в системе Assist показана на рис. 1.2.

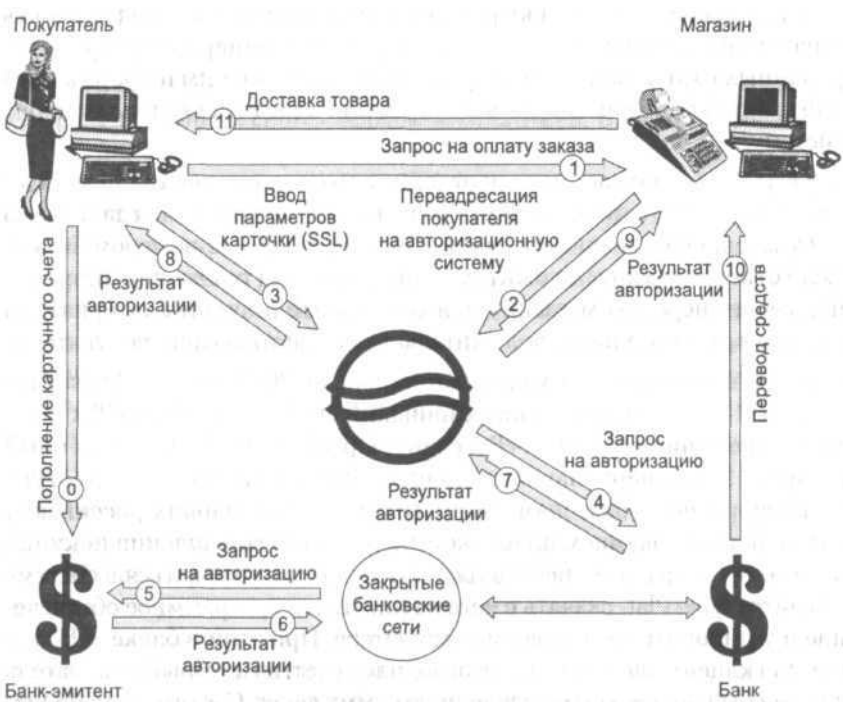

Рис. 1.2. Схема расчетов в системе Assist

Покупатель через Интернет подключается к Web-серверу ТП, формирует корзину товаров и выбирает в качестве способа оплаты пластиковую карту.

ТП формирует заказ и переадресует покупателя на сервер Assist. Одновременно ТП передает на сервер Assist идентификатор ТП, номер заказа и его сумму.

Сервер Assist устанавливает с покупателем защищенное SSL-соединение (подробнее см. далее) и принимает от покупателя параметры его кредитной карты (номер карты, время окончания ее действия, имя держателя карточки, CVV2/CVC2 и, возможно, некоторую другую информацию). К оплате принимаются карты всех известных международных и отечественных платежных систем, включая VISA, Europay/MasterCard, American Express, Diners Club, JCB и STB CARD. Таким образом, конфиденциальная информация о реквизитах карты не предоставляется торговому предприятию.

Сервер Assist производит обработку полученной информации (в частности, совершает проверку реквизитов карты на их принадлежность к различным Negative-файлам, содержащим номера скомпрометированных карт, а также некоторую относящуюся к ним информацию) и формирует авторизационный запрос для передачи его в платежную систему.

Сервер Assist получает из сети ответ на авторизационный запрос. Если ответ содержит отрицательный код ответа, то сервер передает отказ покупателю с описанием причины отказа, а ТП — с номером заказа. Если ответ содержит положительный код ответа (транзакция разрешена), сервер передает магазину положительный результат авторизации с номером заказа, а также положительный код авторизации покупателю.

Первым пользователем услуг виртуального POS-сервера Assist был банк «Платина», фактически ожививший свой проект CyberPlat с помощью решения компании «Рексофт». Проект CyberPlat, запущенный в марте 1998 г., первоначально предоставлял услугу оплаты доступа в Интернет пользователям Демос (один из крупнейших российских ISP) с использованием пластиковых карт. Для совершения покупки в системе CyberPlat клиент должен был зарегистрироваться в системе на сайте CyberPlat, скачать с него специальное программное обеспечение и установить его на своем компьютере. При этом в банке «Платина» для клиента автоматически заводился счет, на который покупатель должен был положить определенную сумму денег. С этого счета производились расчеты за электронные покупки клиента.

Очевидно, что схема CyberPlat была замкнутой, монобанковской и могла рассчитывать на успех в весьма ограниченном секторе бизнеса (например, при оплате услуг внутри замкнутого сообщества покупателей и продавцов).

С 2000 г. услугами Assist стали пользоваться платежная система STB CARD и Альфа-банк. В результате сотрудничества с STB CARD на сервере появились дополнительные возможности, включая «захват» дополнительных данных по карте (CVV2/CVC2, динамическая аутентификация владельцев карточки STB Card).

Банк «Платина» сегодня перестал пользоваться услугами сервера Assist, создав его аналог — сервер CyberPOS. Оператором системы CyberPlat является компания Cyberplat.com, выделившаяся из банка «Платина».

Идея создания виртуального POS-сервера оказалась весьма плодотворной и сегодня взята на вооружение всеми банками, занимающимися ЭК. Кроме того что виртуальный POS-сервер позволяет ТП с минимальными затратами внедрить оплату по пластиковым картам, эффективность решений на основе единого сервера с точки зрения безопасности оказывается более высокой.

Поясним сказанное. Рассмотрим упрощенные модели распределенной и централизованной систем обработки платежей. В централизованной системе платежи осуществляются с помощью единого для всех ТП сервера, а в распределенной — каждым ТП самостоятельно. Пусть в системе имеется m одинаковых торговых предприятий, через каждое из которых обрабатываются n карточек. Предположим, что система подвергается атаке хакеров, целью которой является получение информации о реквизитах карт, хранящихся в системе. В случае централизованной системы вся информация о nm карточках хранится на одном сервере, а в случае распределенной — на сервере каждого ТП хранится информация только об n картах. Будем считать, что вскрытие сервера означает получение хакерами информации о всех картах, хранящихся на сервере.

Обозначим через P_c и P_d — вероятности того, что атака хакеров соответственно на единый сервер централизованной системы и сервер одного ТП в распределенной системе завершится неудачно. Пусть c — средние потери от попадания информации о реквизитах одной карты в руки мошенника (сюда входят потенциальные потери от использования карты, стоимость блокировки карты и т. п.). Обозначим также через F(p) затраты, которые необходимо сделать для того, чтобы обеспечить такой уровень защиты сервера (ТП или центрального сервера),

при котором вероятность того, что атака мошенников на сервер закончится провалом, равна p. Из общих соображений очевидно, что F(p) — монотонно возрастающая функция, определенная на интервале [0,1), и lim F(p)= °°, когда p—>1. Пусть F_o — ограничение сверху на расходы, связанные с повышением безопасности системы.

Легко показать, что средние потери от атаки мошенников равны $C_c=cmn(1-P_c)$ и $C_d=cmn(1-P_d)$ для централизованной и распределенной систем соответственно, где P_c и P_d являются решениями уравнений:

$F(P_c)=F_o$;

$mF(P_d)=F_o$.

В силу монотонности возрастания функции F(p) очевидно, что выполняется неравенство $P_c>P_d$ и, следовательно, $C_c<C_d$.

Таким образом, при ограниченных затратах на создание системы эффективнее вкладывать средства в повышение безопасности центрального сервера, чем сервера каждого ТП по отдельности. При этом эффект тем более явный, чем больше ТП работает в системе.

В модели предполагалось, что множества карт, работающих в каждом ТП, не пересекаются. На практике одни и те же карты обслуживаются в разных ТП. Поэтому при взломе одного ТП становятся известны реквизиты карт, хранящиеся в базах данных других ТП. Это еще больше усиливает эффект от создания единого защищенного сервера ЭК.

Помимо систем Assist и CyberPlat известны системы Элит+ (разработка компании АйТи, используемая Автобанком), Cashew (разработка компании DataX Florin, используемая банком Менатеп С.-Петербург), ЦЭП (разработка компании Web Plus, используемая банком ПСБ С.-Петербург).

Представляет интерес проект PayCash (совместная разработка банка «Таврический» (С.-Петербург) и группы компаний «Алкор-Холдинг»). Система PayCash реализует цифровой эквивалент чека. В проекте принимают участие несколько банков, каждый из которых имеет возможность выпустить собственные электронные деньги.

Комиссионные платежной системы PayCash за процессинг транзакции составляет 1-2 % от ее размера. На январь 2001 г. в системе были зарегистрированы 30 магазинов и 11 тысяч пользователей. Ежедневно к системе подключалось около 60 пользователей.

Другим примером системы электронной наличности является система WebMoney Transfer. Система предоставляет возможность пользователю

Интернета осуществлять безналичные расчеты в масштабе реального времени с использованием электронной наличности WEBMONEY (WM).

Подробнее о принципах функционирования систем PayCash и WebMoney Transfer читатель может узнать в главе «Системы электронной наличности».

В мае 2000 г. была запущена в эксплуатацию Система Интернет-платежей (СИП) Сбербанка РФ. Система была разработана компанией «СмартКард-Сервис». Она позволяет производить оплату товаров и услуг в Интернет-магазинах с помощью микропроцессорных карт системы СБЕРКАРТ Сбербанка.

Наконец, следует отметить совместный проект банка «Олимпийский» с компанией Europay по реализации проекта ЭК на базе протокола SET (о протоколе SET — Secure Electronic Transaction — подробно рассказано далее). Проект начат в ноябре 1998 г. Сведения о проекте очень скупы. Известно только, что в нем участвуют несколько сотен карт и один Интернет-магазин.

Известно, что проект ЭК на базе протокола SET и решения IBM Payment Suite был запущен российской компанией Транскредиткарт. Проект реализуется для предприятий МПС (автоматизируются безналичные расчеты за перевозку, топливо и т. п.).

В данном обзоре необходимо также упомянуть наиболее известные сегодня российские электронные магазины. По данным magazin.ru, Интернет-магазины по типу продаваемой ими продукции распределены так, как это показано на рис. 1.3.

Рис. 1.3. Виды продукции, продаваемые в российских Интернет-магазинах

Наиболее известным российским магазином электронной коммерции является магазин Ozon (www.ozon.ru). Магазин начал свою работу

в апреле 1998 г. Сегодня он предлагает покупателям несколько тысяч наименований книжных изданий, компакт-диски и DVD, периодику и видеокассеты. К концу 1999 г. Ozon вышел на самоокупаемость, а в начале 2000 г. 51 % акций магазина были проданы инвесторам за $1,8 млн.

Магазин Bolero (www.bolero.ru) возник летом 1999 г. Сегодня на сайт магазина ежедневно заходят несколько тысяч человек. Магазин торгует книгами (более 24 тыс. наименований), музыкальными записями (более 25 тыс.), DVD и Video CD (около 800), играми (более 440), видеокассетами (около 4650 наименований), товарами для детей, журналами и газетами (более 550 наименований). Ежедневно в магазине совершается свыше 100 покупок. Если заказ сделан утром и доставка производится в пределах Москвы, то он исполняется в течение суток.

Компьютерный электронный магазин Dostavka.ru (www.Dostavka.ru) начал работать в декабре 1998 г. Цены в Dostavka.ru находятся в промежутке между ценами компьютерных рынков (типа московской «Горбушки») и салонов — ближе все-таки к рынку. Однако если есть спрос на определенный товар, то цена повышается. Ассортимент магазина насчитывает несколько сотен позиций. Доставка товаров производится только в Москве.

Магазин Ramis (www.ramis.ru) представляет собой электронный магазин по продаже расходных материалов для офисной техники.

На Web-узле www.gost.ru находится электронный магазин по покупке необходимых покупателю стандартов ГОСТ.

В конце 2000 г. в Рунете открылась система бронирования и продажи билетов на все зрелищные мероприятия в режиме реального времени (www.parter.ru). Сейчас через эту систему можно заказать билеты на различные концерты, спортивные мероприятия, а также на спектакли лучших театров страны.

В середине декабря 1999 г. усилиями компании KompTek International и инвестиционного фонда net-Bridge в Рунете был открыт аукцион «Молоток.Ру». Схема функционирования аукциона строится следующим образом: продавец регистрируется, ставит в базу данных свой товар и назначает за него минимальную цену. Для регистрации продавца достаточно указать адрес электронной почты. Затем начинаются торги, продолжающиеся 3, 7, 15 или 30 дней. После завершения сделки продавцу и покупателю (который также регистрируется по адресу в электронной почте) высылается контактная информация, и они свя-

зываются друг с другом самостоятельно. Количество успешно завершаемых сделок составляет около 35 % от всего количества продаж через аукцион. По данным на середину 2000 г. в аукционе «Молоток.Ру» участвовало около 10 тыс. человек, выставлялось 5 тыс. лотов на сумму более $14 млн.

Большую популярность в России приобретает интернет-страхование. Крупнейшим страховым Интернет-представительством в Рунете является сайт Ингосстраха (www.ingos.ru). Функции Интернет-представительства Ингосстраха не ограничиваются только ролью виртуальной витрины, дающей посетителю информацию о предоставляемых компанией услугах. Основным отличием www.ingos.ru от большинства официальных сайтов других страховых компаний является хорошо отлаженный механизм обратной связи, осуществляемый как через почту, размещенную на сервере Ингосстраха, так и через анкеты, заполняемые потенциальными клиентами. В последних посетители сайта могут поместить подробную информацию о конкретном предмете, который они хотели бы застраховать, сумме и сроках страховки. Подробный ответ с указанием реальных страховых продуктов, более всего отвечающих запросам клиента, возвращается клиенту в течение одного дня с момента обращения.

Кроме этого, на сайте имеется специальный калькулятор, позволяющий клиенту, сидя за домашним компьютером и варьируя параметры страхования (страховые суммы, лимит ответственности и т. п.), самостоятельно оптимизировать свою страховую защиту.

Заключительный этап продажи услуги клиенту Ингосстраха не является электронным. Для заключения реальной сделки требуется присутствие клиента в офисе компании. Однако значительная часть сделки (подготовка документов) производится в Интернет-представительстве, и клиенту требуется совсем немного времени для того, чтобы подписать в офисе компании уже подготовленные договоры, предварительно лолучив разъяснения по любому интересующему вопросу.

Виртуальный офис компании «Группа ренессанс страхование» находится по адресу www.renins.com. Компания предлагает продукты, охватывающие основные направления страхования: квартиры, дачи, несчастные случаи, автогражданская ответственность и страхование выезжающих за рубеж.

Главным разделом сайта www.renins.com, бесспорно, является Интернет-магазин, в котором осуществляется продажа страховых полисов с использованием пластиковых карт. В настоящее время продается семь страховых продуктов, не требующих андеррайтинга — предваритель-

ного осмотра клиента. К таким продуктам относятся страхование от несчастных случаев, выезжающих за рубеж, страхование гражданской ответственности и т. п.

Компания РОСНО уже долгие годы является одним из лидеров в сфере социальных страховых продуктов. Для удобства посетителей представленные на сайте www.rosno.ru продукты разбиты на семь основных категорий, в числе которых медицинское страхование, страхование жизни, жилища, автомобиля, гражданской ответственности и т. д.

Основным разделом Web-сайта www.rosno.ru является «Центр Интернет-Продаж». Здесь клиент имеет возможность ознакомиться со страховыми продуктами компании, которые можно приобрести в онлайновом режиме. Для удобства все страховые программы поделены на четыре основные категории: автомобили, имущество, жизнь и здоровье, путешествия. Выбрав интересующий его продукт, клиент может ознакомиться с его описанием, рассчитать цену на предложенном здесь же калькуляторе. Если цена полиса устраивает клиента, то ему предлагается прочитать правила страхования и приступать к заполнению анкеты, которая фактически является заявлением на страхование. Расплатиться за страховку можно с помощью кредитной карточки.

В Рунете представлены также виртуальные офисы Промышленно-страховой компании (ПСК) (www.iic.ru), компании «Ресо-Гарантия» (www.reso.ru), Закрытого акционерного общества авиационного и космического страхования «АВИКОС» (www.avicos.ru), компании «Центр Брокер» (www.insurance2000.ru).

Опрос регулярной аудитории Рунета, проведенный агентством monitoring.ru, показал, что доля имеющих опыт приобретения товаров и услуг через Интернет составляет минимум 12 %. В Москве и Санкт-Петербурге эта доля составляет минимум 21 %. В остальной части европейской территории России рассматриваемый показатель вчетверо меньше (5 %). На Урале и в Западной Сибири доля имеющих опыт совершения электронных покупок составляет 8 %, в Восточной Сибири и на Дальнем Востоке — 16 %. При этом 66 % тех, кто имеет опыт приобретения товаров и услуг через Интернет, проживают в Европейской части России. Только на Москву и Санкт-Петербург приходится 47 % всех имеющих опыт приобретения товаров и услуг через Сеть. Активная аудитория Интернета предпочитает следующие темы: новости (64 %); развлечения, анекдоты, игры (59 %); общение, чаты (47 %); информация о товарах и услугах (40 %); бизнес, финансы (37 %). Максимальная аудитория предпочитает следующие темы: развлечения, анекдоты, игры

(35 %); общение, чаты (32 %); новости (31 %); наука, образование (21 %). Средний возраст всей активной аудитории составляет 30 лет. Самые молодые люди в этой аудитории Рунета объединены интересом к музыке, литературе, кино (средний возраст 24 года). Затем следует группа со средним возрастом 26 лет, объединенная интересом к общению, чатам.

Среди посетителей российских Интернет-магазинов значительно больше россиян, чем в аудитории Рунета в целом. Если в целом на русскоязычных ресурсах 2/3 их посещений приходится на российских пользователей, то на сайтах Интернет-магазинов по данным отчета, составленного компанией SpyLog, российская аудитория дает более 3/4 трафика.

Преобладание российских пользователей неудивительно, если принять во внимание, что в выборку были включены магазины, ориентированные в первую очередь на российский рынок. Данное ограничение особенно заметно сказалось на доле аудитории из стран СНГ и Прибалтики — в секторе онлайновой торговли доля ближнего зарубежья не превышает 6 % против 14 % в целом по Рунету (данные по хитам). Русскоязычную аудиторию из бывших республик СССР отличает и крайне низкая активность на сайтах Интернет-магазинов — в среднем задень на каждого посетителя из Украины или Прибалтики приходится около 3 посещений против 4,5 посещений для российских посетителей и 5-6 посещений для посетителей из стран дальнего зарубежья. Это позволяет говорить о том, что среди посетителей из ближнего зарубежья (несмотря на немногочисленность данной категории) преобладают случайные посетители.

Помимо России, только у одной страны — Израиля — доля в аудитории Интернет-магазинов (2,1 % по посещениям) выше, чем в целом по Рунету (1,8 %). Очевидно, что подобный результат достигается за счет интереса русской диаспоры (а ее доля в населении максимальна именно в Израиле) к книгам, музыке и видео из России, которые можно заказать через Интернет. В аудитории соответствующих магазинов доля «стран диаспоры» составляет 18 %. В том числе США — 11,6 %, Израиля — 4,3 %, Германии — 2,1 %. В то же время в аудитории магазинов другого профиля (компьютерная техника, сотовые телефоны, продукты и т. д.) доля «стран диаспоры» составляет лишь 3-3,5 %. В противоположном направлении изменяется процент российских пользователей — 67 % в книжных магазинах, магазинах музыки и видео и около 85 % в прочих магазинах.

По данным magazin.ru на март 2000 г. предпочтения российских Интернет-покупателей распределялись следующим образом.

Рис. 1.4. Распределение электронных покупок по видам товаров/услуг

По данным raexport.ru распределение оборотов российских Интернет-магазинов по товарным категориям таково:

- компьютерные товары — 54 %;
- книги, видео, музыка — 29 %;
- продукты и бытовые товары — 17 %.

Сегодня в России для доставки товаров, купленных через Интернет, в 55 % случаев используются курьерские службы, *а в 26%* — почтовые посылки.

По оценкам компании Torg.ru в более чем 80 % случаев оплата товаров совершается либо наличными при доставке курьером, либо банковским переводом на счет магазина. В остальных случаях расчеты за покупку производятся с помощью пластиковых карт и электронной наличности.

Результаты более детального анализа использования пластиковых карт для оплаты покупок в Рунете приведены на сайте www.raexport.ru. Эти данные показывают, что пластиковые карты применяются главным образом для покупок программного обеспечения (20 % всех продаж ПО), а также книг и продуктов (3 %). В остальных случаях используются такие средства оплаты, как наличные, наложенный платеж и банковский перевод.

В результате оказывается, что менее 1 % всех покупок в Интернете совершается с использованием пластиковых карт.

Глава 2. Проблема безопасности

Типы мошенничества, масштабы проблемы и основные требования безопасности в электронной коммерции

Безопасность является ключевым вопросом для внедрения электронной коммерции. Легенды о мошенничествах, совершенных через Интернет (кстати говоря, часто преувеличенные), уже стали притчей во языцех. Мошеннические транзакции, совершенные с помощью украденных реквизитов карт, магазины, бесследно исчезающие с рынка после успешно исполненных афер, фиктивные магазины, предназначенные для сбора информации о картах клиентов, — все это постоянные спутники сегодняшней ЭК.

Психологический фактор, связанный с осознанием угрозы потенциального мошенничества, остается основным препятствием для использования Интернета в качестве средства проведения коммерческих операций. Люди до сих пор не рассматривают Интернет как безопасную среду, чему способствуют как объективная информация о степени безопасности работы в Интернете, так и новомодные фильмы и рассказы о хакерах, успешно преодолевающих любые препятствия на пути к сколь угодно защищенной информации. Опросы показывают, что более всего люди боятся потенциальной угрозы получения кем-либо их персональных данных при работе через Интернет. По данным платежной системы VISA около 23 % транзакций ЭК так и не производится из-за боязни клиента ввести запрашиваемую электронным магазином персональную информацию о клиенте.

Как результат, люди главным образом используют Интернет в качестве информационного канала для получения интересующей их информации. Лишь немногим более 2 % всех поисков по каталогам и БД в Интернете заканчиваются покупками.

Приведем некоторые данные о масштабах мошенничеств в ЭК.

Примерно 25 % всех сообщений chargeback (отказ от платежа), генерируемых в платежных системах, приходится на транзакции Cardholder

Not Present, среди которых большая часть являются транзакциями ЭК. Заметим, что транзакции ЭК занимают второе место среди всех видов мошенничества по кредитным картам, уступая лишь мошенничествам, совершенным по украденным или потерянным картам (Lost/Stolen) — 40 %, и сравнявшись с мошенничествами по подделанным картам (Counterfeit) — 25 %. Полезно также отметить, что создание и отправка одного сообщения chargeback обходится банку-эмитенту в среднем в $10—15, а во многих случаях, связанных с электронной коммерцией, эта сумма может быть в несколько раз больше.

По данным платежной системы VISA объем сообщений chargeback в классе транзакций ЭК в 2000 г. варьируется от 0,5 % до 1 %. Для сравнения — средний объем мошенничеств в этой платежной системе составляет 0,1 %. По данным исследования, выполненного компанией Gartner Group, уровень мошенничества в ЭК в 12 раз выше, чем при выполнении обычных покупок с помощью пластиковых карт. Доля мошеннических транзакций ЭК имеет постоянную тенденцию к росту. Кроме того, следует иметь в виду, что мошенничества в ЭК имеют в основном латентный характер, поскольку наиболее распространенной стратегией мошенников является выполнение транзакций на небольшие суммы, которые часто остаются незамеченными пострадавшими владельцами счетов.

Общий объем транзакций ЭК в системах VISA и MasterCard в 2000 г. составлял около $40 млрд; при этом размер отказов от платежей (chargeback) варьируется от $250 до 500 млн.

На региональной конференции Russia Sub-Regional Meeting компании VISA, проходившей весной 2000 г. в Сан-Франциско, выражалась серьезная обеспокоенность быстрым ростом мошенничества в платежных системах, отмечаемым с сентября 1998 г. В частности, с сентября 1998 г по сентябрь 1999 г. рост уровня мошенничества в ЭК в системе VISA составил 31 % и общая сумма украденного составила $313 млн за год.

По данным консалтинговой компании Meridien Research в 2000 г. сумма похищенных через Интернет средств достигла $1,6 млрд. Больше всего от электронных краж пострадали Соединенные Штаты. По прогнозам той же компании, если ситуация с безопасностью в ЭК не поменяется кардинальным образом, в 2005 г. объем потерь будет составлять уже $15,5 млрд.

Некоторые Интернет-продавцы утверждают, что каждая четвертая попытка провести транзакцию через Интернет является мошеннической. Большинство таких транзакций завершаются отказом от авторизации из-за неправильного номера карты и/или срока действия карты. Еще

более угрожающе выглядят данные системы VISA, утверждающей, что 47 % случаев предъявления ее карточек через Интернет оказываются мошенническими.

Следует отметить, что все приведенные выше цифры являются приблизительными (и на это указывают их источники). Это связано с разными обстоятельствами. В частности, только с середины 2000 г. стало обязательным «помечать» транзакции ЭК специальным образом, что позволило платежным системам корректно учитывать транзакции, совершенные через Интернет (до этого такие транзакции в основном идентифицировались системами как MO/TO-транзакции).

Кроме того, известны факты сокрытия банками случаев совершения мошенничеств в их торговых предприятиях. Проблема латентности мошенничеств, связанных с транзакциями ЭК, часто вызвана небольшим размером таких транзакций. Маленький размер транзакции делает ее незаметной для владельца счета. Так, например, в случае нашумевшего дела, связанного с российским сайтом polit.ru (ТП, работавшее через систему CyberPlat), более 90 % владельцев карт не заметили транзакции, никогда ими не совершавшиеся, в виду малости размеров последних.

В соответствии с данными международных платежных систем все конфликты, связанные с 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 украденных реквизитов карт (номер карты, срок ее действия и т. п.).

Существуют и другие причины возникновения конфликтов этого класса. Случается, что транзакция выполняется одним из членов семьи владельца карты, о чем последний ничего не знает. Еще одна причина — владелец карты по информации, полученной в своем банке, не узнает имени ТП, в котором он совершал покупку. Поэтому так важно, чтобы ТП оформляло электронный чек, выдаваемый клиенту в качестве подтверждения приема заказа от покупателя, правильным образом, о чем подробнее будет рассказано далее.

Второй класс конфликтов в специальных комментариях не нуждается. К сожалению, иногда случается так, что некоторые 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 определять наличие того или иного товара на складе. В результате только после приема заказа выясняется, что интересующего клиента товара в ТП уже нет. Другая причина состоит в перегрузке ТП заказами (это характерно для праздничных дней, когда обороты вырастают на порядок). В результате обязательства магазина по доставке товара в оговоренные сроки оказываются сорванными, что, как правило, рассматривается клиентом как невыполнение заказа. Во избежание chargeback этого класса ТП должно иметь в своем арсенале развитый бэк-офис, эффективно управляющий запасами товаров на складах, а также обладающий модулем логистики, прогнозирующим сроки доставки товара покупателю.

Другим универсальным способом решения проблемы является задержка отправки финансового сообщения (презентмента) эмитенту владельца карты до момента исполнения заказа.

Наконец, третий класс конфликтов связан со случаями, когда ТП к согласованной с покупателем цене вдруг неожиданно для последнего добавляет дополнительные платы (налоги, плату за доставку и т. п.). Несогласие клиента с таким подходом к делу иногда выливается в жалобу последнего своему банку, генерирующему в свою очередь отказ от платежа, направляемый обслуживающему банку.

В России по данным STB CARD, крупнейшего российского процессора транзакций, выполняемых по пластиковым картам, уровень мошенничества в Интернете составляет примерно 0,5-3 % от оборотов в ЭК. К этим цифрам нужно относиться осторожно, принимая во внимание общие объемы этого бизнеса в России сегодня (несколько тысяч транзакций в день), а также виды услуг, оказываемых электронными торговыми предприятиями (сегодняшний сектор рынка ЭК в России — продажа книг, сувениров, подписка на журналы и газеты и т. п. — не представляет серьезного интереса для мошенников). При этом количество попыток совершить мошенническую транзакцию по данным STB CARD составляет 5-15 % от общего количества транзакций.

По данным МВД РФ количество преступлений, совершаемых через Интернет, растет, и растет быстро. Если в 1998 г. число подобных преступлений находилось на отметке 80, то в 1999 г. их было уже около 200, а в первом квартале 2000 г. больше, чем за весь предыдущий год.

Классификация типов мошенничества в электронной коммерции

Высокий уровень мошенничества в Интернете является сдерживающим фактором развития ЭК, поскольку покупатели, торговля и банки боятся пользоваться этой технологией из-за опасности понести финансовые потери.

Приведем классификацию возможных типов мошенничества через Интернет, приводимую международными платежными системами:

- транзакции, выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т. п.);
- компрометация данных (получение данных о клиенте через взлом БД торговых предприятий или путем перехвата сообщений покупателя, содержащих его персональные данные) с целью их использования в мошеннических целях;
- магазины, возникающие, как правило, на непродолжительное время, для того чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;
- злоупотребления торговых предприятий, связанные с увеличением стоимости товара по отношению к предлагавшейся покупателю цене или повтором списаний со счета клиента;
- магазины и торговые агенты (Acquiring Agent), предназначенные для сбора информации о реквизитах карт и других персональных данных покупателей.

Обычно в рамках подобной классификации фигурирует еще пункт «Информационные сайты». Речь идет о сайтах, помогающих всевозможными рекомендациями и даже программными средствами совершить мошенническую транзакцию. Мы выносим этот пункт из общего перечня возможных типов мошенничества, поскольку он не связан непосредственно с процессом ЭК.

Коротко остановимся на перечисленных типах мошенничества в отдельности. Как уже отмечалось, первый тип мошенничества является наиболее массовым. Для совершения транзакции ЭК мошеннику обычно достаточно знать только номер карты и срок ее действия. Такая информация попадает в руки мошенников различными путями. Наиболее распространенный способ получения мошенниками реквизитов карт — сговор с сотрудниками торговых предприятий. ТП, через которые проходят сотни и тысячи транзакций по пластиковым картам,

зачастую хранят информацию о реквизитах карт в своих БД или на слипах (бумажных документах, подтверждающих факт совершения в ТП транзакции). Результатом сговора становится передача информации о реквизитах карт в руки криминальных структур.

Другой способ получения информации о реквизитах карт, ставший популярным в последнее время, — кража БД карточек в ТП, о чем будет рассказано чуть ниже.

Еще одним способом генерации правильного номера карты является программа CreditMaster, используемая мошенниками с 1995 г. Сегодня версия 4.0 этой программы может быть найдена на ряде сайтов в Интернете. Программа генерирует правильные номера карт, эмитированных некоторыми банками, используя для генерации номеров тот же алгоритм, что и банк-эмитент.

Достаточно распространенным является способ, когда криминальные структуры организуют свои магазины и торговые агенты (см. пятый тип мошенничества) с главной целью получить в свое распоряжение значительные наборы реквизитов карт. Часто такие магазины представляют собой различного рода порносайты. Сегодня западными спецслужбами установлена тесная связь порнобизнеса в Интернете с преступными группировками, специализирующимися на мошенничествах с пластиковыми картами.

Другая функция подобных магазинов состоит в их использовании для «отмывания» полученных реквизитов карт. Через подобные сайты «прокачиваются» сотни тысяч и даже миллионы украденных реквизитов карт.

Иногда обе функции — кража и «отмывание» — совмещаются в одном магазине. Например, воспользовавшись однажды услугами порносайта, владелец карты с удивлением выясняет, что стал подписчиком такого сайта, и, таким образом, с него ежемесячно будет взиматься плата за подписку, отказаться от которой весьма проблематично.

Наконец, существует и еще один способ узнать правильные реквизиты карт. Точнее не узнать, а эмпирически вычислить. Дело в том, что Интернет представляет собой прекрасный плацдарм для проведения различного рода «испытаний» с целью определения правильных реквизитов карт. Например, если мошеннику известен номер карты, но не известен срок ее действия, то определить этот параметр карты не составляет большого труда. Действительно, пластиковая карта обычно выпускается сроком на два года. Параметр «срок действия карты» определяет месяц и последние две цифры года, когда действие карты за-

канчивается. Таким образом, мошеннику требуется перебрать всего лишь 24 возможных варианта этого параметра. В реальном мире сделать это не просто. В виртуальном мире решение подобной задачи не составляет труда. Мошеннику нужно отправить не более 24 авторизационных запросов для того, чтобы с вероятностью 1 определить верный срок действия карты. После этого воспользоваться известными реквизитами карты можно различными способами. Проще всего совершить транзакцию ЭК. Более эффективный способ воспользоваться добытым знанием — изготовить поддельную карту с вычисленными реквизитами карты и использовать ее для оплаты покупок в реальных ТП. В этом случае такое мошенничество попадет в разряд «подделанная карта» (Counterfeit).

Приведенные выше рассуждения относились к случаю, когда известен номер карты и требовалось определить срок ее действия. Нужно сказать, что с помощью Интернета вполне решаемой становится задача вычисления обоих основных параметров пластиковой карты — ее номера и срока действия. Действительно, в большинстве случаев номер карты представляет собой число, состоящее из шестнадцати десятичных цифр (хотя в соответствии со стандартом ISO 7812 «Идентификационные карты — система нумерации и процедура регистрации идентификаторов эмитентов» номер карты может состоять из 19 цифр). Из 16 цифр номера карты 6 первых представляют собой BIN (Bank Identification Number), предоставляемый банку либо международной платежной системой, участником которой он является, либо непосредственно организацией American Bankers' Association, уполномоченной ISO на выдачу идентификаторов банкам, если банк реализует собственную независимую карточную программу. Кроме того, достаточно часто крупные и средние банки используют 7 и 8-ю цифры номера для идентификации своих филиалов и отделений. Наконец, последняя цифра номера карты — цифра проверки на четность по алгоритму Luhn Check Parity, однозначно определяемая всеми остальными цифрами номера карты.

Таким образом, как правило, только 7 цифр номера карты являются независимыми переменными. Остальные цифры определены платежной системой и банком-эмитентом. Эти цифры не являются конфиденциальными хотя бы потому, что содержатся в множестве различных таблиц, доступных широкому кругу специалистов. Кроме того, чтобы выяснить значения зависимых переменных номера карты, мошеннику достаточно получить для себя в интересующем его банке пластиковую карту.

С учетом того, что средний банк выпускает под одним префиксом (первые 8-11 цифр карты) 50 000-500 000 карт, легко видеть, что если банк

генерирует номер карты по случайному закону, то плотность заполнения пространства возможных номеров карт (верхняя граница отношения количества выпущенных карт ко всему возможному множеству значений номера карты) составит 0,005-0,05. С учетом числа различных вариантов срока действия карты получается, что мошеннику требуется перебрать в среднем порядка 500-5000 различных вариантов параметров карты для достижения своей цели. Очевидно, такая задача является вполне решаемой с учетом того, что мошенник имеет возможность направить авторизационные запросы одновременно в достаточно большое количество Интернет-магазинов.

Можно показать, что для того, чтобы с вероятностью Ро найти правильный номер карты при плотности заполнения диапазона возможных значений номеров р, необходимо перебрать не более

$$n = \left[\frac{9\log(1-P_0)}{9\log(1-p)\ldots} \right] + 1$$

значений номеров карт. Здесь знак [x] обозначает целую часть x. В частности при P_0=0,99 и р=0,05, п =90. Таким образом, с учетом срока действия карты необходимо перебрать не более 2160 значений реквизитов карт, чтобы с вероятностью 0,99 добиться «успеха».

Иногда помимо номера карты и срока ее действия требуется дополнительно сообщить торговому предприятию специальный цифровой код, называемый в системе VISA CW2, а в системах Europay/MasterCard — CVC2. Этот цифровой код состоит из трех десятичных цифр, которые печатаются методом индент-печати на оборотной стороне карты на панели подписи сразу вслед за номером карты, и получается с помощью специального открытого алгоритма, применяемого к таким параметрам карты, как номер карты и срок ее действия. Алгоритм базируется на применении алгоритма шифрования DES (см. далее) и использует пару секретных ключей, известных только эмитенту карты. Таким образом, зная номер карты и срок ее действия, вычислить цифровой код без знания секретных ключей невозможно.

С1 апреля 2001 г. в платежных системах Еигорау и MasterCard обслуживающие банки обязаны вставлять в авторизационные запросы для транзакций Cardholder Not Present значения CVC2. При этом, к сожалению, далеко не все эмитенты к этому моменту будут способны верифицировать полученные значения кода в своих системах (сегодняшние оценки показывают, что когда обслуживающий банк передает в сеть значение цифрового кода CVC2/CVV2, лишь примерно в 30 % случаев эмитент прове-

ряет этот параметр). Из-за того что сегодня практически всегда (случай использования протокола SET не рассматривается) ответственность за мошенничество по транзакции ЭК лежит на обслуживающем банке, некоторые эмитенты, даже определив, что значение цифрового кода неверно, дают положительный ответ (Approval) на авторизационный запрос.

Отметим, что использование цифрового кода CVV2/CVC2 в некоторой степени поможет борьбе с мошенничествами в ЭК, но не решит проблемы в целом. Действительно, несмотря на то что применение этого кода потребует от мошенника знания еще трех дополнительных цифр, сам код является статической информацией и, следовательно, рано или поздно попадет в руки мошенников теми же способами, что и номер карты. По-видимому, это стало основной причиной, по которой VISA решила пока не принимать решения об обязательном использовании значений CVV2. В качестве контраргумента против обязательного использования этого кода в ЭК VISA рассматривает повышение вероятности компрометации CVV2 в среде Интернет (подчеркнем, что CVV2 в общем случае используется для проведения транзакций «покупка» методом голосовой авторизации, что существенно повышает безопасность транзакции, выполняемой с помощью этого способа авторизации).

Отметим также, что существует еще один способ повышения безопасности транзакции ЭК — использование метода VISA Address Verification System (AVS). Суть метода состоит в следующем. ТП запрашивает у клиента параметр Cardholder Billing Address (адрес клиента, по которому он получает из своего банка-эмитента так называемые стейтменты, отчет о транзакциях, совершенных клиентом по своей карте в течение некоторого периода времени), который направляется в авторизационных запросах банку-эмитенту владельца карты для верификации. Для того чтобы метод AVS можно было применять, необходимо, чтобы параметр Cardholder Billing Address поддерживался в авторизационных запросах, передаваемых обслуживающим банком эмитенту карты. До последнего времени метод AVS поддерживался в системе VISA только американскими банками. С 15 мая 2001 г. система VISA предлагает банкам на опционной основе внедрить специальные изменения в авторизационных запросах обслуживающего банка с целью поддержки метода AVS (VISA International Address Verification System).

Технология AVS уже несколько лет успешно используется на американском рынке пластиковых карт. С апреля 2001 г. метод AVS является обязательным для банков в Великобритании.

У метода AVS два недостатка. Во-первых, он, так же как и метод проверки CVC2/CW2, является статическим и, следовательно, попадание

в руки мошенников нового параметра является лишь вопросом времени. Во-вторых, этот метод поддерживается только системой VISA, и хотя на долю этой платежной системы в мире приходится более 50 % всех транзакций ЭК, это все-таки не весь рынок платежей в Интернете. Другими словами, метод AVS не является на сегодняшний день универсальным.

Остановимся теперь на втором типе мошенничества — компрометации персональных данных владельцев пластиковых карт. 2000-й год стал рекордсменом по числу взломов БД карточек в информационных системах крупных ТП. Так, в марте этого года появилось сообщение о том, как в Уэльсе два подростка украли более 26 тысяч реквизитов карт из БД одного из электронных магазинов. К сожалению, это был единственный случай, когда мошенники были задержаны.

Другой пример является еще более масштабным. В начале 2000 г. российским хакером была вскрыта БД объемом 300 000 записей. После того как мошенник, представившийся Максимом, потребовал за сохранение тайны о случившемся выкуп в размере $100 тыс и получил в ответ отказ, часть украденных номеров карт была выставлена в Интернете для общего обозрения. Спецслужбы, занимавшиеся расследованием данного случая, отметили чрезвычайно высокий профессиональный уровень хакера — для вскрытия БД использовались методы, известные только профессионалам в области защиты информации, Кроме того, преступник так искусно скрыл следы своего присутствия на сайте ТП, что единственное, что можно было установить, так это то, что он действовал, используя российский IP-адрес.

Известно также о случае кражи реквизитов 485 тысяч карт, выставленных в сети National Aeronautic & Space Administration после отказа заплатить преступнику запрошенный им выкуп.

В середине 2000 г. Интернет-магазин Egghead.com объявил о вскрытии его системы защиты информации и краже БД карточек. БД карточек этого магазина содержала реквизиты 3,7 млн карт.

Тревогу у мировой общественности вызывает активизация действий российских хакеров. За 2000 г. более 40 американских коммерческих сайтов подверглись нападению со стороны организованных групп, действующих с территории России и Украины: хакеры завладели номерами более миллиона кредитных карт. Согласно заявлениям представителей ФБР, речь идет об одной из самых масштабных атак на электронные коммерческие сайты.

Интернет-магазин является идеальной мишенью для мошенников, желающих украсть реквизиты работающих карт. По данным исследования, проведенного Международной ассоциацией потребителей, более

двух третей сайтов торговых точек хранят эти данные по самым разным соображениям и для разных целей. К таким соображениям может относиться необходимость хранения информации о выполненных платежах, установление отношений со своими покупателями (Client Relationship Management), технические причины и т. п. Говоря о технических причинах, можно упомянуть технологию, используемую в Amazon и состоящую в том, что реквизиты карт запоминаются на сайте этого ТП, в том числе и для того, чтобы при следующем обращении клиента ему не нужно было бы вводить реквизиты своей карты заново.

Поданным компании Meridien Research уязвимость Интернет-магазинов усугубляется еще и тем, что лишь 30 % онлайновых продавцов используют надежные системы защиты для борьбы с компьютерными мошенниками.

В заключение остановимся на третьем типе мошенничества — магазинах-бабочках, открывающихся с целью «отмывания» украденных реквизитов карт. После того как в руках криминальных структур появляются украденные реквизиты карт, возникает задача ими воспользоваться. Один из способов — организация виртуального ТП, «торгующего» программным обеспечением или другими информационными ресурсами (программы телевизионных передач, подписка на новости и т. д.). В действительности, такое ТП, как правило, имеет свой сайт, но ничем реально не торгует. При этом в обслуживающий банк регулярно направляются авторизационные запросы, использующие украденные номера карт, а следовательно магазин регулярно получает от обслуживающего банка возмещения за совершенные в нем «покупки». Так продолжается до тех пор, пока уровень chargeback (отказов от платежей), от эмитентов украденных реквизитов карт не станет свидетельством того, что имеет место мошенничество. Обычно к этому моменту и сами магазины, почувствовав запах жаренного, исчезают и становятся предметом поиска правоохранительных органов.

Магазины-бабочки обычно выбирают две крайние стратегии своей работы. Выбор стратегии определяется размером украденной БД карточек. Если размер украденной БД достаточно большой (десятки тысяч карт), то выбирается стратегия, в соответствии с которой транзакции делаются на небольшие суммы (порядка $10 США). Основная идея такой стратегии заключается в том, что действительный владелец карты заметит небольшую потерю средств на своем счете далеко не сразу и в результате за имеющееся в распоряжении мошенников время (как правило, 1-3 месяца) можно на подобных небольших транзакциях украсть сотни тысяч долларов.

Наоборот, когда в распоряжении мошенников несколько десятков карт, выбирается стратегия выполнения транзакций на крупные суммы

(несколько тысяч долларов). В этом случае активная жизнь магазина-бабочки составляет несколько недель, после чего магазин исчезает.

Резюмируя все сказанное, следует отметить следующее:

- в основе всех мошенничеств в ЭК лежит попадание в руки криминала информации о реквизитах действующих карт;
- внедрение дополнительных методов повышения безопасности транзакций ЭК (CVC2/CVV2, AVS), сводящихся к увеличению размеров статических реквизитов карт, даст эффект в течение относительно небольшого интервала времени, но не позволит решить проблему кардинальным образом. Криминал не оставит попыток приобретения реквизитов карт, используя для этого самые разнообразные методы, начиная от классических (сговора с персоналом ТП) и заканчивая вскрытием БД карточек ТП и созданием специальных магазинов, ставящих своей главной целью завладеть информацией о номерах карт.

Способы решения проблемы безопасности в электронной коммерции

С самого начала внедрения электронной коммерции стало очевидно, что методы идентификации владельца карты, применяемые в обычных транзакциях, являются неудовлетворительными для транзакций ЭК.

Действительно, при совершении операции покупки в физическом магазине продавец имеет возможность рассмотреть предъявляемую для расчетов пластиковую карту на предмет ее соответствия требованиям платежным системам (в частности, проверить наличие голограммы, специальных секретных символов, сверить подпись на панели подписи и торговом чеке и т. п.). Кроме того, продавец может потребовать от покупателя документ, удостоверяющий его личность. Все это делает мошенничество по поддельной карте достаточно дорогим мероприятием.

В случае транзакции ЭК все, что требуется от мошенника — знание реквизитов карты. Затраты, связанные с изготовлением поддельной физической карты, в этом случае не требуются. Безусловно, это не может не привлечь внимание криминала к этому типу коммерции, свидетелями чему мы становимся уже сегодня.

В мире пластиковых карт с магнитной полосой самым надежным способом защиты транзакции от мошенничества является использование PIN-кода для идентификации владельца карты его банком-эмитентом. Секретной информацией, которой обладает владелец карты, является

PIN-код. Он представляет собой последовательность, состоящую из 4-12 цифр, известную только владельцу карты и его банку-эмитенту. PIN-код применяется всегда при проведении транзакций повышенного риска, например при выдаче владельцу карты наличных в банкоматах. Выдача наличных в банкоматах происходит без присутствия представителя обслуживающего банка (ситуация похожа на транзакцию ЭК). Поэтому обычных реквизитов карты для защиты операции «снятие наличных в банкомате» недостаточно и используется секретная дополнительная информация — PIN-код.

Более того, общая тенденция развития платежных систем — более активное использование PIN-кода для операций «покупка» по дебетовым картам. Казалось бы, использование подобного идентификатора могло бы помочь решить проблему безопасности в ЭК, однако это не так. К сожалению, в приложении к ЭК этот метод в классическом виде неприменим.

Действительно, использование PIN-кода должно производиться таким образом, чтобы этот секретный параметр на всех этапах обработки транзакции оставался зашифрованным (PIN-код должен быть известен только владельцу карты и ее эмитенту). В реальном мире это требование реализуется за счет использования в устройствах ввода транзакции специальных физических устройств, называемых PIN-PAD и содержащих Hardware Security Module — аппаратно-программные устройства, позволяющие хранить и преобразовывать некоторую информацию весьма надежным способом. Эти устройства хранят специальным способом защищенный секретный коммуникационный ключ, сгенерированный обслуживающим банком данного ТП. Когда владелец карты вводит значение PIN-кода, оно немедленно закрывается (шифруется) коммуникационным ключом и отправляется внутри авторизационного запроса на хост обслуживающего банка. Точнее говоря, шифруется не сам PIN-код, а некоторый электронный «конверт», в который код помещается. На хосте обслуживающего банка зашифрованный идентификационный код перекодируется внутри Hardware Security Module хоста (хост обслуживающего банка также имеет свое устройство шифрования) в блок, зашифрованный на коммуникационном ключе платежной системы, и передается в сеть для дальнейшего предъявления эмитенту. По дороге к эмитенту PIN-код будет преобразовываться еще несколько раз, но для наших рассуждений это не важно. Важно другое — для того чтобы следовать классической схеме обработки PIN-кода, каждый владелец карты должен хранить криптограммы коммуникационных ключей всех обслуживающих банков, что на практике невозможно.

Классическую схему можно было бы реализовать с помощью применения асимметричных алгоритмов с шифрованием PIN-кода владельца карты открытым ключом ТП. Однако для представления PIN-кода в платежную сеть его необходимо зашифровать, как это принято во всех платежных системах, симметричным ключом. Автор не знает ни одного стандартного Hardware Security Module, способного выполнить трансляцию PIN-кода, зашифрованного с помощью асимметричного криптоалгоритма, в PIN-код, зашифрованный на симметричном алгоритме шифрования.

Существует другое, неклассическое решение по использованию PIN-кода. Например, можно на компьютере владельца карты шифровать PIN-код плюс некоторые динамически меняющиеся от транзакции к транзакции данные на ключе, известном только эмитенту и владельцу карты. Такой подход потребует решения задачи распределения секретных ключей. Эта задача является весьма непростой (очевидно, что у каждого владельца карты должен быть свой индивидуальный ключ), и если уж она решается, то использовать ее решение имеет смысл для других, более эффективных по сравнению с проверкой PIN-кода методов аутентификации владельца карты.

В то же время идея проверки PIN-кода была реализована для повышения безопасности транзакций ЭК по картам, БД которых хранится на хосте процессора STB CARD. В общих чертах STB CARD реализует следующую схему. Владельцы карт, эмитенты которых держат свою БД карточек на хосте STB CARD, могут получить дополнительный PIN-код, называемый ПИН2. Этот код представляет собой последовательность из 16 шестнадцатеричных цифр, которая распечатывается в PIN-конверте, передаваемом владельцу карты (специальный бумажный конверт, используемый банком-эмитентом для хранения в нем секретной информации, относящейся к эмитированной карте), и вычисляется эмитентом с помощью симметричного алгоритма шифрования, примененного к номеру карты и использующего секретный ключ, известный только эмитенту карты.

Далее во время проведения транзакции ЭК на одном из ТП, обслуживаемом банком STB CARD, у владельца карты в процессе получения данных о клиенте запрашивается информация по ПИН2. Клиент вводит значение кода ПИН2 в заполняемую форму и возвращает ее ТП.

Здесь нужно сделать важное замечание относительно сказанного ранее. Владелец карты в действительности ведет диалог в защищенной SSL-сессии не с ТП, а с виртуальным POS-сервером, через который работает ТП (система STB CARD в настоящее время использует сервер Assist).

Возвращаясь к схеме STB CARD, отметим, что, конечно же, в заполненной клиентом форме ПИН2 не содержится, а в действительности все выглядит следующим образом: ТП (точнее, сервер Assist), определив, что имеет дело с картой банка STB CARD, передает владельцу карты форму, содержащую подписанный Java-апплет, реализующий некоторый симметричный алгоритм шифрования. При этом ПИН2 играет роль секретного ключа этого алгоритма шифрования, а шифруемые данные получаются в результате применения хэш-функции к номеру карты, сумме и дате транзакции, а также случайному числу £„ генерируемому ТП. Таким образом, в заполненной владельцем карты форме присутствует только результат шифрования перечисленных выше данных о транзакции на ключе ПИН2.

Далее ТП формирует авторизационное сообщение, передаваемое на хост обслуживающего банка, содержащее помимо «стандартных» данных о транзакции еще результат шифрования и случайное число £„

Эмитент карты, получив сообщение ТП, по номеру карты вычисляет значение ПИН2, и далее по номеру карты, сумме и дате транзакции, а также по случайному числу %, вычисляет результат шифрования этих данных на ключе ПИН2. Если полученная величина совпадает с аналогичной величиной из сообщения ТП, верификация PIN-кода считается выполненной успешно. В противном случае транзакция отвергается.

Таким образом, технология проверки PIN-кода, принятая в системе STB CARD, в действительности обеспечивает не только динамическую аутентификацию клиента, но еще и гарантирует «сквозную» целостность некоторых данных о транзакции (сумма транзакции, номер карты). Под «сквозной» целостностью здесь понимается защита от модификации данных на всем протяжении их передачи от клиента до банка-эмитента.

Минусы данного подхода состоят в следующем:

- Для реализации схемы проверки значения PIN-кода необходимо, чтобы ТП «умело» формировать соответствующую форму с Java-апплетом, что сразу сужает область применения схемы в относительно небольшом множестве ТП.
- Использование длинного (шестнадцать шестнадцатеричных цифр) ключа делает его применение на практике крайне неудобным для владельца карты.
- Защита от подставки (форма, запрашивающая ПИН2, предоставляется владельцу карты не ТП, а мошенником, желающим узнать значение ПИН2) основана на надежности аутентификации клиентом сервера ТП, а также на подписывании апплета секретным клю-

чом сервера ТП. Поскольку нарушение обеих защит приводит только к появлению на экране монитора владельца карты соответствующего предупреждения, сопровождаемого вопросом — продолжить сессию или нет, то особенно доверять этим формам защиты не стоит.

Обеспечить надежную защиту от подставки можно с помощью электронного бумажника клиента (специального программного обеспечения, которое клиент может «скачать» на свой компьютер с некоторого сайта), заменяющего по своей функциональности Java-апплет в форме ТП. Такой электронный бумажник может использовать сколь угодно мощные средства шифрования данных. Секретные ключи владельца карты могут держаться в порядке повышения надежности их хранения на диске компьютера, дискете или микропроцессорной карте. Доступ к электронному бумажнику должен производиться по паролю его владельца.

В результате проведенного анализа платежные системы сформировали основные требования к схемам проведения транзакции ЭК, обеспечивающим необходимый уровень ее безопасности. Эти требования сводятся к следующему:

- Аутентификация участников покупки (покупателя, торгового предприятия и его обслуживающего банка). Под аутентификацией покупателя (продавца) понимается процедура, доказывающая (на уровне надежности известных криптоалгоритмов) факт того, что данный владелец карты действительно является клиентом некоторого эмитента-участника (обслуживающего банка-участника) данной платежной системы. Аутентификация обслуживающего банка доказывает факт того, что банк является участником данной платежной системы.
- Реквизиты платежной карты (номер карты, срок ее действия, CVC2/CVV2 и т. п.), используемой при проведении транзакции ЭК, должны быть конфиденциальными для ТП.
- Невозможность отказа от транзакции для всех участников транзакции ЭК, то есть наличие у всех участников неоспоримого доказательства факта совершения покупки (заказа или оплаты).
- Гарантирование магазину платежа за электронную покупку — наличие у ТП доказательства того, что заказ был ТП выполнен.

Всюду далее под протоколом ЭК понимается алгоритм, определяющий порядок взаимодействия участников ЭК (владельца карты, торгового предприятия, обслуживающего банка, банка-эмитента и центра сертификации) и форматы сообщений, которыми участники ЭК обмениваются друг с другом с целью обеспечения процессов авторизации и расчетов.

Глава 3. Введение в криптографию

Общие понятия

Как уже отмечалось ранее, криптография играет одну из главных ролей в развитии технологий и стандартов ЭК. В используемых протоколах ЭК решаются типовые для различных областей техники задачи защиты информации от несанкционированного доступа, к числу которых относятся:

- обеспечение целостности информации (невозможность для третьей стороны, расположенной между участниками информационного обмена, модифицировать передаваемую информацию таким образом, чтобы принимающая сторона атого не заметила);
- обеспечение конфиденциальности информации (невозможность для третьей стороны получить информацию, содержащуюся в передаваемых сообщениях);
- аутентификация источника информации (подтверждение того, что передающая сторона является тем, за кого она себя выдает); остальную часть этого пункта нужно вычеркнуть то есть невозможность для третьей стороны присвоить себе авторство какого-либо сообщения);
- нотаризация информации (невозможность отказаться от авторства сообщения).

Для решения перечисленных задач используются различные криптографические алгоритмы. Под криптоалгоритмом понимается взаимнооднозначное преобразование, отображающее множество возможных сообщений отправителя, содержание которых необходимо скрыть от третьей стороны, во множество сообщений, называемых также криптотекстами, понятных только отправителю и адресату. Криптоалгоритмы иначе называют алгоритмами шифрования.

Все алгоритмы шифрования делятся на два класса:

- симметричные алгоритмы шифрования;
- асимметричные алгоритмы шифрования.

Симметричные алгоритмы шифрования основаны на использовании обеими сторонами информационного обмена общего секрета, называемого ключом. Знание ключа X полностью определяет криптографическое преобразование $Z=E_X(Y)$, которое еще иначе называют засекречиванием сообщения Y. Это преобразование является взаимно однозначным, то есть существует такая функция $E_X'(Z)$, что для любых Z и Y, связанных равенством $Z=E_x(Y)$, верно $Y=E_x^{-1}(Z)$. Обратное преобразование часто называют расшифрованием или дешифрованием сообщения Z.

Симметричные алгоритмы появились в глубокой древности для засекречивания важных сообщений. Уже знаменитый греческий историк Геродот (V век до нашей эры) приводил примеры писем, понятных только отправителю и адресату. Спартанцы использовали специальный механический прибор, при помощи которого важные сообщения писались особым способом, обеспечивающим сохранение тайны сообщения.

Самым надежным симметричным криптографическим алгоритмом является код Вернама. Суть алгоритма состоит в том, что для каждого отправляемого сообщения Y, представленного в виде последовательности двоичных нулей и единиц, по случайному закону генерируется из нулей и единиц последовательность той же длины, что и отправляемое сообщение. Эта последовательность играет в схеме Вернама роль одноразового ключа X. Тогда криптографическое преобразование состоит в побитном сложении по модулю 2 значений X и Y. Очевидно, что для «вскрытия» описанного криптоалгоритма (то есть для определения Y) необходимо перебрать все возможные значения ключа X.

Очевидными недостатками этого метода являются необходимость передачи получателю значения ключа Y для каждого шифруемого сообщения, а также переменная длина ключа. Конечно, различные значения ключа в схеме Вернама можно было бы перенумеровать и один раз передать надежным образом получателю (например, передачей из рук отправителя в руки получателя файла со значениями ключа). После этого в конце каждого зашифрованного сообщения можно сообщать получателю, каким по номеру значением ключа пользовался отправитель для засекречивания сообщения. Но при этом очевидно, что объем возможных значений ключа должен быть соизмерим с объемом информации, которым обмениваются стороны, что приводит к тому, что схема Вернама практически не используется (сегодня эта схема применяется в основном в военных системах для передачи очень важной информации).

Далее будет подробнее рассказано о других симметричных алгоритмах. В основе таких алгоритмов лежит принцип использования одного клю-

ча относительно небольшого размера. Такие алгоритмы позволяют преобразовывать различные сообщения Y_1, Y_2, ...,Y_n таким образом, что, даже зная значения функции $Z_j=E_x(Y_j)$ (i=1, ...,n) для достаточно большого числа n, невозможно определить значение ключа X (отметим, что при использовании схемы Вернама для определения ключа достаточно знать единственную пару значений функции Z и сообщения Y).

Суть асимметричных алгоритмов (иначе схемы, основанные на таких алгоритмах, называют криптосистемами с общественными или открытыми ключами) состоит в следующем. В математике известны такие функции E, для которых обратная функция D вычисляется достаточно сложно, если не известен некоторый параметр (в криптографических схемах этот параметр становится секретным ключом). Функция E предоставляется в распоряжение любому желающему отправить сообщение обладателю параметра. Для шифрования информации, предназначенной обладателю параметра, достаточно применить к передаваемому сообщению преобразование E. Тогда обладатель параметра, используя обратное преобразование D, легко расшифровывает полученное сообщение. Наоборот, лицо, не обладающее заветным параметром, не сумеет вычислить обратное преобразование и, следовательно, восстановить передаваемое сообщение. Понятие «не сумеет» имеет достаточно специфический смысл, который будет разъяснен далее.

Асимметричные алгоритмы являются идеальным механизмом для решения задач обеспечения целостности передаваемой информации и аутентификации ее источника. Решаются эти задачи с помощью схем с открытыми ключами следующим образом. В первую очередь к передаваемому сообщению Y (далее без ограничения общности предполагается, что сообщение Y имеет двоичное представление) применяется преобразование H(Y), называемое хэш-функцией, или дайджестом сообщения, отображающее сообщение Y в двоичную последовательность фиксированной длины (как правило, меньшей длины). Множество значений хэш-функции будет обозначаться M. Таким образом, преобразование H(Y) не является взаимно однозначным (зная значение H(Y) почти всегда невозможно однозначно определить значение Y), и потому его относят к классу односторонних функций. К преобразованию H(Y) предъявляют несколько плохо формализуемых требований, на качественном уровне состоящих в следующем:

- мощность множества M должна быть достаточно большой (на практике используются значения H(Y) длиной от 128 до 256 битов, хотя длина значения хэш-функции определяется конкретной задачей);

Q сообщения Y «равномерно» отображаются с помощью H(Y) в элементы множества M, то есть каждому элементу множества M соответствует примерно одинаковое количество сообщений Y, отображаемых в этот элемент (примерно |A|/|M|, где |A|, |M| — мощности, соответственно, множества всех возможных сообщений Y и множества значений хэш-функции);

- функция H(Y) не должна быть непрерывной, то есть из «близости» значений Y_x и Y_2 не следует «близость» значений $H(Y_t)$ и $H(Y_2)$.

Для практических целей, очевидно, достаточно, чтобы выполнялось неравенство |M| < |A|. Легко показать, что в этом случае вероятность того, что для любых случайно выбранных сообщений Y, и Y_2 выполняется H(Yj)=H(Y_2), равна |M|"'. В случае, когда функция H(Y) отображает сообщения в множество всех двоичных последовательностей длины т, вероятность события H(Y,)=H(Y_2) равна $2^{т}$. Длина значения хэш-функции на практике определяется вероятностью того, что значения хэш-функции от двух случайно выбранных сообщений не равны друг другу. Например, при т=160 такая вероятность приблизительно равна $0{,}68* 10^{-48}$, что делает событие H(Y,)=H(Y_2) фактически невероятным.

После того как для сообщения Y вычислено значение хэш-функции H(Y), к нему применяется закрытое преобразование D отправителя сообщения. Значение s=D(H(Y)) и является электронной цифровой подписью (ЭЦП) сообщения Y.

Для проверки (верификации) цифровой подписи принимающая сторона применяет к s обратное преобразование E и полученное значение hj=E(s) сравнивает со значением h_2=H(Y_r), где Y_r — полученное сообщение, которое в общем случае может отличаться от переданного сообщения (например, из-за попытки исказить переданное сообщение).

Если hj=h_2, то ЭЦП верна, что, во-первых, аутентифицирует источник информации (передающую сторону), а во-вторых, подтверждает целостность полученного сообщения (Y=Y_r). Напомним читателю, что целостность сообщения подтверждается с вероятностью того, что значения хэш-функции от двух различных аргументов совпадают.

Теперь рассмотрим, как симметричные и асимметричные алгоритмы используются для решения задач обеспечения безопасности информационного обмена. Для решения задач аутентификации источника информации и обеспечения ее целостности, как правило, используются асимметричные алгоритмы шифрования. Эти алгоритмы по своей природе предназначены для решения подобных задач в системах информационного обмена между многими пользователями (закрытое преобразование для подписи и открытое — для проверки подписи).

Для решения задачи обеспечения конфиденциальности передаваемой информации обычно применяются симметричные алгоритмы. Если открытое и закрытое преобразования в асимметричном алгоритме определены на одном множестве сообщений и являются коммутативными, то есть выполняется равенство E(D(Y))=D(E(Y)), то асимметричный алгоритм может использоваться и для шифрования сообщений. Действительно, передающая сторона преобразует сообщение Y в сообщение E(Y) с помощью открытого преобразования адресата сообщения. Тогда обратное преобразование сможет выполнить только получатель сообщения, а значит, содержание Y будет известно только адресату, что и требовалось получить.

Нужно отметить, что свойством коммутативности обладают многие известные асимметричные алгоритмы (например, самый известный алгоритм — RSA). Однако на практике свойство «шифрования» таких асимметричных алгоритмов используется очень редко и, как правило, только для того, чтобы две стороны информационного обмена в начале конфиденциального диалога обменялись между собой симметричным ключом шифрования, который далее используется для шифрования сообщений внутри диалога. Это обстоятельство связано с тем, что при равной степени защиты, обеспечиваемой симметричными и асимметричными алгоритмами, первые работают на 2-4 порядка быстрее вторых. Скорость работы алгоритма (вычислительная сложность алгоритма) является ключевым фактором во многих системах информационного обмена, что и определяет главную роль симметричных алгоритмов при решении задачи обеспечения конфиденциальности информационного обмена.

Комбинирование симметричных и асимметричных алгоритмов мастерски реализовано в протоколе SET с целью оптимизации времени выполнения транзакции ЭК.

Краткий обзор симметричных алгоритмов шифрования

Обзор начнем с самого популярного в мире симметричного алгоритма шифрования — алгоритма DES (Data Encryption Standard).

Алгоритм DES был разработан фирмой IBM и в 1977 г. принят Национальным институтом стандартов и технологий (National Institute of Standards and Technology) в качестве стандарта Правительства США для шифрования информации категории «less-than-top-secret» (ниже,

чем высшей категории секретности). С тех пор он повторно сертифицировался в качестве такого стандарта каждые 5 лет вплоть до 1993 г. В 1998 г. Национальный институт стандартов и технологий США отказался сертифицировать DES, что было связано с тем, что уровень развития вычислительной техники сделал возможным вскрытие DES относительно дешевыми средствами.

DES является так называемым «блочным шифром» (когда шифруемая информация обрабатывается блоками фиксированной длины, в случае DES длина блока составляет 64 бита) и имеет ключ длиной 56 битов (ключ представляется двоичной последовательностью длиной 64 бита, которая получается из последовательности битов ключа добавлением после каждых 7 битов ключа бита проверки на нечетность; таким образом, в двоичном представлении ключа в позициях 8, 16, 24,..., 64 стоят биты проверки на нечетность).

В основе алгоритма DES лежат многочисленные нелинейные преобразования (перестановки, подстановки, сдвиги и S-преобразования), выполняемые над отдельным элементами шифруемого блока. Такие преобразования могут быть описаны системой нелинейных уравнений, решение которой является NP-полной задачей (не существует известного полиномиального по сложности алгоритма решения).

Очень схематично опишем работу алгоритма DES. Сначала 64-битовый блок шифруемой информации W подвергается начальной фиксированной перестановке (каждый бит w занимает положение, задаваемое специальной таблицей, определенной DES). Получившийся в результате блок w представляется в виде $W=L(0)R(0)$, где $L(0), R(0)$ соответственно первые и последние 32 бита W.

Алгоритм DES является циклическим. Если вычислены значения $L(n-1)$, $R(n-1)$ для $1 \le n \le 16$, то $L(n), R(n)$, определяются следующими равенствами:

$$L(n)=R(n-1);$$

$$R(n)=L(n-1) \oplus (R(n-1),K(n));$$

где $\oplus$ означает побитовое сложение, функция f определена далее, а $K(n)$ — 48-битовые последовательности, получаемые из ключа DES с помощью фиксированного набора определенных в стандарте DES перестановок, сдвигов и подстановок. Криптотекст оригинального блока W представляет собой блок $L(16)R(16)$.

Очевидно, что расшифрование криптотекста осуществляется с помощью следующего набора равенств:

$$R(n-1)=L(n);$$
$$L(n-1)=R(n)\oplus(L(n),K(n))$$

для $1\le n\le 16$, После вычисления с помощью этих равенств значений L(0), R(0) расшифрование начального блока очевидно.

Функция /(x,y), где x — двоичная переменная длиной 32 бита, а y — переменная длиной 48 битов, имеет областью допустимых значений множество всевозможных последовательностей длиной 32 бита и строится следующим образом. Переменная x «расширяется» до блока x_t длиной 48 битов с помощью определенной в стандарте DES следующей таблицы:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

После такого «расширения» блок x, побитно складывается по модулю 2 с блоком y. Результирующий блок B, состоящий из 48 битов, делится на 8 шестибитовых блоков $B=B_1B_2B_3B_4B_5B_6B_7B_8$. В свою очередь, каждый из этих восьми блоков преобразуется в четырехбитовые блоки $A_1A_2A_3A_4A_5A_6A_7A_8$ с помощью специальных нелинейных преобразований S,,..., S_8. Каждое S-преобразование задается определенной в алгоритме DES таблицей, состоящей из 4 строк и 16 столбцов. Элементами таблицы являются целые десятичные числа, принимающие значения от 0 до 15.

Рассмотрим таблицу для преобразования S_7. В соответствии с DES таблица имеет следующий вид:

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Строки таблицы пронумерованы сверху вниз от 0 до 3, а столбцы — слева направо от 1 до 16.

Тогда преобразование S_7, отображающее B_7 (последовательность из 6 битов $Z_1, Z_2, Z_3, Z_4, Z_5, Z_6$) в Ау, строится следующим образом. Определяются два числа $0 \le S_T \le 3$ и $1 \le C_L \le 16$, двоичные представления которых соответственно равны $S_T=(Z,Z_6)$, $C_L=(Z_2Z_3Z_4Z_5)$. Далее из таблицы выбирается элемент, расположенный на пересечении строки S_T и столбца C_L. Вспомним, что элементами таблицы являются числа от 0 до 15. Поэтому для двоичного представления любого числа таблицы достаточно 4 битов. Двоичное представление выбранного элемента таблицы и есть последовательность A_7.

Завершается определение функции / применением к 32-битному блоку $A_1A_2A_3A_4A_5A_6A_7A_8$ определенной в стандарте DES перестановки.

Алгоритм DES обладает рядом интересных свойств. Первое свойство, касающееся симметрии, почти очевидно и состоит в том, что если в шифруемом блоке и ключе DES все 0 заменить на 1 и наоборот, то в результате шифрования получится блок, который образуется из первоначального криптотекста инверсией 0 и 1. Действительно, в DES используются только операции перестановки, подстановки, сдвиги и сложение по модулю 2, которые не зависят от того, как «называются» цифры 0 и 1.

Второе свойство носит название лавинообразного эффекта и является весьма желательным с точки зрения секретности: незначительное изменение исходного сообщения или ключа приводит к большим изменениям в криптотексте.

DES был впервые опубликован в 1973 г., и с тех пор во всем мире о нем написано такое количество различных статей и разделов в специальных книгах по криптографии, что, казалось бы, он должен быть давно вскрыт. Однако в течение долгого времени не происходило не только взлома этого шифра, но, по существу, даже снижения оценок его криптографической стойкости.

Сегодня известны два метода вскрытия DES. Первый метод состоит в полном переборе всех возможных вариантов ключа и их проверки на правильность расшифрования до получения истинного значения. В случае DES необходимо перебрать 2^{56} (или примерно $7{,}2 \times 10^{16}$) возможных вариантов ключа.

Конечно, прогресс вычислительной техники за последние годы был настолько большим, что перебор всех возможных вариантов ключа DES уже не кажется сейчас столь же невероятной задачей, какой он представлялся еще в 1993 г. Известны две успешные атаки на алгоритм DES, совершенные в 1999 г. с привлечением компьютеров, подключенных к Интернету (open project). В первом случае ключ был скомпромети-

рован примерно за 3 месяца, и для его поиска было проанализировано 85 % всех возможных значений ключа. Во втором случае ключ был вскрыт за 6 недель, и для этого потребовалось перебрать около 25 % всех значений ключа. Кроме того, известен случай, когда компьютер, построенный за деньги организации Electronic Privacy Information Center и состоящий из 1728 процессоров, обеспечивающих перебор 88 млрд вариантов ключа в секунду, вскрыл DES за 56 часов работы.

В результате сегодня алгоритм DES уже не считается надежным, и в качестве наиболее простой альтернативы ему предлагается алгоритм Triple DES (другое обозначение — 3DES), использующий ключ длиной 112 битов.

Другой метод вскрытия DES называется дифференциальным криптоанализом. Он позволяет уменьшить число проверяемых ключей, но требует наличия криптотекстов для 2^{47} выбранных значений шифруемых блоков. Трудно представить ситуацию, когда дифференциальный криптоанализ мог бы использоваться на практике. Поэтому этот метод имеет больше теоретическое, чем прикладное значение.

Важным достоинством DES является его высокая производительность. Так, DES быстрее алгоритма RSA (см. далее) той же криптостойкости, что и DES (для этого длина ключа в RSA должна быть равна 384 бита), в 100 раз, если используется программная реализация обоих криптоалгоритмов, и в 1000—10 000 раз, если применяется реализация алгоритмов в специализированных вычислительных устройствах, называемых Hardware Security Module.

Даже программная реализация DES на 486 PC позволяет шифровать данные со скоростью 400 Кбит/с.

Экспорт программного обеспечения, использующего DES, до последнего времени контролировался Агентством национальной безопасности США. В результате в экспортируемом программном обеспечении использовался DES с ограниченной длиной ключа, равной 40 бит.

Как уже отмечалось, в 1998 г. Национальный институт стандартов и технологий отказался сертифицировать DES в качестве стандарта Правительства США.

После нескольких лет обсуждений американский Национальный институт стандартов и технологий 2 октября 2000 г. утвердил вместо DES новый стандарт блочного симметричного алгоритма шифрования AES (Advanced Encryption Standard).

Новый стандарт имеет очень хорошие шансы стать международным, если не де-юре, то, по крайней мере, де-факто. Во-первых, он был при-

нят на основе открытого конкурса, в котором участвовали алгоритмы, предложенные математиками из многих стран (США, Канады, Австралии, Бельгии, Германии, Норвегии, Франции, Южной Кореи, Японии и даже Коста-Рики). Во-вторых, победителем стал алгоритм Rijndael, разработанный бельгийскими криптографами Винсентом Рэменом и Ионом Даменом. Название этого алгоритма образовано из первых букв фамилий его авторов, поэтому в транскрипции с фламандского оно произносится примерно как «рэндал». Бельгийское, а не американское происхождение Rijndael наверняка поможет AES получить признание в Европе, долгое время с подозрением относившейся к DES.

Алгоритм Rijndael был подвергнут скрупулезному анализу не только специалистами Национального института стандартов и технологий и Агентства национальной безопасности США, но и их конкурентами, среди которых были самые блестящие криптографы и криптоаналитики мира. Однако никому не удалось выявить уязвимые места этого алгоритма.

Rijndael может работать с ключами длиной 128, 192 и 256 битов, и поэтому в обозримом будущем он защищен от атак методом полного перебора всех возможных ключей. Кроме того, алгоритм сочетает в себе высокое быстродействие и умеренные требования к памяти. Поэтому он может быть реализован в самых различных устройствах, включая SIM мобильного телефона и смарт-карты. И наконец, Rijndael не защищен патентами и доступен для свободного использования в любых продуктах.

Большое распространение в последние годы получил симметричный алгоритм Triple DES. Этот алгоритм использует ключ, состоящий из двух ключей DES, и состоит из трех шагов. На первом шаге с помощью первого ключа и алгоритма DES 64-битный блок шифруется. На втором шаге с помощью второго ключа и в соответствии с алгоритмом DES полученный на первом шаге криптотекст дешифруется. На последнем, третьем шаге результат дешифрования, полученный на втором шаге, вновь шифруется с помощью первого ключа и алгоритма DES. Полученный 64-битный блок является криптотекстом Triple DES. Таким образом, алгоритм Triple DES требует трехкратного использования DES, откуда и происходит его название.

Очевидно, что для вскрытия алгоритма Triple DES методом полного перебора потребуется проверить 2^{112} (или примерно $5{,}2 \times 10^{33}$) различных ключей.

Скорость шифрования алгоритма Triple DES примерно в 3 раза ниже производительности DES и в случае программной реализации алгоритма на компьютере 486 PC составляет около 150 Кбит/с.

Следуя примеру США в разработке открытого национального стандарта шифрования, в 1989 г. государственный стандарт шифрования данных для сетей ЭВМ приняли в СССР. Он получил обозначение ГОСТ 28147-89 и имел гриф «Для служебного пользования» до конца существования самого СССР. В России он был принят официально с 1992 г. как стандарт шифрования данных наряду с другими бывшими стандартами СССР. Стандарт был формально объявлен полностью открытым в мае 1994 г. Стандарт ГОСТ 28147-89 так же, как и DES, является блочным шифром. Длина блока информации составляет также 64 бита. Длина ключа равняется 256 битам, и ни о какой практической возможности перебора всех допустимых вариантов ключа не только сегодня, но и в XXI веке не может быть и речи.

Примерно в это же время (в 1989 г.) был разработан и опубликован альтернативный алгоритму DES проект открытого национального стандарта шифрования данных Японии, получивший обозначение FEAL. Он также является блочным шифром, использует блок данных из 64 битов и ключ длиной 64 бита. Впрочем, ни он, ни какой-либо другой алгоритм так и не принят до настоящего времени в качестве национального стандарта шифрования Японии.

В 1990 г. К. Лэй и Дж. Мэсси (Швейцария) предложили проект международного стандарта шифрования данных, получивший обозначение IDEA (International Data Encryption Algorithm), который в международном криптографическом сообществе оценивается весьма высоко и за последние годы усилиями международных организаций по стандартизации (прежде всего европейских) активно выдвигался на роль официального общеевропейского стандарта шифрования данных. Длина ключа алгоритма IDEA равна 128 битов для шифрования блока длиной 64 бита. Как будет показано далее, алгоритм будет оставаться стойким к взлому на протяжении нескольких ближайших десятилетий.

Алгоритм IDEA использует три группы операций — побитовое сложение по модулю 2, сложение по модулю 2^{16}, умножение по модулю $2^{16}+1$. Операции производятся над блоками длиной 16 битов, получающимися в результате деления шифруемого блока на 4 подблока. Алгоритм является циклическим — используется 8 циклов преобразований.

Сегодня алгоритм IDEA запатентован в США и большинстве европейских стран. Держателем патента является компания Ascom-Tech. Некоммерческое применение стандарта является бесплатным.

Алгоритм IDEA быстрее Triple DES, но медленнее DES. Скорость шифрования алгоритма в случае его программной реализации на компьютере 486 PC составляет около 200 Кбит/с.

Алгоритм Skipjack был разработан Агентством национальной безопасности США для проектов Клиппер-чип (Clipper Chip) и Кэпстоун-чип (Capstone chip). Алгоритм использует ключ длиной 80 битов и использует 32 цикла на каждую операцию шифрования/дешифрования.

Проект Клиппер-чип был объявлен администрацией президента США в 1994 г. и должен был положить начало внедрению в США «Стандарта шифрования с депонированием ключа». Главный замысел проекта состоял в том, чтобы по решению суда предоставить правоохранительным органам беспрепятственный доступ к шифруемой с помощью Клиппер-чипа информации. Для этого в чипе используется алгоритм Skipjack с двумя ключами. Знание одного из ключей (мастер-ключа) достаточно для того, чтобы было возможно дешифровать любое сообщение, зашифрованное с помощью Клиппер-чипа. При изготовлении микросхемы этот мастер-ключ разделялся на две половины, подлежащих хранению в государственных организациях. Если правоохранительные органы получают необходимую санкцию в суде, они могут получить обе половины ключа и читать любую информацию, шифруемую с помощью соответствующей микросхемы. Сегодня можно утверждать, что идея проекта Клиппер-чипа провалилась. В то же время, известно, что Агентство национальной безопасности использует алгоритм Skipjack для шифрования собственных сообщений. Это подтверждает высокий уровень криптостойкости этого алгоритма.

Алгоритмы RC2 и RC4 — шифры с переменной длиной ключа для очень быстрого шифрования больших объемов информации (были разработаны Роном Райвестом). Эти два алгоритма быстрее, чем DES, и способны повышать степень защиты за счет выбора более длинного ключа. RC2 — блочный алгоритм, и его можно применять как альтернативу DES. RC4 представляет собой потоковый шифр и работает почти в десять раз быстрее DES.

Результаты сравнительного анализа рассмотренных алгоритмов приведены в табл. 3.1.

Таблица 3.1. Результаты сравнительного анализа симметричных алгоритмов шифрования

Алгоритм	Криптостойкость	Производительность (для 486 PC, Кбит/с)	Длина ключа (бит)
DES	Низкая	400	56
3DES	Хорошая	150	112
IDEA	Хорошая	200	128
3IDEA	Очень хорошая	~100	256

Таблица 3.1.

Алгоритм	Криптостойкость	Производительность (для 486 PC, Кбит/с)	Длина ключа (бит)
Skipjack	Хорошая	~400	80
CLIPPER chip	Хорошая	—	80

Краткий обзор асимметричных алгоритмов шифрования

Большинство современных асимметричных алгоритмов базируется на сложности решения следующих математических задач:

- Задача факторизации (разложения на множители) большого числа: умножение двух больших чисел является полиномиальной от размеров сомножителей по сложности задачей. При этом обратная задача — разложения на сомножители — является чрезвычайно трудоемкой, так, для разложения на множители числа длиной 200 цифр требуется не менее 10^{24} арифметических операций, что с вычислительной точки зрения является нереализуемой задачей. На сложности решения задачи факторизации основан алгоритм RSA.
- Задача нахождения дискретного логарифма. С точки зрения вычислительной сложности достаточно легко выполнить операцию возведения в степень в конечном поле, но для решения обратной задачи — поиска дискретного логарифма — потребуется практически полный перебор элементов поля; на сложности решения задачи логарифмирования основаны алгоритмы DSA, EGSA, Diffie-Hellman.
- Сложность декодирования в некоторых кодах, исправляющих ошибки, велика: достаточно легко получить кодовое слово (перемножить матрицы), но по кодовому слову найти базовое — задача вычислительно трудная. Этот метод редко используется на практике (известна криптосистема McEHece, использующая коды Гоппа).

Первой и наиболее известной в мире системой цифровой подписи стала система RSA, математическая схема которой была разработана в 1977 г. в Массачусетском технологическом институте (США) и запатентована в США в 1982 г. Она называется так по первым буквам фамилий авторов: R. Rivest, A. Shamir, L. Adleman.

В самых общих чертах система RSA состоит в следующем. Пусть p и q — два различных больших случайно выбранных простых числа (имеющих обычно не менее 100 разрядов в своем десятичном представлении).

Обозначим

$$n=p*q,\ \varphi(n)=(p-1)*(q-1).$$

Случайно выберем большое целое d, взаимно простое с ф(п), и определим 1<e<ф(п), удовлетворяющее сравнению:

$$e*d \equiv 1 \pmod{\varphi(n)}.$$

Число е определяется с помощью алгоритма Евклида для нахождения наибольшего общего делителя двух целых чисел. Можно показать, что для нахождения е потребуется не более 2xlog ф(п) арифметических операций (здесь log означает логарифм по основанию 2).

Числа n, e и d называются, соответственно, модулем, экспонентой зашифрования и экспонентой расшифрования. Числа п и е образуют открытый ключ, тогда как оставшиеся числа p, q, ф(п) и d являются секретными. На практике следует оставить в качестве секретного ключа только экспоненту расшифрования d, а числа p, q, ф(п) могут быть уничтожены.

Процедура шифрования в схеме RSA определяется равенством

$$D(Y)=Y^e \pmod{n}=Z,$$

а процедура расшифрования — равенством

$$E(Z)=Z^d \pmod{n}=Y.$$

$Y^{(e*d)}=Y^{(C*\varphi(n)+1)}$

Докажем, что E(D(Y))=Y. Поскольку $e*d=C*\varphi(n)+1$, при некотором В соответствии с хорошо известной в теории чисел теоремой Эйлера $Y^{(C*\varphi(n)+1)} \equiv Y \pmod{n}$, что и доказывает равенство E(D(Y))=Y.

Для определения двух больших простых чисел p и q произвольно выбирается нечетное *целое* число r подходящего размера (скажем, 100-разрядное) и проверяется на простоту с помощью тестов Соловея-Штрассена. В случае если r не проходит тест на простоту, процедуре проверки подвергается число r+2 и т. д.

По теореме Чебышева о функции распределения числа простых чисел существует примерно $(10^{100})/\ln(10^{100})-(10^{99})/\ln(10^{99})$ 100-разрядных простых чисел (здесь In означает натуральный логарифм). Если это

число сравнить с числом $(10^{100}-100^{99})/2$ всех 100-разрядных нечетных чисел, видно, что вероятность успеха для конкретного теста приблизительно равна 0,00868.

Как следует из определения схемы RSA, секретное и обратное преобразования являются коммутативными, что означает, что алгоритм RSA может использоваться для шифрования информации. Это свойство является чрезвычайно важным и широко используемым на практике.

Операцией, необходимой для зашифрования и расшифрования, является возведение в степень $a^r \pmod n$. Для ее реализации на практике используется метод последовательного возведения в квадрат (a^2, a^4, a^8,...). Если $k=[\log_2 r]+1$, то можно показать, что для получения $a^r \pmod n$ методом последовательного возведения в квадрат потребуется не более $2*k+1$ произведений.

Обычно на практике экспонента расшифрования выбирается небольшой по размеру (иногда экспонента расшифрования одна и та же для целых групп пользователей). Это делает процедуру шифрования быстрее процедуры расшифрования, а процедуру верификации подписи быстрее процедуры подписывания. Алгоритмически процедуры с открытым ключом требуют $O(K^2)$ операций, с закрытым ключом — $O(K^3)$ операций, а процедура генерации ключей — $O(K^4)$ операций, где K — число битов в двоичном представлении модуля n.

Известны аппаратно-программные реализации алгоритма RSA, имеющие производительность более 600 Кбит/с при n=512 бит.

Существуют два подхода к вскрытию алгоритма RSA. Первый состоит в попытке разложения n на простые множители (задача факторизации). Старейший и самый медленный метод разложения, решето Эратосфена, гарантирует решение задачи за $n^{0,5}$ проверок. Асимптотически самые быстрые алгоритмы факторизации требуют времени работы порядка $O(e^{(1+\varepsilon)\times\sqrt{(\ln n \ln\ln n)}})$ для произвольно малого ε.

Другой метод вскрытия RSA состоит в нахождении e-го корня по модулю n.

Поскольку $c=\tau^e$, то e-й корень c представляет собой сообщение т. К настоящему времени не известно, чтобы этот метод сводился к задаче факторизации, так же так неизвестен способ вскрытия RSA, базирующийся на его использовании.

Сегодня криптосистемы RSA с модулем 384 бита считаются легко вскрываемыми, с модулем 512 битов — вскрываемыми правительственными службами, 784 бита — достаточно надежными, 1024 бита — надежными на ближайшие десятилетия.

В последние годы специалистам по компьютерной теории чисел с помощью весьма изощренных методов и мощных вычислительных систем (использовались самые быстрые суперкомпьютеры типа CRAY-3 или распределенные сети из нескольких сотен VAX-станций) удается иногда разлагать на множители целые числа из 150 десятичных знаков.

Алгоритм RSA де-факто является международным стандартом ЭЦП. Однако при рассмотрении вопроса о возможности практического использования метода RSA существуют следующие аргументы против:

- метод RSA защищен патентом США, и для его использования в коммерческих продуктах необходимо лицензионное соглашение с держателем патента — корпорацией RSA Data Security (США);
- для обеспечения стойкости подписи на уровне 10^{18} необходимо использовать целые числа длиной не менее 360 битов (или 108 десятичных знаков) каждое, что требует достаточно больших вычислительных затрат;
- при вычислении ключей в системе RSA необходимо проверять большое количество условий, невыполнение каждого из которых допускает возможность фальсификации подписи;

а метод RSA позволяет без знания секретных ключей легко получать подписи под определенными новыми документами.

Другой распространенный асимметричный алгоритм шифрования EGSA был разработан в 1984 г. американцем Т. Эль-Гамалем. Этот алгоритм не защищен патентом, что стало одним из доводов, использованных в августе 1991 г. Национальным институтом стандартов и технологий США для обоснования выбора алгоритма EGSA в качестве основы для национального стандарта DSA (Digital Signature Algorithm) перед комиссией Конгресса США.

Протокол подписи EGSA строится следующим образом. Рассматривается конечное поле GF(p), где p — большое простое число. Секретным ключом создания подписи служит целое число x, $0<x<q$. Открытым ключом проверки подписи — порядок поля p, образующая a подгруппы простого порядка q мультипликативной группы поля GF(p) и экспонента $b \equiv a^x \pmod p$

Для создания подписи сообщения m, $0<m<q$, выполняются следующие действия:

1. Генерируется случайное число k, $0<k<q$.
2. Находится r, $0<r<p$, такое, что $r \equiv a^k \pmod p$
3. Находится число s, являющееся решением сравнения $m \equiv xr+sk \pmod q$

Подписью для сообщения m является пара (r, s).

Для проверки подписи выполняются следующие действия:

1. Проверяется неравенство r<p. Если оно не выполняется, подпись неверна.
2. Проверяется сравнение $a^m \equiv b^r r^s (\mathrm{mod}\ p)$. Если сравнение выполняется, то подпись подлинная, в противном случае — нет.

Необходимость и достаточность выполнения последнего сравнения очевидна. Действительно, $(b^r)(r^s)=a^{(xr+ks)}=a^{(cq+m)}$ при некотором целом неотрицательном c. Поскольку a — образующая подгруппы простого порядка q мультипликативной группы, $a^q \equiv 1(\mathrm{mod}\ p)$ и потому выполняется $a^m \equiv b^r r^s (\mathrm{mod}\ p)$

По сравнению с методом RSA алгоритм EGSA имеет целый ряд преимуществ:

- во-первых, при заданном уровне стойкости алгоритма цифровой подписи целые числа, с которыми приходится проводить вычисления, короче, что, соответственно, уменьшает сложность вычислений и позволяет заметно сократить объем используемой памяти;
- во-вторых, при выборе параметров достаточно проверить всего два простых условия;
- в-третьих, процедура шифрования по этому методу не позволяет вычислять (как в RSA) цифровые подписи под новыми сообщениями без знания секретного ключа.

Однако при всех перечисленных выше преимуществах алгоритм EGSA имеет и некоторые недостатки. В частности, при том же уровне стойкости длина подписи и время ее проверки оказываются больше, чем в RSA. Кроме того, повторение одного и того же случайного числа k в течение срока действия ключа x приводит к его раскрытию. Для этого достаточно решить систему из двух линейных уравнений.

Схема цифровой подписи К. Шнорра напоминает алгоритм EGSA. Рассматривается конечное поле GF(p), где p — большое простое число. Секретным ключом создания подписи служит целое число x, 0<x<q.

Открытым ключом проверки подписи служат порядок поля p, образующая a подгруппы простого порядка q мультипликативной группы поля GF(p) и экспонента $b \equiv a^x (\mathrm{mod}\ p)$

Для создания подписи сообщения m выполняются следующие действия:

1. Генерируется случайное число k, 0<k<q.
2. Находится r, 0<r<p, такое, что $r \equiv a^k (\mathrm{mod}\ p)$.

3. Находится e=h(m‖r), где h — хэш-функция, m‖r — конкатенация сообщения m и r.
4. Находится число s, 0<s<q, такое, что выполняется сравнение $s \equiv k - xe \pmod q$.

Подписью для сообщения m является пара (e,s).

Для проверки подписи выполняются следующие действия:

1. Вычисляется r,, 0<r, <p, такое, что выполняется сравнение $r_1 \equiv a^s b^e \pmod p$.
2. Находится $e_1 = h(m \| r_1)$
3. Проверяется равенство e=e,. Если оно выполняется, то подпись подлинная, в противном случае — нет.

Необходимость и достаточность с точностью до коллизий, связанных с хэш-функцией последнего равенства очевидна. Действительно, $0 < r_1 < p$, $r_1 \equiv a^{(s+xe)} \pmod p$. Поскольку, как следует из схемы Шнорра, выполняются равенства

$$s + xe = Aq + b,$$

$$k = Bq + b$$

при некоторых целых A,B, b, то $r_1 = a^k \pmod p$. Отсюда следует условие проверки подписи.

Как и в схеме Эль-Гамаля, повторение одного и того же случайного числа k в течение срока действия ключа x приводит к его раскрытию.

Обзор не был бы полным без упоминания о первом асимметричном алгоритме шифрования — алгоритме Diffie-Hellman. Алгоритм Diffie-Hellman сегодня активно применяется для решения задачи организации обмена ключами в системах со многими пользователями.

Суть алгоритма состоит в следующем. Все операции производятся в некотором конечном поле GF(q) с примитивным элементом g. Порядок поля q представляет собой большое число (в алгебре доказывается, что порядок любого конечного поля представляет собой степень некоторого простого числа; на практике в качестве q используется простое число). Теперь рассмотрим двух участников криптосистемы — A и B. Каждый из них генерирует для себя секретное число (соответственно, a и b), которое хранится в секрете. Кроме того, каждый участник системы вычисляет в поле GF(q) величину g^a и g^b, соответственно. Вычисленные экспоненты являются публичными открытыми ключами, известными всем участникам криптосистемы.

Тогда, если A хочет организовать защищенное соединение с B, A генерирует сессионный ключ для некоторого симметричного алгоритма

шифрования следующим образом: А берет публичный ключ стороны В — g^b — и возводит его в степень своего секретного ключа a. В результате получается ключ $g^{(a*b)}$. Очевидно, что этот же ключ может быть получен и стороной В на основании знания собственного секретного ключа b и открытого ключа А — g^a.

Вскрытие алгоритма Diffie-Hellman близко к решению задачи нахождения логарифма в дискретном конечном поле, являющейся NP-полной задачей.

Криптостойкость алгоритма существенно зависит от выбора порядка поля, его примитивного элемента, а также размера секретных экспонент.

В последнее время большое внимание уделяется алгоритмам ECC (Elliptic Curve Cryptography), основанным на применении конструкций, называемых эллиптическими кривыми. В основе этих алгоритмов лежит тот факт, что для уравнения $a \times x = b$ относительно x при известных a и b и при условии, что a, b, x принадлежат эллиптической кривой E, не известно другого алгоритма решения, кроме перебора всех возможных значений x. Более того, в силу сложности самой конструкции эллиптических кривых даже такой простой способ ее решения, как полный перебор, трудно оценить с вычислительной точки зрения. Поэтому оценки надежности систем цифровой подписи ECC до последнего времени считались специалистами существенно менее обоснованными, чем аналогичные оценки для задачи разложения на множители и дискретного логарифмирования. Лишь за последние 4-5 лет доверие аналитиков к конструкциям эллиптических кривых существенно возросло.

По современным оценкам сложности при уровне надежности алгоритмов ECC, соответствующим криптостойкости алгоритмов, основанным на задаче дискретного логарифмирования с длиной ключа 512 битов, можно ограничиться эллиптической кривой, точки которой описываются парами целых чисел, каждое из которых имеет длину 160 битов. Это позволяет сократить общую длину записи секретного ключа с 512 битов до 320, что, в свою очередь, уменьшает сложность вычислений (а значит, и время) в 2,4 раза. При этом в случае ECC сложность верификации ЭЦП в 36-480 раз больше, чем при использовании RSA.

Таким образом, эллиптические алгоритмы представляют особый интерес для приложений, связанных с микропроцессорными картами и ЭК, когда необходимо разгрузить процессоры карты и компьютера пользователя при операциях подписывания, а также использовать меньше памяти для хранения ключа (актуально только для карты).

В России приняты стандарты: ГОСТ Р 34.10-94 «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного

криптографического алгоритма» и ГОСТ Р 34.11-94 «Функция хэширования». В основу российского стандарта положены схемы Эль-Гамаля и Шнорра.

Завершим обзор асимметричных алгоритмов шифрования перечнем наиболее часто используемых алгоритмов формирования дайджестов (хэш-кодов) сообщений.

MD2, MD4 и MD5 — алгоритмы дайджеста, разработанные Роном Райвестом. Каждый из них вырабатывает 128-битный хэш-код. Алгоритм MD2 — самый медленный, MD4 — самый быстрый. Алгоритм MD5 можно считать модификацией MD4, в котором скоростью пожертвовали ради увеличения надежности.

SHA-1 (Secure Hash Algorithm) — это алгоритм вычисления дайджеста сообщения, вырабатывающий хэш-код длиной 160 битов. Алгоритм SHA одобрен правительством США (как часть проекта Capstone). Он надежнее алгоритмов MDx, так как вырабатывает более длинный хэш-код, что снижает вероятность того, что разные входные последовательности будут преобразованы в одно значение хэш-кода.

В российском стандарте ГОСТ Р 34.11-94 длина дайджеста определена равной 256 битам.

Методы оценки криптостойкости

Остановимся теперь на оценке криптостойкости сегодняшних криптографических алгоритмов. Начнем с описания модели вскрытия секретного ключа.

Закон Мура, в соответствии с которым вычислительная производительность микропроцессоров увеличивается в 2 раза каждые 18 месяцев или, что то же самое, в 100 раз каждые 10 лет. Сегодня типовой компьютер (Pentium based PC), подключенный к Интернету, имеет производительность около 100 MIPS (под 1 MIPS понимается производительность старого компьютера DEC VAX 11/780). Следовательно, средняя производительность PC в 2010 г. будет составлять 10 000 MIPS.

Оценки общего количества компьютеров в мире показывают, что сегодня их число составляет 100 миллионов. Число компьютеров за 10 лет увеличивается в 10 раз. Другими словами, в 2010 г. число компьютеров станет равно 1 миллиарду. По оценкам специалистов, 0,3 % всех компьютеров, подключенных к Интернету, могут быть вовлечены в криптоатаку (такие атаки относятся к классу Open Project и больше рассчитаны на общественное мнение, чем действительно направлены

на компрометацию секретного ключа). Предполагается, что в будущем доля компьютеров, которые могут быть вовлечены в криптоатаку, составит 0,1 %.

Кроме атак, относящихся к классу Open Project, существуют атаки, принадлежащие классу Covert Project, суть которых состоит в том, что используются недоиспользованные циклы корпоративных вычислительных систем. Например, вычислительная мощность системы только одной компании Sun Microsystems составляет 100 000 MIPS. Таким образом, уже в 2010 г. вычислительная мощность, доступная для атаки класса Covert Attack, будет составлять 100 млн MIPS.

Предполагается, что разумная оценка для времени, затрачиваемого на криптоатаку, — 1 год.

В таблице приведены доступные вычислительные мощности, выраженные в MY (1MY=MIPS*1 год).

Таблица 3.2. Сравнительные оценки доступной вычислительной мощности

Год	Covert Attack	Open Project
2000	10^5	10^7
2010	10^8	10^{10}
2020	10^{11}	10^{13}

Из этой модели, в частности, следует, что сегодня надежными могут считаться симметричные алгоритмы с длиной ключа не менее 80 битов. На вскрытие алгоритма DES, о котором говорилось выше, было потрачено 0,5 MY, что находится в хорошем соответствии с данными приведенной таблицы.

Другой подход к оценке криптостойкости сегодняшних алгоритмов шифрования приведен в книге Брюса Шнайера «Applied Cryptography». В книге приведены данные по затратам на создание компьютера (цены 1995 г.), необходимого для взлома симметричного алгоритма с различной длиной ключа. Некоторые из этих данных приведены в таблице 3.3.

Таблица 3.3. Затраты на взлом симметричного алгоритма в зависимости от длины ключа

Стоимость в тыс. $	40 битов	56 битов	64 бита	80 битов	128 битов
100	2 сек	35 час	1 год	70000 лет	10^{19} лет
1000	0,2 сек	3,5 час	37 дней	7000 лет	10^{18} лет
100 000	2 мс	2 мин	9 час	70 лет	10^{16} лет

Таблица 3.3. *(продолжение)*

Стоимость в тыс.$	40 битов	56 битов	64 бита	80 битов	128 битов
1 000 000	0,2 мс	13 сек	1 час	7 лет	10^{15} лет
100 000 000	2 мкс	0,1 сек	32 сек	24 дня	10^{13} лет

Наконец, представляет несомненный интерес соответствие длин ключей симметричного алгоритма шифрования и алгоритма RSA при одинаковой криптостойкости алгоритмов (табл. 3.4).

Таблица 3.4. Сравнение длин ключей симметричного алгоритма и RSA

Длина секретного ключа (симметричный алгоритм), бит	Длина открытого ключа (RSA), бит
56	384
64	512
80	768
112	1792
128	2304

Тот факт, что вычислительная мощность, которая может быть привлечена к криптографической атаке, за 10 лет выросла в 1000 раз, означает необходимость увеличения за тот же промежуток времени минимального размера симметричного ключа и асимметричного ключа, соответственно, примерно на 10 и 20 битов.

Системы управления ключами

С появлением большого числа криптосистем, основанных на использовании принятых в мире стандартов шифрования, встала новая не менее важная проблема, связанная с тем, что для обмена зашифрованными сообщениями между двумя участниками криптосистемы необходимо, чтобы обоим участникам обмена были заранее доставлены тщательно сохраняемые в секрете ключи для зашифрования и расшифрования сообщений.

Эта проблема становится тем более сложной, чем больше удаленных друг от друга пользователей желают обмениваться между собою зашифрованными сообщениями. Так, для сети из N пользователей необходимо иметь одновременно в действии $N \times (N-1)/2$ различных ключей. Тогда уже при N=1000 количество необходимых ключей будет близко

к полумиллиону. Поскольку из соображений безопасности секретные ключи для шифрования должны меняться как можно чаще, то изготовление, упаковка и рассылка их с надежными курьерами из некоего абсолютно надежного центра (как это привычно делают в действующих системах «закрытой связи») становится задачей совершенно нереальной.

Решение проблемы было предложено в виде технологии открытого распределения ключей (Public Key Infrastructure). Суть этой технологии состоит в том, что пользователи самостоятельно и независимо с помощью датчиков случайных чисел генерируют свои индивидуальные ключи, которые хранят в секрете от всех на своем индивидуальном носителе: дискете, специальной магнитной или процессорной карточке, таблетке энергонезависимой памяти Touch Memory (фирмы Dallas Semiconductor) и т. п. Затем каждый пользователь из своего индивидуального ключа вычисляет с помощью известной процедуры свой так называемый «открытый ключ», то есть блок информации, который он делает общедоступным для всех, с кем хотел бы обмениваться конфиденциальными сообщениями.

Открытыми ключами пользователи могут обмениваться между собой непосредственно перед передачей зашифрованных сообщений. Другая, более простая с организационной точки зрения альтернатива — поручить третьей стороне сбор всех открытых ключей пользователей в единый каталог. Администратор каталога должен заверить открытые ключи пользователей своей подписью и разослать этот каталог всем остальным участникам обмена. Сегодня службы администрирования открытых ключей принято называть центрами сертификации (ЦС).

В качестве стандарта для единого каталога ключей может использоваться протокол X.500.

Открытые ключи, заверенные ЦС, называют сертификатами. Сертификат открытого ключа — это объект, связывающий пользователя с его ключом. Сертификат используется при проверке цифровой подписи.

Обычно сертификаты хранятся как объекты службы каталогов или на специально выделенных для этого серверах. В случае компрометации ключа или изменения данных самого сертификата сертификаты должны отзываться. Для этого их заносят в список отозванных сертификатов (Certificate Revocation List, CRL), поддерживаемый ЦС.

X.509 — это стандарт, описывающий формат и синтаксис сертификатов. Различные протоколы, использующие защиту данных и аутентификацию, например SET, SSL, S-HTTP и другие, применяют сертификаты X.509. Первая версия стандарта X.509 была опубликована в 1988 г. Текущая версия — третья.

Главная задача сертификата — установить соответствие между пользователем и его открытым ключом. В состав полей сертификата стандарта X.509, в частности, входят:

- номер версии стандарта X.509;
- номер сертификата;
- идентификатор алгоритма ЭЦП;
- идентификатор сертификационной службы, выдавшей сертификат;
- идентификатор владельца сертификата;
- срок действия сертификата;
- сертифицируемый открытый ключ.

Наибольшее распространение в мире технология открытого распределения ключей для шифрования конфиденциальных сообщений получила в корпоративных телекоммуникационных сетях и общедоступных сетях обмена электронными данными, прежде всего, в сети Интернет. Американский программист Филипп Циммерман (Zimmerman) даже написал общедоступный пакет программ для обмена сообщениями по электронной почте, получивший название PGP (Pretty Good Privacy). Основная идея Циммермана состояла в создании качественной, надежной программы шифрования для электронной почты, базирующейся на использовании наиболее сильных криптоалгоритмов, опубликованных в то время (на рубеже 80-90-х годов) в открытой литературе. Пакет PGP в первых его версиях вместе с исходными текстами программ был распространен в 1991 г. по сетям электронной почты практически во всем мире и был использован многими программистами в разработках средств защиты информации как неплохой, а главное, бесплатный материал.

Пакет PGP удачно совместил в себе возможности шифрования сообщений симметричными блочными алгоритмами, распределения симметричных ключей с помощью асимметричного алгоритма шифрования RSA, а также создания электронных подписей сообщений.

Предполагая возможное вмешательство правительства США в процесс развития подобных технологий в будущем, Циммерман вместе с программой версии 1.0 распространял и исходные тексты программы, положив начало традиции, поддерживаемой вплоть до настоящего времени. Это быстро привело к тому, что за улучшение программы взялись многочисленные добровольцы, и через несколько лет, по признанию самого Циммермана, в пакете PGP практически не осталось строк кода, написанных им самим.

Поскольку вплоть до последнего времени (до 17 декабря 1999 г.) по американским законам криптографическое программное обеспечение не разрешалось экспортировать без разрешения госдепартамента, а к 1993 г. пакет уже был распространен по всей планете, правительство США определило, что имело место нарушение закона. Было начато расследование, и только благодаря действиям группы юридической защиты программиста, созданной правозащитным движением, а также компании, развернутой в прессе в его поддержку, следствие по делу PGP было закрыто.

После этого Циммерман основал собственную компанию PGP для коммерческой раскрутки ставшего столь популярным продукта. К лету 1997 г. был готов самостоятельный продукт PGP Personal Privacy 5.0. В этой версии программа приобрела графический интерфейс и могла работать в операционных средах систем DOS, UNIX, Windows 95, Windows NT и Apple Macintosh.

В декабре 1997 г. компания была куплена Network Associates. Изменила свой статус и программа. Начиная с шестой версии, появившейся в сентябре 1998 г., PGP в качестве клиента входит в состав большого криптографического пакета PGP Enterprise Security, разработанного специально для защиты корпораций. При этом компания Network Associates сохранила распространяемую бесплатно версию PGPfreeware, хотя и лишенную множества дополнительных функций, но по-прежнему свободно доступную в Интернете.

Помимо протокола PGP существуют и другие системы управления ключами. Достаточно популярным является протокол Kerberos, разработанный в Массачусетском технологическом институте. Протокол реализует несколько функций. Одна из них — хранение личных ключей в защищенной БД. Ключ известен только Kerberos и его владельцу. Еще одна функция — доверенный посредник между двумя абонентами, желающими обменяться секретными ключами. Kerberos также предоставляет услуги аутентификации и рассылки ключей.

Известен также протокол SKIP (Simple Key Management for Internet Protocols). Это протокол управления ключами, разработанный компанией SUN Microsystems. SKIP легко реализуется. В нем описан способ вычисления ключа на основе сертификатов открытых ключей. Однако использование SKIP налагает определенные ограничения на выбор алгоритмов шифрования и хэширования. Протокол SKIP заявлен как необязательный компонент спецификации IPSec (Internet Protocol Security).

Кроме перечисленных протоколов для управления ключами используются алгоритмы Diffie-Hellman и KEA (Key Exchange Algorithm).

Протоколы и методы защиты информации в Интернете

На основе перечисленных выше симметричных и асимметричных криптоалгоритмов строятся различные протоколы защиты информации в Интернете.

Самый известный протокол Интернета — SSL (Secure Socket Layer). Этот протокол был разработан компанией Netscape и является составной частью всех известных Интернет-браузеров и Web-серверов (сегодня используется версия 3.0 протокола SSL). Протокол реализуется между транспортным и сеансовым уровнями Эталонной модели взаимодействия открытых систем (ЭМВОС). Это, с одной стороны, означает возможность использования протокола для организации защищенной сессии между программами, работающими по различным протоколам прикладного уровня ЭМВОС (FTP, SMTP, Telnet, HTTP и т. п.), а с другой — закрытие любых данных, передаваемых в SSL-сессии, что приводит к снижению производительности протокола.

Последняя версия протокола SSL поддерживает три режима аутентификации:

- взаимную аутентификацию сторон;
- одностороннюю аутентификацию сервера (без аутентификации клиента);
- полную анонимность.

Очевидно, что последний вариант представляет собой экзотический случай, так как взаимодействующие стороны оказываются незащищенными от возможных атак, связанных с подменой участников, хотя при этом и обеспечивается защита от несанкционированного доступа самого установленного соединения.

В упрощенном виде процедура установления защищенного режима взаимодействия между клиентом и Web-сервером в соответствии с протоколом SSL выглядит следующим образом (рассматривается вариант односторонней аутентификации сервера со стороны клиента).

Этап установления SSL-сессии (-«рукопожатие»).

1. КЛИЕНТ посылает СЕРВЕРУ запрос (Client hello) на установление защищенного соединения, в котором передает некоторые формальные параметры этого соединения:
   - текущее время и дату;
   - случайную последовательность (RAND_CL) длиной 28 байтов;

- набор поддерживаемых клиентом симметричных криптографических алгоритмов (например, RC4_128, RC440, RC2128, RC2_40, DES40, DES56 и других) и хэш-алгоритмов (MD5, SHA-1), используемых при формировании кода для проверки целостности передаваемого сообщения (MAC — Message Authentication Code);
- набор поддерживаемых алгоритмов сжатия (все реализации протокола SSL должны поддерживать-метод CompressionMethod.null) и других.

Следует отметить, что КЛИЕНТ имеет возможность в запросе указать идентификатор SSL-сессии, которая была установлена ранее или поддерживается в настоящий момент времени. В этом случае процедура согласования параметров для устанавливаемой сессии не требуется (используются параметры, согласованные для сессии с указанным в запросе идентификатором SSL-сессии).

Кроме того, полезно отметить, что инициировать SSL-сессию может и Web-СЕРВЕР. Для этого СЕРВЕР может в любой момент времени направить КЛИЕНТУ сообщение Hello request, которое информирует КЛИЕНТА о том, чтобы он направил СЕРВЕРУ сообщение Client Hello.

2. СЕРВЕР обрабатывает запрос от КЛИЕНТА и в ответном сообщении (Server hello) передает ему следующий согласованный набор параметров:
   - идентификатор SSL-сессии;
   - конкретные криптографические алгоритмы из числа предложенных клиентом (если по какой-либо причине предложенные алгоритмы или их параметры не удовлетворяют требованиям сервера, сессия закрывается);
   - сертификат сервера, заверенный цифровой подписью ЦС (в формате X.509 v.3);
   - случайную последовательность (RAND_SERV);
   - цифровую подпись для перечисленных выше данных.
3. КЛИЕНТ проверяет полученный сертификат СЕРВЕРА с помощью открытого ключа ЦС, который ему известен; при положительном результате проверки КЛИЕНТ выполняет следующие действия (при отрицательном результате проверки сессия закрывается):
   - генерирует случайную 48-байтную последовательность Pre_MasterSecret (часть совместного секрета, известного только СЕРВЕРУ

и КЛИЕНТУ); шифрует ее на открытом ключе сервера, полученном в сертификате сервера, и посылает СЕРВЕРУ;

- с помощью согласованных хэш-алгоритмов формирует главный совместный секрет (MasterSecret), используя в качестве параметров часть совместного секрета Pre_MasterSecret, посланную СЕРВЕРУ на предыдущем шаге случайную последовательность RANDCL и полученную от него случайную последовательность RAND_SERV;
- используя MasterSecret, вычисляет криптографические параметры SSL-сессиии: формирует общие с сервером сеансовые секретные ключи симметричного алгоритма шифрования (для приема и для передачи) и секреты для вычисления MAC;
- переходит в режим защищенного взаимодействия.

4. СЕРВЕР расшифровывает полученный Pre_MasterSecret с помощью своего секретного ключа и выполняет над ним те же операции, что и КЛИЕНТ:
   - с помощью согласованных хэш-алгоритмов формирует главный совместный секрет (MasterSecret), используя в качестве параметров PreMasterSecret посланную КЛИЕНТУ на предыдущем шаге случайную последовательность RANDSERV и полученную от него случайную последовательность RANDCL;
   - используя MasterSecret, вычисляет криптографические параметры SSL-сессиии: формирует общие с клиентом сеансовые секретные ключи одноключевого алгоритма шифрования и секрет для вычисления MAC;
   - переходит в режим защищенного взаимодействия.
5. Поскольку при формировании параметров SSL-сессии КЛИЕНТ и СЕРВЕР пользовались одними и теми же исходными данными (согласованными алгоритмами, общим секретом Pre_MasterSecret и случайными последовательностями RAND_CL и RAND_SERV), то очевидно, что в результате описанных выше действий они выработали одинаковые сеансовые секретные ключи шифрования и секреты, используемые для защиты целостности передаваемых сообщений. Для проверки идентичности параметров SSL-сессии КЛИЕНТ и СЕРВЕР посылают друг другу тестовые сообщения, содержание которых известно каждой из сторон:
   - КЛИЕНТ формирует сообщение из собственных посылок в адрес СЕРВЕРА на этапе 1 (а) и посылок, полученных от СЕРВЕРА

на этапе 1 (б), внося элемент случайности в виде последовательности MasterSecret, уникальной для данной сессии; формирует код для проверки целостности сообщения (MAC), шифрует сообщение на общем сеансовом секретном ключе и отправляет СЕРВЕРУ;

- СЕРВЕР, в свою очередь, формирует сообщение из собственных посылок в адрес СЕРВЕРА на этапе 1 (б), посылок, полученных от КЛИЕНТА на этапе 1 (а), и последовательности MasterSecret; формирует код для проверки целостности сообщения (MAC), шифрует сообщение на общем сеансовом секретном ключе и отправляет КЛИЕНТУ;
- в случае успешной расшифровки и проверки целостности каждой из сторон полученных тестовых сообщений SSL-сессия считается установленной, и стороны переходят в штатный режим защищенного взаимодействия.

Этап защищенного взаимодействия с установленными криптографическими параметрами SSL-сессии.

1. Каждая сторона при передаче сообщения формирует код для последующей проверки целостности сообщения на приемной стороне (MAC) и исходное сообщение вместе с кодом шифрует на своем секретном сеансовом ключе.
2. Каждая сторона при приеме сообщения расшифровывает его и проверяет на целостность (вычисляется MAC и сверяется с кодом проверки целостности, полученным вместе с сообщением); в случае обнаружения нарушения целостности сообщения SSL-сессия закрывается.

Описанная процедура установления SSL-сессии, безусловно, не обладает полнотой изложения, однако дает представление о возможностях протокола SSL.

Как следует из описания протокола SSL, асимметричные алгоритмы шифрования используются только на этапе установления защищенной сессии. Для защиты информационного обмена от несанкционированного доступа используются только симметричные алгоритмы. Это делается в первую очередь для того, чтобы повысить производительность протокола SSL (напомним, что симметричные алгоритмы, как правило, на 3 порядка быстрее асимметричных).

Для защиты трафика в Интернете помимо протокола SSL используется протокол S-HTTP (Secure HTTP). Этот протокол обеспечивает целостность и защиту документов, передаваемых по протоколу HTTP. В отличие от протокола SSL, расположенного между транспортным

уровнем (TCP) и протоколами сеансового уровня, протокол S-HTTP находится на прикладном уровне ЭМВОС, что позволяет с его помощью защищать не транспортное соединение, а данные, передаваемые по соединению. Это повышает производительность протокола защиты информации, но ценой ограничения применимости механизма защиты только приложением HTTP.

Протокол PCT (Private Communication Technology) обеспечивает защиту для клиент-серверных приложений. Функционально PCT похож на SSL Так же как в SSL, при установлении сеанса связи PCT согласует секретный ключ и симметричный алгоритм шифрования. Основное отличие от SSL в том, что PCT отделяет аутентификацию от шифрования. Кроме того, PCT более эффективен, поскольку использует меньшее множество сообщений и они более короткие по сравнению с SSL. PCT поддерживает алгоритмы RSA, Diffie-Hellman, Fortezza для управления ключами; DES, RC2 и RC4 — для шифрования данных; DSA и RSA — для цифровой подписи.

PCT реализован в Microsoft Internet Explorer версии 3 и выше, а также в Microsoft Internet Information Server версии 2 и выше.

В Интернете применяются и другие протоколы защиты информации: S/MIME — для защиты электронной почты, S/WAN — для защиты соединений (как правило, между маршрутизаторами), PGP — для защиты электронной почты, Secure Shell — для защиты сеансов telnet и передачи файлов. На этих протоколах ввиду их специального назначения, не связанного с ЭК, мы останавливаться не будем.

Упомянем лишь протокол IPSec, предназначенный для шифрования данных на сетевом уровне (данный протокол в отличие от всех перечисленных ранее является независимым не только от приложения, но и от транспортного уровня, что, в частности, позволяет применять его для защиты данных приложений, использующих в качестве транспортного протокола UDP). IPSec состоит из трех протоколов: Authentication Header, Encapsulating Secure Payload (ESP) и Internet Key Exchange (IKE). Первый протокол обеспечивает аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений. С помощью протокола AH аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными.

Протокол ESP обеспечивает шифрование потоков данных. Протокол IKE решает задачу распределения ключей на базе протокола Diffie-Hellman. В используемых протоколах в качестве алгоритма шифрования чаще всего используются DES или Triple DES, а в качестве алго-

ритма ЭЦП — RSA. Однако ничто не запрещает использовать в качестве алгоритма шифрования другие методы, краткий обзор которых приведен далее. В этом случае ПО отдельных компонентов ЭК должно поддерживать набор соответствующих алгоритмов шифрования.

Сегодня протокол IPSec находит распространение в основном в двух конфигурациях. Первая конфигурация — протокол сетевого уровня для передачи данных между шлюзами, за которыми располагаются обычные локальные сети, поддерживающие IPv4 для передачи незашифрованных данных из локальной сети.

Вторая конфигурация — закрытие данных внутри самой локальной сети, для чего все рабочие места и сервера сети обязаны поддерживать протокол IPSec. Сегодня большинство современных операционных систем (Windows 2000, OpenBSD, Linux, Solaris) поддерживают протокол IPSec.

Обзор методов защиты данных в Интернете не будет полным, если в нем не упомянуть о технологии межсетевых экранов (Firewall), широко используемой для защиты информации в Интернете. В ЭК межсетевые экраны, в частности, широко применяются для защиты от хакеров таких компонентов электронной коммерции, как Internet Payment Gateway, Server Based Wallet, Payment Server. Подробнее об этих компонентах будет рассказано в главе, посвященной решениям на базе протокола SET.

В основном межсетевые экраны можно разделить на три категории:

- пакетные фильтры (фильтры без памяти);
- фильтры сеансового уровня;
- фильтры прикладного уровня.

Пакетные фильтры блокируют или пропускают пакеты только на основе свойств последних, к числу которых относятся IP-адреса и номера портов отправителя и адресата. Этот тип межсетевого экрана является самым простым в реализации и обслуживании и почти никак не влияет на пропускную способность сети. Однако уровень такой защиты невысок. Так, например, правила фильтрования можно обойти, используя вложение протоколов. Например, если запрещен протокол HTTP, но разрешен Telnet, то для прохождения HTTP-трафика его достаточно вложить в сеанс Telnet.

Другой пример успешного прохождения через пакетный фильтр — address spoofing (имитация адресов). Хакер может использовать в качестве адреса отправителя адрес авторизованного клиента, и тогда пакетный фильтр пропустит пакет хакера.

Фильтр сеансового уровня занимает промежуточное положение между пакетным фильтром и фильтром прикладного уровня. Он сохраняет необходимые данные о предыдущих пакетах и решение о маршрутизации очередного пакета принимает как на основе этих данных, так и на основе содержимого пакета. Естественно, этот тип фильтров более сложный, поскольку помимо проверки самих пакетов необходимо просматривать и обновлять память. В правилах фильтрования можно учитывать как адреса отправителя и получателя, так и тип обслуживания (задается в заголовке IP-пакета).

Фильтр сеансового уровня следит за подтверждением связи (квитированием) между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет примерно следующую процедуру. Когда авторизованный клиент запрашивает некоторую услугу, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации (например, может ли DNS-сервер определить IP-адрес клиента и ассоциированное с ним имя). Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за процедурой квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 1000, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ пакет, помеченный флагом ACK и содержащий число, на единицу большее, чем в принятом пакете (в нашем случае 1001), подтверждая таким образом прием пакета SYN от клиента. После этого осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом (например, 2000), а клиент подтверждает его получение передачей пакета ACK, содержащего число 2001. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня считает запрошенный сеанс допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в пакетах TCP, оказываются логически связанными между собой.

После того как шлюз определил, что авторизованный клиент и внешний хост являются авторизованными клиентами TCP, и проверил допустимость данного сеанса, он устанавливает соединение. Начиная

с этого момента, шлюз просто копирует и перенаправляет пакеты, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, относящиеся к одному из сеансов связи, зафиксированных в этой таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы.

Для копирования и перенаправления пакетов в шлюзах сеансового уровня используются специальные приложения, которые иногда называют канальными посредниками (pipe-proxy). Большинство шлюзов сеансового уровня не являются самостоятельными продуктами и поставляются в комплекте со шлюзами прикладного уровня. Примерами таких шлюзов являются Gauntlet Internet Firewall компании Trusted Information Systems, AltaVista Firewall компании DEC и ANS Interlock компании ANS.

Шлюз сеансового уровня выполняет еще одну важную функцию защиты — трансляцию адресов (Network Address Translation), при которой производится преобразование внутренних IP-адресов в один «надежный» IP-адрес. Этот адрес ассоциируется с фильтром, из которого передаются все исходящие пакеты. В результате в сети со шлюзом сеансового уровня все исходящие пакеты оказываются отправленными из этого шлюза, что исключает прямой контакт между внутренней авторизованной сетью и внешней сетью, а также скрывает от внешних пользователей архитектуру внутренней защищаемой сети. Таким образом, фильтры сеансового уровня защищают внутренние сети от нападений типа address spoofing (имитация адресов).

Наиболее известным стандартом для реализации шлюза сеансового уровня является протокол SOCKS. Версия 5 этого протокола включает в себя процедуры аутентификации взаимодействующих сторон, а также контроль организации сессии в протоколе UDP. Протокол SOCKS 5 поддерживается большинством имеющихся на рынке браузеров, а также поддерживается различными операционными системами, включая Unix, Windows, Mackintosh и другие.

Фильтры прикладного уровня обеспечивают высокую степень защиты, но за счет снижения производительности и увеличения сложности. Такие фильтры реализуются как выделенные межсетевые экраны. Сам сервер приложения находится в частной сети за межсетевым экраном. Внешние клиенты подключаются к последнему, который ведет себя как сервер приложения. Фактически, клиент не может обнаружить, что взаимодействует с межсетевым экраном, который в этом случае называется прикладным прокси-сервером (proxy application server).

С другой стороны, межсетевой экран «притворяется» клиентом и пересылает принятые клиентские запросы настоящему серверу приложений. Но прежде межсетевой экран на основе заданных правил решает вопрос о допустимости такого запроса и наличия у клиента права на запрашиваемые действия. Таким образом, межсетевой экран имеет полное представление об используемых приложениях и протоколах. Единственный недостаток прокси-сервера — снижение общей производительности.

В отличие от фильтра сеансового уровня, посредники прикладного уровня пропускают только пакеты, которые им поручено обслуживать. Например, программа-посредник службы Telnet может копировать, перенаправлять и фильтровать лишь трафик, генерируемый этой службой. Если шлюз прикладного уровня использует только программы-посредники служб FTP и Telnet, то он будет пропускать пакеты этих служб, блокируя при этом пакеты всех остальных служб.

В отличие от шлюзов сеансового уровня, которые копируют и слепо перенаправляют все поступающие пакеты, посредники прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета. Эти посредники могут фильтровать отдельные виды команд или информацию протоколов прикладного уровня, которые им поручено обслуживать.

Такие продукты, как Eagle компании Raptor Systems, ANS Interlock компании ANS, Sidewinder Security Server компании Secure Computing Corporation, Firewall-1 компании Checkpoint, включают в себя программы-посредники прикладного уровня для служб FTP, Telnet, HTTP. Утилиты этих шлюзов позволяют фильтровать определенные команды, используемые этими службами. Например, можно сконфигурировать шлюз таким образом, чтобы он предотвращал использование клиентами команды FTP Put, которая дает возможность пользователю, подключенному к FTP-серверу, записывать на него информацию.

В дополнение к фильтрации многие фильтры прикладного уровня регистрируют все выполняемые сервером действия и, что особенно важно, предупреждают администраторов о возможных нарушениях защиты (Intrusion Detection System). Например, при попытках проникновения в систему извне BorderWare Firewall Server компании Secure Computing позволяет фиксировать адреса отправителя и получателя пакетов, время, в которое эти попытки были предприняты, и используемый протокол. Продукт Black Hole компании Milkyway Networks также фиксирует все попытки проникновения в систему и предупреждает о них администратора, посылая ему сообщения по электронной почте или на пейджер.

Юридические аспекты защиты информации в России

Остановимся теперь на правовых аспектах применения средств защиты информации от несанкционированного доступа в России.

В настоящее время правовая база отношений субъектов в области защиты информации основывается на следующих основных нормативных актах:

- Конституции РФ,
- Гражданском Кодексе РФ,
- Федеральных законах РФ «Об информации, информатизации и защите информации», «О государственной тайне».

Федеральный закон «Об информации, информатизации и защите информации» принят Государственной Думой 25 января 1995 г., подписан Президентом РФ 20 февраля 1995 г. и с тех пор остается единственным на сегодняшний день Федеральным законом, трактующим общие вопросы регулирования отношений в области защиты информации. В сферу его действия включена защита информации, прав субъектов, участвующих в информационных процессах и информатизации (ст. 1, разд. 1).

В статье 5 закона, в частности, говорится о юридической силе электронного документа с цифровой (электронной) подписью:

«Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдения установленного режима их использования».

В статье 21 «Защита информации» говорится следующее:

«Режим защиты информации устанавливается: в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании Закона РФ «О государственной тайне» в отношении конфиденциальной документированной информации — собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона».

3 апреля 1995 г. Президентом РФ был подписан указ № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

Указ носит жесткий характер, монополизирующий контролирующие функции в области разработки, производства, внедрения и эксплуатации криптографических средств за ФАПСИ. В нем, в частности, говорится:

«Запретить использование *государственными организациями*... шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата ФАПСИ...»

«Предложить ЦБ РФ и ФАПСИ принять необходимые меры в отношении коммерческих банков, уклоняющихся от обязательного использования имеющих сертификат ФАПСИ защищенных технических средств хранения, обработки и передачи информации при их взаимодействии с подразделениями ЦБ РФ».

«В интересах информационной безопасности РФ и усиления борьбы с организованной преступностью запретить деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, без лицензий, выданных ФАПСИ в соответствии с Законом РФ «О ФАПСИ».

Ситуация несколько либерализовалось весной 1998 г., когда появились новые положения Банка России о работе с электронными документами. Положение «О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями» Ы17-П (далее — Положение 17-П) наконец-то делает полностью законной в рамках банковской системы России широко распространенную практику проведения коммерческими банками расчетов без обязательного предоставления клиентами платежных поручений на бумажных носителях.

Второй документ — Положение «О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России» №20-П (далее — Положение 20-П) определяет те условия, при которых кредитные организации могут вести расчеты через систему ЦБ РФ в электронной форме.

Положение 17-П, принятое Банком России 10 февраля 1998 г., введено им в действие с момента официального опубликования 18 февраля 1998 г. в «Вестнике Банка России». В качестве его законодательной основы был взят новый Гражданский кодекс Российской Федерации, а именно ст. 160 (п. 1.1 Положения 17-П), которая трактует все возможные легальные способы оформления сделок в Российской Федерации.

Так, Гражданский кодекс РФ допускает «использование при совершении сделок... электронно-цифровой подписи либо иного аналога собственноручной подписи... в случаях и порядке, предусмотренных законом, иными правовыми актами или соглашением сторон».

В Положении 17-П основной упор делается именно на соглашение сторон, зафиксированное в виде договора, как основу их работы с электронными документами. Например, п. 1.7 гласит: «Участники документооборота устанавливают процедуру признания АСП и используют ее в порядке и на условиях, предусмотренных договором между участниками или с Администрацией».

При этом АСП (аналог собственноручной подписи) определяется как *«персональный идентификатор* кредитной организации либо клиента кредитной организации, являющийся контрольным параметром правильности составления всех обязательных реквизитов платежного документа и неизменности их содержания».

В Положении 17-П вводится понятие выделенного центра, называемого в документе Администрацией, к функциям которого относятся «регистрация владельцев АСП, регистрация средств создания и проверки подлинности АСП участников документооборота и хранение эталонов программно-технических средств, предназначенных для составления платежных документов, а также эталонов документации на эти средства».

Это, по существу, составление и поддержание базы данных, аналогичной картотеке образцов подписей клиентов банка в принятых сейчас технологиях работы с бумажными платежными документами. Кроме того, на Администрацию, естественно, возлагаются и задачи хранения резервных или эталонных копий «средств создания и проверки правильности АСП», в частности эталонных копий программного обеспечения для вычисления и проверки цифровых подписей.

В качестве Администрации, согласно этому Положению, в банковской сфере может выступать только отдельное юридическое лицо или подразделение юридического лица (п. 1.6), которое, впрочем, не обязано иметь для этого какие-либо специальные разрешения или лицензии.

Его роль в работе системы электронного документооборота и взаимоотношения с другими участниками определяются отдельным договором (п. 3.2).

Более того, создание специальной Администрации обязательно только при организации документооборота *между более чем двумя участниками* (п. 1.8). Это означает, что работа с электронными документами в системах типа «клиент-банк», где обмен электронными документами происходит непосредственно только между двумя участниками — конкретным клиентом и конкретным банком, не требует обязательного создания специального юридического лица — Администрации. Эти функции вполне могут выполнять сотрудники банка.

Развернутое определение такого варианта АСП, как ЭЦП, дано в Положении 20-П, принятом ЦБ РФ 12 марта 1998 г. В нем ЭЦП определяется как «вид АСП, являющийся средством защиты информации и обеспечивающий возможность контроля целостности и подтверждения подлинности электронных документов. ЭЦП позволяет подтвердить ее принадлежность зарегистрированному владельцу».

Таким образом, в принятых руководящих документах по работе кредитных организаций и их клиентов с электронными документами Банк России пошел по ясному и четко определенному пути, полностью отвечающему логике и требованиям действующего законодательства РФ: от Конституции и Гражданского кодекса до постановлений Правительства РФ.

Второй раздел каждого положения описывает конкретные процедуры работы пользователей с электронными документами: подписывание, передачу, прием, проверку подлинности документа и выдачу квитанции, ведение журналов и архивов. По существу, эти процедуры являются полными аналогами обычных действий при обработке бумажных документов, описаны в привычных терминах и не вызывают к.аких-то серьезных вопросов.

Так, констатируется, что юридическая основа работы — договор между сторонами: «Для создания и проверки АСП могут использоваться программно-технические и иные средства в порядке, *устанавливаемом договором* между участниками документооборота или с Администрацией» (п. 2.2 Положения 17-П). Далее в нем указывается, что «платежные документы, подписанные АСП, признаются имеющими *равную юридическую силу с другими формами поручений* владельцев счетов, подписанных ими собственноручно» (п. 2.3). А п. 2.3 Положения 20-П констатирует, что «ответственность за содержание реквизитов элек-

тронного документа несет владелец ЭЦП, подписавший данный электронный документ, если иное не предусмотрено договором».

Тем самым, эти положения официально подтверждают, что ЦБ признает правильным обязательный пункт договора между сторонами, согласно которому сторона, чей аналог подписи под электронным документом признается правильным по установленной договором сторон процедуре, принимает на себя все обязательства, вытекающие из такого документа, как это принято в бумажном документообороте.

Процедура проверки цифровой подписи пользователя под электронным документом является, согласно п. 2.4 Положения 17-П, окончательным аргументом при установлении достоверности этого документа и должна быть установлена заранее в договоре между сторонами.

Эти положения не требуют от участников придерживаться какой-то определенной процедуры подписывания и проверки электронных документов. Таким образом, полностью на усмотрение участников документооборота оставляется выбор конкретных методов и средств выполнения АСП и ее проверки. Для соблюдения требований ЦБ РФ достаточно, чтобы стороны согласовали заранее все детали процедуры выполнения АСП и проверки ее подлинности, а также официально в рамках подписываемого ими договора о работе с электронными документами подтвердили свое согласие принимать на себя все обязательства, вытекающие из тех электронных документов, которые признаются, согласно установленной процедуре проверки, подписанными.

По соглашению сторон могут быть использованы любые алгоритмы или программы, признаваемые в договоре как достаточные средства для достоверного подтверждения подлинности и авторства электронных документов.

Стороны из соображения удобства использования той или иной вычислительной базы или программного обеспечения могут применять также несколько различных алгоритмов цифровой подписи одновременно или различные их программные реализации.

Таким образом, существующей нормативной базы достаточно для решения многих проблем регулирования правовых отношений в финансовой области. Сегодня практически все используемые системы ЭЦП являются по своей сути межкорпоративными (например, системы «клиент-банк», межбанковских расчетов, электронного документооборота), и неотъемлемым условием юридической значимости ЭЦП в них является предварительное заключение бумажного соглашения о ее использовании. В то же время, появление систем электронной коммер-

ции, а также глобальная информатизация всего общества настоятельно требуют более универсального механизма «легализации» ЭЦП по сравнению с описанным ранее.

Такой механизм существует в мировой практике — это технология ЭЦП с сертификатами. Она специфицирована Международным телекоммуникационным союзом в его рекомендации X.509 и нашла свое развитие в различных приложениях, включая системы электронной коммерции, системы обработки микропроцессорных карт и т. п. Суть технологии cot гоит в том, что некоторая организация, называемая сертификационным или регистрационным центром, заверяет своей подписью образцы всех обратившихся к ней лиц. Именно для того, чтобы придать технологии ЭЦП с сертификатами юридическую силу, и необходим «Закон об электронно-цифровой подписи».

Общее мнение специалистов о «Законе об электронно-цифровой подписи» состоит в следующем. Обязательность лицензирования и получения государственных сертификатов на средства ЭЦП и деятельность регистрационных центров не должны являться категорическим императивом. В случае же введения системы лицензирования и сертификации она должна быть прозрачной и носить заявительный, а не разрешительный характер. Кроме того, необходимы альтернативные предлагаемой ФАПСИ системы сертификации, например, под эгидой Государственной технической комиссии при Президенте РФ и Госстандарта.

Нецелесообразно возлагать на регистрационные центры финансовую ответственность в дополнение к той, что устанавливается уже действующим законодательством. Более разумно предусмотреть механизм страхования рисков, связанных с использованием ЭЦП.

Глава 4. В мире Secure Electronic Transaction

Электронная коммерция на основе протокола SSL

Сегодня наиболее распространенным протоколом, используемым при построении систем ЭК (по различным оценкам не менее 99 % всех транзакций ЭК совершаются с его использованием) является протокол SSL, о котором достаточно подробно рассказывалось в предыдущей главе книги. Принято все протоколы ЭК, использующие SSL, называть также протоколом SSL. Как правило, это не приводит к путанице, поскольку из контекста обычно понятно, о чем в конкретном случае идет речь. Кроме того, использование протокола SSL в протоколах электронной коммерции однотипно — для закрытия соединения между владельцем карты и ТП, а также ТП и его обслуживающим банком. Тем самым решается задача обеспечения конфиденциальности и целостности информации, циркулирующей между участниками ЭК в процессе проведения транзакции. Нужно отметить, что последнее утверждение верно с некоторыми оговорками, о которых будет сказано далее.

Широкое распространение протокола SSL объясняется в первую очередь тем, что он является составной частью всех известных Интернет-браузеров и Web-серверов. Это означает, что фактически любой владелец карты, пользуясь стандартными средствами доступа к Интернету, получает возможность провести транзакцию с использованием SSL.

Другие достоинства SSL — простота протокола для понимания всех участников ЭК и хорошие операционные показатели (скорость реализации транзакции). Последнее достоинство связано с тем, что протокол в процессе передачи данных использует только симметричные протоколы шифрования, которые на 2-4 порядка быстрее асимметричных при том же уровне криптостойкости.

В то же время, протокол SSL в приложении к ЭК обладает рядом существенных недостатков.

Протоколы ЭК, основанные на использовании SSL, не поддерживают аутентификации клиента Интернет-магазином, поскольку сертификаты клиента в таких протоколах почти не используются. Использование «классических» сертификатов клиентами в схемах SSL является делом практически бесполезным. Такой «классический» сертификат, полученный клиентом в одном из известных центров сертификации, содержит только имя клиента и, что крайне редко, его сетевой адрес (большинство клиентов не имеет выделенного IP-адреса). В таком виде сертификат мало чем полезен ТП при проведении транзакции ЭК, поскольку может быть без большого труда получен и мошенником. Для того чтобы сертификат клиента что-нибудь значил для ТП, необходимо, чтобы он устанавливал связь между номером карты клиента и его банком-эмитентом. Причем любой Интернет-магазин, в который обращается за покупкой владелец карты с сертификатом, должен иметь возможность проверить эту связь (возможно, с помощью своего обслуживающего банка).

Другими словами, такой сертификат должен быть получен клиентом в своем банке-эмитенте. Формат сертификата, специальные процедуры маскировки номера карты в сертификате (очевидно, номер карты не должен присутствовать в сертификате в открытом виде), процедуры распространения и отзыва сертификатов, а также многое другое в этом случае должно быть оговорено между всеми участниками транзакции ЭК. Иначе говоря, требуется создание иерархической инфраструктуры центров сертификации (по аналогии с тем, как это делается в протоколе SET, о чем будет рассказано далее). Без создания такой инфраструктуры все разговоры об обеспечении взаимной аутентификации участников транзакции ЭК — непонимание сути вопроса.

Отсутствие аутентификации клиента в схемах SSL является самым серьезным недостатком протокола, который позволяет мошеннику успешно провести транзакцию, зная только реквизиты карты. Тем более, протокол SSL не позволяет аутентифицировать клиента обслуживающим банком (аутентификация клиента обслуживающим банком является важным элементом защиты последнего от недобросовестных действий ТП и обеспечивается протоколом SET).

При использовании протокола SSL ТП аутентифицируется только по своему адресу в Интернете (URL). Это значит, что клиент, совершающий транзакцию ЭК, не аутентифицирует ТП в том смысле, о котором говорилось ранее (не получает доказательств существования договорных отношений между ТП и его обслуживающим банком-участником платежной системы). Аутентификация ТП только по URL облегчает

мошенническим ТП доступ к различным системам ЭК. В частности, торговые предприятия, занимающиеся сбором информации о картах клиентов, могут получить сертификат в каком-либо известном центре сертификации общего пользования (например, Verisign, GTE, Thawte и т. п.) на основании только своих учредительных документов, после чего дорога к мошенничествам для них становится открытой.

Справедливости ради нужно сказать, что проверка сертификата сервера ТП производится только по URL сервера из-за того, что так устроены все известные браузеры на рабочих местах клиентов. Протокол SSL позволяет передавать приложениям, работающим через браузер, информацию, которая может анализироваться этими приложениями (например, имя владельца сертификата, время и дату начала установления сессии и т. п.). На основе анализа полученных данных приложение может вмешиваться в процесс работы протокола (например, признать аутентификацию одного из участников SSL-сессии неуспешной и прервать сессию). Чтобы такой дополнительный анализ был возможен, требуется специальное приложение, использующее функциональность браузера. Такое приложение реализуется в рамках так называемого электронного бумажника или кошелька клиента — специального программного обеспечения, предназначенного для реализации клиентом электронной покупки.

Использование электронного кошелька помимо того, что подразумевает некоторые усилия со стороны клиента (кошелек нужно загрузить), а также наличие центра, распределяющего такие кошельки, само по себе не решает проблему. Для решения проблемы требуется все та же иерархическая инфраструктура центров сертификации, о которой говорилось в предыдущем пункте. Легальность ТП должна устанавливаться только проверкой того факта, что сертификат открытого ключа ТП, соответствующий его закрытому ключу, выдан обслуживающим банком, имеющим всем известный сертификат платежной системы.

Протокол SSL не поддерживает цифровой подписи, что затрудняет процесс разрешения конфликтных ситуаций, возникающих в работе платежной системы (читатель может легко проверить из описания протокола, что цифровая подпись используется в начале установления SSL-сессии при аутентификации участников сессии). Для доказательства проведения транзакции требуется либо хранить в электронном виде весь диалог клиента и ТП (включая процесс установления сессии), что дорого с точки зрения затрат ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение клиентом товара.

При использовании SSL не обеспечивается конфиденциальность данных о реквизитах карты для ТП (как это, впрочем, происходит и в транзакциях «покупка» в обычных неэлектронных ТП).

Большинство браузеров, используемых сегодня в России, в силу ранее существовавших экспортных ограничений использует криптоалгоритмы с ключами ограниченной длины. Ограничение на длину ключа симметричного алгоритма составляло 40 битов, на длину RSA-ключа — 512 битов. Такие ограничения, как показано в главе «Введение в криптографию», существенно снижают криптостойкость используемых алгоритмов. Снятие ограничений Государственным Департаментом США на размер секретных ключей (решение было принято 17 декабря 1999 г.) не позволяет надеяться на быстрое распространение криптографически «усиленных» браузеров, и еще в течение 3-4 лет значительное количество браузеров, используемых в России, будут все еще иметь ключи ограниченного размера.

Нужно отметить, что положение с ограниченным размером ключа браузера можно поправить, если клиент обладает необходимой квалификацией. Для начала клиент должен проверить длину симметричного ключа, поддерживаемого его браузером. Такую проверку легко выполнить, подключившись к Web-серверу www.fortify.neL В нижней правой части окна браузера имеется пункт SSL Check. Если его выбрать, то будет организована SSL-сессия между браузером клиента и сервером. Сервер выберет максимально криптостойкий алгоритм шифрования, доступный на браузере клиента, и сообщит об этом клиенту: в окне браузера появится список симметричных алгоритмов шифрования с указанием длины ключа, а алгоритм, поддерживаемый браузером, в этом списке будет выделен специальным образом.

Если в результате проверки выяснится, что размер ключа меньше 64 битов, очень рекомендуется увеличить его до 128 битов. Для этого необходимо загрузить версию браузера без экспортных ограничений. Если клиент поддерживает одну из версий Netscape Navigator, то это можно сделать сразу после проверки длины ключа в том же окне браузера, выбрав внизу параметр Download.

Если клиент работает на Internet Explorer 4.0, то соответствующую версию браузера можно скачать с ftp-сервера по адресу ftp://ftp.tuniv.szczecin.pl/dskl/ftp.replay.com/pub/browsers/128bit/MS-lexplorer-v40/ie401w95nt_128upgrade.exe. На этом же сервере можно найти заплатки для других версий Internet Explorer.

По правилам международных платежных систем Europay/MasterCard при использовании протокола SSL транзакции по дебетовым картам

запрещены (VISA летом прошлого года приняла решение разрешить транзакции ЭК по дебетовым картам VISA/Electron). Молодые люди составляют значительную часть аудитории пользователей Интернета, и в то же время в силу отсутствия кредитной истории они же являются обладателями дебетовых карт.

Введем следующее определение. Протокол ЭК называется *устойчивым,* если он обеспечивает на уровне криптостойкости признанных алгоритмов цифровой подписи и шифрования:

- аутентификацию владельца карты другими участниками ЭК: ТП и ОБ;
- аутентификацию ТП другими участниками ЭК: владельцем карты и ОБ;
- аутентификацию обслуживающего банка торговым предприятием;
- конфиденциальность сообщений, которыми обмениваются участники ЭК через Интернет;
- конфиденциальность информации о реквизитах карты для ТП;
- целостность данных, которыми обмениваются участники ЭК;
- невозможность отказа от транзакции (non-repudiation) — наличие для каждого участника транзакции электронного практически неопровержимого доказательства факта совершения транзакции.

Как следует из сказанного ранее, протокол SSL не является устойчивым.

Описание протокола SET

Архитектура системы центров сертификации

Как уже отмечалось ранее, необходимым условием создания глобальной системы аутентификации, основанной на использовании асимметричной криптографии, является наличие иерархической однокорневой системы центров сертификации. Основные функции системы ЦС — генерация и распределение сертификатов открытых ключей, обновление сертификатов, а также генерация и распределение списков отозванных ключей (Certificate Revocation Lists, или сокращенно CRL).

В протоколе SET система ЦС имеет 4-уровневую архитектуру, показанную на рис. 4.1 и базирующуюся на использовании протокола X.509.

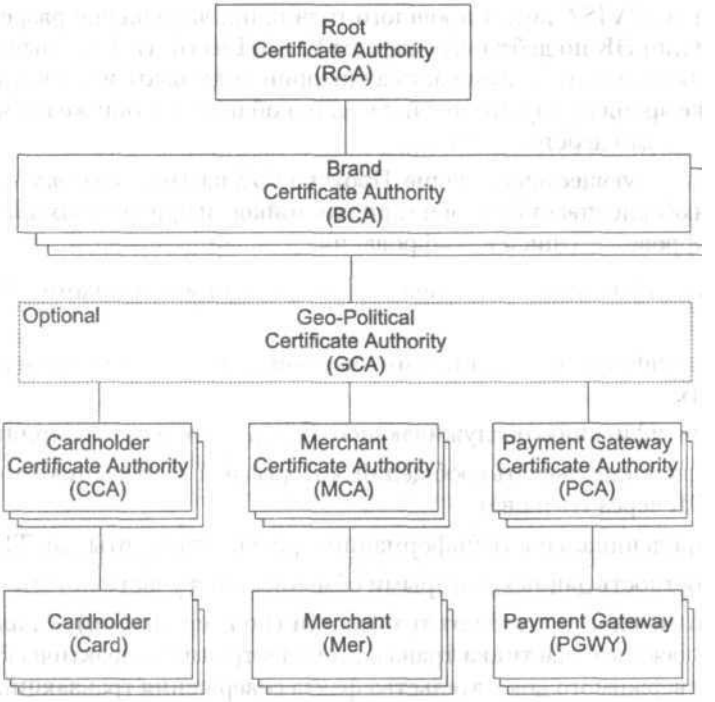

Рис. 4.1. Архитектура системы центров сертификации в стандарте SET

На верхнем уровне располагается Корневой ЦС (Root Certificate Authority, или сокращенно RCA). Он отвечает за генерацию сертификатов для ЦС следующего нижележащего уровня Центров сертификации международных платежных систем (Brand Certificate Authority, или сокращенно BCA), генерацию сертификатов для собственных открытых ключей, а также генерацию и распределение CRL для возможно скомпрометированных ключей ЦС уровня BCA. Оператором RCA является компания SETCo, специально созданная для развития и распространения стандарта SET.

На втором уровне иерархии системы ЦС находятся ЦС платежных систем. В настоящее время такие ЦС созданы в платежных системах VISA, Europay/MasterCard, American Express и других. ЦС уровня BCA отвечает за генерацию сертификатов для ЦС следующих уровней — GCA, CCA, MCA, PCA, а также за генерацию, поддержку и распространение CRL для сертификатов, ранее подписанных данным BCA. Оператором BCA является соответствующая платежная система.

На третьем уровне системы ЦС SET располагается Геополитический ЦС (Geo-Political Certificate Authority, или сокращенно GCA). Наличие ЦС уровня GCA позволяет платежной системе проводить более гибкую политику генерации и распределения сертификатов ключей для ЦС уровня CCA, MCA, PCA в отдельных геополитических зонах земного шара, а также повышать эффективность процедур генерации, поддержания и распространения CRL по сертификатам, эмитированным GCA. Оператор ЦС уровня GCA определяется правилами соответствующей платежной системы. Например, по правилам систем VISA и MasterCard оператором GCA может быть либо сама платежная система, либо Group Member — банк, имеющий статус Группового участника платежной системы.

Наконец, на четвертом, нижнем уровне системы ЦС SET располагаются три так называемых оконечных (End-Entity) типа ЦС: ЦС для владельцев платежных карт (Cardholder Certificate Authority, или сокращенно CCA), ЦС для ТП (Merchant Certificate Authority, или сокращенно MCA) и ЦС для платежных шлюзов (Payment Gateway Certificate Authority, или сокращенно PCA). Центры сертификации уровня End-Entity отвечают за генерацию сертификатов для основных участников транзакции ЭК — для владельца карты, ТП и платежного шлюза. В этом смысле все остальные ЦС играют вспомогательную роль, обеспечивая единую общую инфраструктуру центров доверия, позволяющую любым двум непосредственным участникам транзакции ЭК надежно аутентифицировать друг друга. Кратко остановимся на основных функциях ЦС уровня End-Entity.

ЦС уровня CCA отвечает за генерацию и доставку сертификатов открытых ключей владельцев карт. Запросы на получение сертификатов поступают в CCA от владельцев карт либо через Web-страницы, либо по электронной почте. Для генерации сертификата владельца карты CCA должен поддерживать специальную процедуру идентификации клиента, определенную эмитентом карты. CCA также отвечает за распространение среди владельцев карт списков CRL, сгенерированных RCA, BCA, GCA, PCA. Оператором CCA могут являться банк-эмитент карточек, для которых выпускаются сертификаты, платежная система или третья сторона, определяемая правилами конкретной платежной системы.

ЦС уровня MCA отвечает за генерацию и доставку сертификатов открытых ключей ТП. Запросы на получение сертификатов поступают в MCA от ТП либо через Web-страницы, либо по электронной почте. Для генерации сертификата ТП MCA должен поддерживать специаль-

ную процедуру идентификации ТП, определенную обслуживающим банком данного ТП. MCA также отвечает за распространение в адрес ТП списков CRL, сгенерированных RCA, BCA, GCA, PCA. Оператором MCA могут являться обслуживающий банк ТП, платежная система или третья сторона, определяемая правилами конкретной платежной системы.

ЦС уровня PCA отвечает за генерацию и доставку сертификатов открытых ключей платежным шлюзам. PCA также отвечает за генерацию и распространение списка CRL, содержащего ранее эмитированные данным PCA сертификаты открытых ключей, для которых соответствующие им закрытые ключи оказались скомпрометированными на момент рассылки CRL.

PCA отвечает за распространение в адрес платежных шлюзов листов CRL, сгенерированных RCA, BCA, GCA, PCA. Оператором PCA могут являться обслуживающий банк, платежная система или третья сторона, определяемая правилами рассматриваемой платежной системы.

В протоколе SET используются четыре типа пар асимметричных ключей, отличающихся друг от друга по своему назначению:

- ключ для подписи (Digital Signature Key, используется для идентификации владельца ключа);
- ключ для шифрования данных (Key Encipherment/Data Encipherment Key, или иначе Key-Exchange Key, ключ, используемый для шифрования данных в процессе проведения транзакции ЭК);
- ключ для подписывания сертификатов (Certificate Signature Key);
- ключ для подписывания списков отозванных сертификатов CRL (CRL Signature Key).

В табл. 4.1 указаны типы ключей, используемых различными участниками транзакции ЭК.

Таблица 4.1. Типы ключей

Участник системы ЭК	digital signature	key encipherment/ data encipherment	Cert signature	CRL signature
Владелец карты	X			
ТП	X	X		
Платежный шлюз	X	X		
Cardholder Certificate Authority	X	X	X	
Merchant Certificate Authority	X	X	X	
Payment Certificate Authority	X	X	X	X

Таблица 4.L

Участник системы ЭК	digital signature	key encipherment/ data encipherment	Cert signature	CRL signature
Geopolitical Certificate Authority			X	X
Brand Certificate Authority			X	X
Root Certificate Authority			X	X

Как видно из таблицы, владельцу карты достаточно иметь только один ключ типа Digital Signature Key, в то время как PCA для выполнения своих функций должен иметь ключи всех четырех типов. Далее на примерах процессов сертификации владельца карты в CCA и проведения операции покупки будет продемонстрировано использование различных типов асимметричных ключей.

Разнообразие типов ключей, кроме того, что повышает безопасность системы ЭК в целом, дает больше гибкости при проектировании платежной системы. Это достигается за счет того, что для реализации различных функций появляется возможность использовать ключи различной длины, что повышает производительность системы в целом. Например, ключ ТП Key Exchange Key может иметь более короткую длину по сравнению с ключом ТП Digital Signature Key — для того, чтобы при необходимом уровне криптостойкости уменьшить трудозатраты на выполнение криптографических операций на стороне владельца карты.

Размер асимметричных ключей, используемых в протоколе SET, не фиксирован и может со временем меняться. В настоящее время рекомендуются размеры ключей, приведенные в табл. 4.2.

Таблица 4.2. Рекомендуемые размеры асимметричных ключей

Entity	Message Signature	Key-Exchange	Certificate Signing	CRL Signing
Владелец карты	1024			
ТП	1024	1024		
Платежный шлюз	1024	1024		
Cardholder CA	1024	1024	1024	
Merchant CA	1024	1024	1024	
Payment Gateway CA	1024	1024	1024	1024
Brand Geo-political CA			1024	1024
Brand CA			1024	1024
Root CA			2048	2048

Формат сертификата открытого ключа в протоколе SET удовлетворяет стандарту X.509 v.3. Сертификат содержит следующие данные:

- версию протокола X.509 (всегда устанавливается значение, равное 3);
- Serial Number — серийный номер сертификата — уникальный целочисленный номер сертификата, присваиваемый ЦС, выдавшим сертификат;
- Algorithm Identifier — идентификатор алгоритма ЭЦП, используемого ЦС для подписывания сертификата;
- Issuer Name — имя ЦС, генерирующего сертификат;
- срок начала действия сертификата;
- срок окончания действия сертификата;
- Subject Name — имя владельца сертификата;
- идентификатор алгоритма, в котором будет использоваться сертифицируемый ключ;
- значение сертифицируемого открытого ключа;
- расширения (например, информация о ключе ЦС — эмитента данного сертификата; уровень владельца сертификата в протоколе SET, тип сертификата (например, сертификат владельца карты, сертификат ТП и т. п.) и другое);
- цифровую подпись сертификата, сделанную с использованием Certificate Signing Key ЦС.

Подлинность SET-сертификатов удостоверяется с помощью иерархической цепи проверок.

Любой ЦС, выдавший сертификат следующему за ним в иерархии звену, в свою очередь, должен иметь действительный сертификат от вышестоящей организации. Удостоверение происходит путем сравнения на предмет равенства содержимого некоторых полей сертификата нижнего уровня и сертификата более высокого уровня. Сравниваются следующие поля:

- поля Issuer Name в сертификате нижнего уровня и Subject Name в сертификате более высокого уровня;
- поля CertIssuer и CertSerialNumber из X.509 Extensions сертификата нижнего уровня соответственно с полями Issuer Name и Serial Number в сертификате более высокого уровня.

При положительном результате сравнения в сертификате нижнего уровня проверяется:

- срок действия сертификата;
- срок действия ключа, указанного в сертификате;

- уровень владельца сертификата в иерархии системы ЦС;
- соответствие типа сертификата его содержимому;
- использование по назначению ключа, указанного в сертификате, и некоторые другие поля.

В сертификате более высокого уровня проверяется:

- срок действия сертификата;
- срок действия ключа, указанного в сертификате;
- уровень владельца сертификата в иерархии системы ЦС;
- соответствие типа сертификата его содержимому;
- использование по назначению ключа, указанного в сертификате, и некоторые другие поля.

Процедуры генерации, обновления и отзыва сертификатов

В самых общих чертах процедуры генерации сертификатов для участников транзакции ЭК выглядят следующим образом.

Чтобы получить сертификат своего открытого ключа, владелец карты направляет специальный запрос в адрес своего ССА. В ответ ССА передает владельцу карты сертификат своего открытого ключа.

Владелец карты передает ССА номер своей карты, зашифрованный на открытом ключе ССА, и в ответ получает регистрационную форму, соответствующую данной карте.

Владелец карты заполняет регистрационную форму, включая в нее сведения о себе, идентифицирующие владельца карты данные (включая, например, разовый пароль, предоставленный эмитентом карты), а также открытый ключ владельца карты.

ССА с помощью эмитента идентифицирует владельца карты и генерирует для него сертификат открытого ключа.

Более детальное описание процедуры генерации сертификата владельца карты будет приведено далее.

Процедура получения сертификата ключа ТП является более простой по сравнению с процедурой генерации сертификата владельца карты.

На первом этапе ТП обращается в МСА со специальным запросом на получение сертификата своего открытого ключа.

В ответ ТП получает открытый ключ МСА и регистрационную форму.

На втором этапе ТП заполняет регистрационную форму, включая в нее идентифицирующие ТП данные, а также открытый ключ ТП. В ответ после проверки подлинности ТП с помощью его обслуживающего банка MCA генерирует сертификат открытого ключа ТП.

Аналогичным образом с помощью двухэтапной процедуры осуществляется генерация сертификата открытого ключа и для платежного шлюза. Разница состоит в том, что платежный шлюз обращается за сертификатом своего открытого ключа в PCA.

В отличие от владельца карты ТП и платежный шлюз должны получить сертификаты открытых ключей типов Digital Signing Key и Key-Exchange Key.

ЦС уровня End-Entity получают сертификаты своих открытых ключей в ЦС уровня GCA или BCA, GCA в BCA, BCA в RCA. Процедуры получения этих сертификатов не формализованы стандартом SET. Запрос сертификата осуществляется с помощью сообщения формата PKCS# 10, а сертификат от вышестоящего ЦС поступает в формате PKSC#7.

Открытый ключ подписи ЦС уровня RCA распространяется среди производителей прикладного программного обеспечения, работающего с протоколом SET. ПО включает сертификат корневого ключа. В отличие от сертификатов участников, этот сертификат подписывается с использованием закрытого корневого ключа подписи.

Процедуры обновления сертификатов аналогичны процедурам их генерации. В спецификациях SET говорится о том, что на усмотрение эмитента и/или обслуживающего банка в процедурах обновления сертификатов в регистрационных формах может использоваться информация о старых сертификатах открытых ключей.

Специальная процедура смены ключа предусмотрена для Certificate Signing Key ЦС уровня RCA. Этот корневой ключ подписи сертификатов генерируется в двух экземплярах — действующая пара ключей R, и пара ключей R_2, которая будет действовать после окончания срока действия пары $R_г$ В сертификате открытого ключа пары R,, подписанном закрытым ключом этой же пары, содержится значение хэш-функции открытого ключа пары R_2. Поэтому, получив новую пару ключей R_2, участник транзакции ЭК проверяет равенство значений хэш-функции нового открытого ключа со значением, содержащемся в старом сертификате. Таким образом подтверждается подлинность полученного нового сертификата открытого ключа подписи.

Рекомендуемые сроки обновления пар асимметричных ключей приведены в табл. 4.3.

Таблица 4.3. Примерные сроки обновления ключей

Участник транзакции ЭК	Signature	Key-Encipherment	Certificate Signature	CRL Signature
Владелец карты	3 года			
Торговое предприятие	1 год	1 год		
Платежный шлюз	1 год	1 год		
Cardholder CA	1 год	1 год	1 год	
Merchant CA	1 год	1 год	1 год	
Payment Gateway CA	1 год	1 год	1 год	1 год
Geopolitical CA			1 год	1 год
Brand CA			1 год	1 год
Root CA			1 год	1 год

Соответствующие этому примеру сроки хранения сертификатов приведены в табл. 4.4.

Таблица 4.4. Пример периодов хранения сертификатов

Участник транзакции ЭК	Signature	Key-Encipherment	Certificate Signature	CRL Signature
Владелец карты	3 год			
Торговое предприятие	1 год	1 год		
Платежный шлюз	1 год	1 год		
Cardholder CA	1 год	1 год	4 года	
Merchant CA	1 год	1 года	2 года	
Payment Gateway CA	1 год	1 год	2 года	2 года
Geopolitical CA			5 лет	2 года
Brand CA			6 лет	2 года
Root CA			7 лет	2 года

Результаты, приведенные в последней таблице, получаются из предположения, что каждый вышестоящий ЦС выдает сертификат нижестоящему ЦС в последний день действия сертификата вышестоящего ЦС. Проиллюстрируем сказанное на примере расчета срока действия сертификата открытого ключа Certificate Signing Key ЦС уровня RCA. Поскольку в нашем примере среди всех участников транзакции ЭК наибольшим сроком действия обладает ключ владельца карточки (3 года), то рассмотрим следующую цепочку. Предположим, что владелец карты получил сертификат своего ключа в последний день действия Certificate Signing Key ЦС уровня CCA, который, в свою очередь, получил серти-

фикат на этот ключ в последний день действия ключа Certificate Signing Key ЦС уровня GCA. ЦС уровня GCA получил свой сертификат для ключа Certificate Signing Key в последний день действия ключа Certificate Signing Key ЦС уровня BCA, а последний, в свою очередь, получил сертификат на этот ключ в последний день действия сертификата ключа Certificate Signing Key ЦС уровня RCA. В результате для проверки сертификата владельца карты необходимо хранить сертификаты открытых ключей Certificate Signing Key ЦС уровней RCA, BCA, GCA и CCA соответственно 7, б, 5 и 4 года.

Остановимся теперь на процедурах отзыва сертификатов. Сертификат может быть отозван по одной из следующих причин:

- соответствующий сертификату секретный ключ стал известен злоумышленнику;
- сертификат принадлежит субъекту системы ЦС SET, по каким-либо обстоятельствам прекратившему свое функционирование;
- изменились учетные данные сертификата.

Как уже отмечалось ранее, списки отозванных сертификатов CRL генерируют и поддерживают RCA, BCA, GCA, PCA. При этом RCA CRL содержит отозванные сертификаты, принадлежащие RCA и BCA, BCA CRL содержит отозванные сертификаты GCA, CCA, MCA, PCA, GCA CRL — отозванные сертификаты CCA, MCA, PCA, обслуживаемых данным GCA, PCA CRL — отозванные сертификаты платежных шлюзов, обслуживаемых данным PCA. Список CRL всегда подписывается ЦС, сгенерировавшим данный CRL.

Список отозванных сертификатов CRL содержит следующие поля:

- номер версии CRL (значение равно 2);
- идентификатор алгоритма, с помощью которого подписывается CRL;
- имя ЦС, сгенерировавшего CRL;
- дату генерации CRL;
- дату окончания действия CRL;
- серийные номера отзываемых сертификатов;
- дату начала действия CRL;
- некоторые дополнительные данные (номер CRL, идентификационные данные ключа ЦС, сгенерировавшего CRL, включая имя эмитента ключа и его серийный номер).

Владелец карты должен быть гарантирован от того, чтобы в процессе совершения транзакции ЭК он не использовал отозванный сертифи-

кат платежного шлюза (как будет показано далее, для закрытия некоторых конфиденциальных данных, содержащихся в сообщении, передаваемом от владельца карты к ТП, используется открытый ключ шлюза). Для этого необходимо, чтобы владелец карты получал все списки CRL, относящиеся к платежной системе, карта которой используется для совершения данной транзакции. В соответствии со спецификациями SET к спискам CRL данной платежной системы относятся:

- список CRL-C, объединяющий списки RCA CRL, BCA CRL, GCA CRL;
- списки PCA CRL.

Во время проведения транзакции ЭК при получении сертификата шлюза владелец карты проверяет по спискам PCA CRL, не является ли данный сертификат отозванным, а по списку CRL-C для владельцев карты — не является ли отозванным сертификат какого-нибудь ЦС, участвующего в цепочке получения сертификата платежного шлюза.

Владельцу карты нет необходимости проверять, является ли отозванным сертификат торгового предприятия, в котором совершается транзакция ЭК. Это связано с двумя обстоятельствами:

- при использовании протокола SET владелец карты не передает в открытом для ТП виде никакой конфиденциальной информации о реквизитах карты;
- проверка подлинности сертификата ТП возлагается на его обслуживающий банк — именно обслуживающий банк при поступлении к нему транзакции ЭК должен определить, что использовавшийся сертификат был скомпрометирован, и отвергнуть транзакцию.

От владельца карты требуется только проверка по списку CRL-C всех сертификатов, используемых при определении подлинности сертификата ТП.

ТП, так же как и владелец карты, должно уметь определять отозванные сертификаты платежных шлюзов, поскольку именно ТП сообщает владельцу карты сертификаты шлюза в процессе совершения транзакции ЭК.

ТП не должно уметь идентифицировать отозванные сертификаты владельцев карт (эта функция возлагается на эмитентов карт), но должно определять отозванные сертификаты ЦС, участвующих в формировании сертификата владельца карты.

Наконец, платежный шлюз должен проверять по CRL-C отсутствие отозванных сертификатов в цепочке сертификатов ТП и владельца карты.

За распространение и хранение списков CRL отвечают ЦС и платежные шлюзы. В процессе выдачи и обновления сертификатов ЦС сооб-

щают владельцам карт, ТП и платежным шлюзам актуальные на данный момент времени списки CRL. Актуальные списки сообщаются участникам транзакции ЭК и в процессе проведения SET-транзакции. При этом ТП актуализирует списки CRL, получая недостающие списки от платежного шлюза, владелец карты обновляет списки в диалоге с ТП. Кроме того, в рамках SET существует специальная пара сообщений между ТП и платежным шлюзом (Gateway Certificate Request/Response Messages), с помощью которой, в том числе, можно получить обновленные версии списков CRL.

Процедура обновления списков отозванных сертификатов использует каталог всех актуальных на данный момент времени списков CRL в данной платежной системе. Такой каталог называется Brand CRL Identifier (или, сокращенно, BCI). Он состоит из списка номеров всех актуальных на данный момент CRL и подписывается с помощью CRL Signing Key ЦС уровня BCA. Владельцы карт и ТП получают актуальные значения BCI в процессе сертификации-обновления своих ключей от своих ЦС (соответственно — CCA и MCA), а также во время проведения транзакции ЭК в ответных сообщениях, получаемых, соответственно, от ТП и платежного шлюза. ЦС и платежные шлюзы, в свою очередь, получают BCI вместе со всеми ассоциированными с данным BCI списками CRL из ЦС уровня BCA. В соответствии с протоколом SET ЦС и платежные шлюзы обязаны обновлять каталог BCI на ежедневной основе.

Каталог BCI используется для избирательного предоставления только недостающих списков CRL. Например, во время проведения транзакции ЭК владелец карты передает ТП данные о каталоге BCI, актуальном для владельца карты на данный момент времени. ТП возвращает в ответном сообщении актуальный каталог, имеющийся на стороне ТП, а также в общем случае не все списки BCI, ассоциированные с данным CRL, а только те списки, которых не хватает владельцу карты. Такая технология позволяет уменьшить объем сообщений, циркулирующих между участниками транзакции ЭК. Каждый ЦС, поддерживающий генерацию списков CRL, передает вновь сгенерированный список в соответствующий ЦС уровня BCA. RCA также передает CRL, содержащий скомпрометированные корневые ключи, во все во все ЦС уровня BCA.

Опишем теперь процедуру получения сертификата открытого ключа владельцем карты более детально, иллюстрируя, каким образом осуществляется решение основных задач защищенного обмена информацией — аутентификации источника информации и обеспечения целостности и конфиденциальности передаваемой в процессе сертификации информации.

1. Владелец карты генерирует запрос (в терминах SET — сообщение CardCInitReq), содержащий идентификатор пары сообщений (запроса-ответа на получение сертификата владельцем карты; в терминологии протокола SET — RRPID), идентификатор транзакции (в терминологии SET — LID-EE), генерируемый владельцем карты для учета запроса в системе владельца карты, идентификатор платежной системы (в терминологии SET — Brand ID), случайное число Chall-EE и в качестве параметров «отпечатки» всех сертификатов (включая Root certificate), списков CRL и BCI, хранящихся в системе владельца карты. Под «отпечатком» (по-английски — Thumbprint) здесь понимается значение хэш-функции от соответственно сертификата, CRL, BCI. Хэш-функция применяется для того, чтобы уменьшить объем передаваемой информации, в то же время с высокой вероятностью однозначно идентифицируя хэшируемую информацию.
2. CCA обрабатывает полученное от владельца карты сообщение CardCInitReq, производя следующие проверки:
   - проверяет равенство значений RRPID в заголовке и содержимом полученного сообщения;
   - запоминает «отпечатки» сертификатов, CRL, BCI из сообщения CardCInitReq, а также LID-EE и Chall-EE.
3. После этого CCA генерирует ответ (в терминологии SET — CInitCardRes), состоящий из подписываемых с помощью CCA Private Signature Key данных. Данные содержат «отпечатки» сертификатов, CRL, BCI из сообщения CardCInitReq, LID-EE, Chall-EE, параметрически идентификатор запроса LID-CA, генерируемый CCA, «отпечаток» сертификата CCA Key-Exchange ключа, сертификаты CCA Key-Exchange Key, CCA Signature Key, а также «отпечаток» BCI в случае, если в сообщении CardCinitreq «отпечаток» BCI отсутствовал. На этом заканчивается этап инициализации получения сертификата владельцем карты.
4. Владелец карты (точнее, конечно, его программное обеспечение), получив сообщение CardCInitRes, проверяет сертификаты CCA Key-Exchange Key и CCA Signature Key, а также цифровую подпись CCA. Поскольку цифровая подпись CCA относится к данным, включающим Chall-EE, ее проверка эквивалентна аутентификации CCA владельцем карты. Таким образом, проверив цифровую подпись, содержащуюся в полученном от CCA сообщении, владелец карты убеждается в том, что в процессе сертификации своего открытого ключа он имеет дело с подлинным центром сертификации.

5. Далее владелец карты передает в адрес CCA запрос на получение регистрационной формы (в терминологии SET — RegFormReq). При формировании этого запроса владелец карты создает данные RegFormReqData, содержащие:
   - новый идентификатор RRPID сообщений на запрос/ответ регистрационной формы;
   - идентификатор транзакции LID-EE из CardCInitReq;
   - новое случайное число Chall-EE2;
   - идентификатор транзакции LID-CA, если он присутствовал в сообщении CardCInitRes;
   - язык, на котором должна быть написана запрашиваемая форма;
   - некоторые другие данные, например, «отпечатки» сертификатов, CRL и BCI, содержащиеся в системе владельца карты.

После этого владелец карты по случайному закону генерирует симметричный ключ K_r с помощью которого шифруются данные RegFormReqData. Симметричный ключ K, вместе с номером карты, в свою очередь, закрываются CCA Public Key-Exchange Key и передаются CCA.

6. CCA, получив сообщение RegFormReq, с помощью своего Private Key-Exchange Key расшифровывает номер карты и значение ключа Kj и далее с помощью ключа K_y дешифрует RegFormReqData.
7. По номеру карты и языку владельца карты CCA определяет соответствующую регистрационную форму для владельца карты, подписывает эту форму вместе с другими данными (включая Chall-EE2) своим ключом Private Signature Key и отправляет ее владельцу карты.
8. Владелец карты вновь проверяет сертификат ключа Private Signature Key и цифровую подпись CCA и производит следующие действия:
   - заполняет полученную регистрационную форму, включая в нее свое имя, срок действия карты, адрес (account billing address) и любую другую информацию, которая, по мнению эмитента карты, является необходимой для идентификации владельца карты (например, разовый пароль для идентификации владельца карты);
   - генерирует случайное число S,, включаемое в регистрационную форму;
   - генерирует по случайному закону пару симметричных ключей

- объединяет заполненную регистрационную форму, Cardholder Public Key и ключ K_2, подписывает эти данные с помощью Private Signature Key и далее шифрует все получившиеся в результате описанных в этом пункте операций данные с помощью ключа K_3;
- ключ K_3 вместе с номером карты шифруются ключом CCA Public Key-Exchange Key и передаются CCA (это сообщение в терминологии SET называется CertReq).

9. CCA, получив сообщение CertReq, с помощью CCA Private Signature Key расшифровывает значение K_3, далее расшифровывает регистрационную форму и ключ K_2, проверяет цифровую подпись владельца карты. Далее CCA идентифицирует владельца карты (например, по соответствию номера карты разовому паролю, предоставленному ранее эмитентом карты центру сертификации).

   CCA генерирует случайное число S_2, которое комбинируется вместе с числом S, для формирования секрета карты S. Значение S хэшируется вместе с номером карты и сроком ее действия в значение, которое используется в сертификате владельца карты (это делается для того, чтобы номер карты не мог стать известным ТП в результате получения сертификата открытого ключа владельца карты). При этом из полученного значения идентификатора сертификата владельца карты невозможно установить номер карты, даже если известен секрет S и срок действия карты. Наоборот, если известен секрет карты, номер карты и срок ее действия, значение идентификатора сертификата вычисляется легко.

   После этого CCA создает сертификат открытого ключа владельца карты, подписывая его своим Private Signature Key, и формирует ответ CertRes, содержащий значение S_2, сертификат владельца карты и другую информацию (например, логотип платежной системы и/или банка-эмитента). Сформированное сообщение подписывается ключом K_2 и отправляется владельцу карты.

10. Владелец карты с помощью ранее запомненного значения ключа K_2 расшифровывает полученное сообщение CertRes, проверяет сертификат своего открытого ключа и формирует значение секрета S, которое в дальнейшем используется владельцем карты при проведении транзакций ЭК, о чем будет рассказано далее.

Таким образом, процедура получения сертификата открытого ключа состоит из трех этапов.

1. Первый этап характеризуется получением владельцем карты недостающих списков CRL и аутентификацией CCA (используется

стандартная процедура «рукопожатия», когда владелец карты сообщает CCA некоторое случайное число, а CCA возвращает подписанные им данные, содержащие это случайное число).

2. На втором этапе в защищенной с помощью полученного открытого ключа CCA сессии владелец карты запрашивает в CCA регистрационную форму, сообщая CCA номер своей карты. CCA в зависимости от номера карты предоставляет владельцу карты регистрационную форму.
3. Наконец, на третьем этапе клиент заполняет регистрационную форму, включая в нее свой открытый ключ, и направляет ее владельцу карты. Взамен клиент получает от CCA сертификат открытого ключа и некоторый секрет, используемый для маскирования номера карты в сертификате, а также для дальнейшей аутентификации владельца карты его банком-эмитентом.

Реализация транзакций в протоколе SET

Опишем теперь типы транзакций, используемых в протоколе SET. В протоколе SET сообщения, с помощью которых реализуются различные транзакции, имеют парный характер (запрос-ответ).

- **Payment Initialization Request/Response Messages.** Эта пара сообщений используется для взаимной аутентификации владельца карты и ТП, для передачи владельцу карты от ТП необходимых сертификатов и списков CRL, а также предоставления информации ТП о том, карта какой платежной системы будет использоваться при проведении покупки ЭК.
- **Purchase Order Request/Response Messages.** Эта пара сообщений служит для передачи в защищенной сессии от владельца карты к ТП информации о заказе (сумма покупки, валюта, номер ТП и т. п.) и реквизитах карты владельца карты.
- **Authorization Request/Response Messages.** Запрос Authorization Request инициируется ТП и передается платежному шлюзу для передачи ему данных по транзакции и реквизитам карты. В дальнейшем эти данные будут использованы для формирования сообщения, передаваемого эмитенту карты через платежную сеть.
- **Gateway Certificate Request/Response Messages.** Эта пара сообщений позволяет ТП запросить у платежного шлюза его сертификат Key-Exchange Key.
- **Batch Administration Request/Response Messages.** Эта пара сообщений используется для администрирования наборов (batch) тран-

закций для того, чтобы ТП и обслуживающий банк могли провести сверку данных каждой стороны (reconciliation). Запрос позволяет открывать новые наборы транзакций, очищать и закрывать существующие наборы транзакций, а также выяснять их статус.

- **Inquiry Request/Response Messages.** С помощью этой пары сообщений владелец карты может выяснить статус выполнения электронной покупки (получена позитивная авторизация, сделан заказ, в процессе доставки, товар доставлен и т. п.). Inquiry Request может быть отправлен владельцем карты в любое время и любое количество раз.
- **Authorization Reversal Request/Response Messages.** Пара сообщений используется для того, чтобы отменить ранее проведенную авторизацию. Эта пара сообщений может также использоваться для того, чтобы скорректировать размер транзакции в ранее выполненной авторизации.
- **Capture Request/Response Messages.** Сообщение Capture Request передается от ТП к платежному шлюзу и запрашивает у обслуживающего банка платеж за сделанную покупку. Размер запрашиваемого платежа должен быть ранее авторизован банком-эмитентом владельца карты с помощью сообщений Authorization Request/Response. Обычно ТП инициирует запрос Capture Request после выполнения заказа, связанного с электронной покупкой.
- **Credit Request/Response Messages.** Эта пара используется для того, чтобы вернуть ранее сделанный платеж обслуживающего банка в адрес ТП.
- **Credit Reversal/Response Messages.** Эта пара сообщений позволяет ТП отменить кредит в пользу обслуживающего банка.

Рассмотрим теперь подробнее, каким образом реализуется операция электронной покупки с использованием протокола SET.

Владелец карты инициирует покупку с помощью сообщения PinitReq. В этом сообщении владелец карты передает ТП сформированный им идентификатор пары сообщений PinitReq/PinitRes, идентификатор транзакции LID-C, сгенерированный владельцем карты для учета в системе владельца карты, идентификатор платежной системы Brand ID, карточкой которой владелец карты собирается совершить электронную покупку, BIN карточки (первые 6 цифр номера карты), язык, используемый владельцем карты для совершения операции, параметрически «отпечатки» сертификатов, списков CRL и каталога BCI, хранящихся в системе владельца карты, случайное число Chall-C, сгене-

рированное владельцем карты, параметрически идентификатор транзакции в системе ТП, использовавшийся в сообщении, инициировавшем систему владельца карты на совершение транзакции.

В ответном сообщении PinitRes ТП формирует следующие данные:

- копирует из запроса владельца карты данные LID-C и язык;
- генерирует глобальный идентификатор транзакции XID;
- копирует из запроса PinitReq «отпечатки» сертификатов, списки отозванных сертификатов, каталоги BCI, Chall-C;
- генерирует случайное число Chall-M;
- на основании Brand ID, BIN и сертификата владельца карты выбирает соответствующий платежный шлюз и вставляет в сообщение сертификат Key-Exchange Key этого платежного шлюза;
- вставляет в сообщение текущий каталог BCI, если в запросе клиента «отпечаток» каталога BCI отсутствовал либо присутствовал «отпечаток» уже неактуального каталога (напомним, что в соответствии с принятыми в протоколе SET соглашениями наряду с BCI в поле CRL данных SignedData передаются также ассоциированные с данным BCI списки CRL);
- некоторые другие данные.

ТП подписывает данные своим закрытым ключом Signing Key и направляет сформированное таким образом сообщение владельцу карты.

Остальные этапы реализации электронной покупки будут описаны менее детально.

Владелец карты проверяет полученные сертификаты открытого ключа подписи ТП и открытого ключа Key-Exchange Key платежного шлюза, после чего проверяется цифровая подпись ТП в полученном сообщении. Таким образом, владелец карты аутентифицирует ТП.

После этого владелец карты начинает формирование сообщения PReq. Это сообщение состоит из двух частей: инструкции по заказу (Order Instruction, или сокращенно — OI) и платежной инструкции (Payment Instruction, или сокращенно PI).

OI предназначено для ТП и включает в себя значение Chall-M из сообщения PinitRes, идентификатор транзакции XID, размер транзакции и валюту транзакции, идентификатор ТП, идентификатор batch, к которому должна быть отнесена покупка, номер заказа в системе магазина, хэш-функцию от PI (H_2) и некоторую другую информацию. PI предназначено для платежного шлюза и включает в себя идентификатор

транзакции XID, величину TranStain, представляющую собой хэш-функцию от секрета карты S и XID, хэш-функцию OI (H,), параметрически значение CVC2/CVC2,2-ю дорожку магнитной полосы карты и другую информацию.

Далее владелец карты вычисляет хэш-функцию от последовательности, состоящей из значений хэш-функции от PI и 01 (H), и подписывает полученное значение своим секретным ключом.

Владелец карты генерирует случайным образом симметричный ключ K,, с помощью которого он шифрует PL Значение ключа K, вместе с данными по карте (номер карты, срок ее действия и секрет карты), в свою очередь, закрываются с помощью открытого ключа Key-Exchange Key платежного шлюза. Сообщение Preq состоит из OI, зашифрованной инструкции PI, зашифрованных данных о реквизитах карты и ключе K,, цифровой подписи владельца карты.

ТП, получив сообщение PReq, проверяет сертификат владельца карты, после чего проверяет цифровую подпись владельца карты. Для проверки цифровой подписи ТП вычисляет значение хэш-функции от 01 и далее, используя значение хэш-функции для PI (H_2), вычисляет общее значение H. После этого с помощью открытого ключа владельца карты дешифруется полученное из сообщения PReq значение цифровой подписи. Если дешифрованное значение совпадает с общим значением, — подпись была сделана владельцем сертификата открытого ключа владельца карты. Таким образом ТП аутентифицирует владельца карты.

Далее ТП подготавливает сообщение AuthReq. В это сообщение без изменений из сообщения PReq включены зашифрованная платежная инструкция PI, зашифрованный симметричный ключ K, и данные о реквизитах карты, а также цифровая подпись владельца карты. Кроме этих данных ТП формирует авторизационный запрос, содержащий информацию о размере транзакции, идентификаторе ТП, идентификатор транзакции XID, случайное число Chall-P и другую. Эта информация подписывается ключом Signing Key ТП, закрывается симметричным ключом K_2, сгенерированным ТП по случайному закону, который в свою очередь закрывается открытым ключом Key-Exchange Key платежного шлюза.

Платежный шлюз, получив AuthReq, дешифрует с помощью закрытого ключа Key-Exchange Key оба симметричных ключа K, и K_2, а также данные о реквизитах карты, дешифрует данные о транзакции и PI, проверяет подпись владельца карты (по аналогии с тем, как это делает ТП, для этого используется значение H,, содержащееся в PI), проверяет на

равенство значения XID из информации о транзакции и из PL Таким образом, платежный шлюз аутентифицирует как ТП, так и владельца карты. На основании полученных данных платежный шлюз готовит стандартное сообщение (например, в формате ISO 8583) для передачи его в платежную систему на авторизацию эмитента карты.

Получив из платежной системы ответ, платежный шлюз генерирует и подписывает своим закрытым Signing Key сообщение AuthR.es (в сообщении содержится случайная величина Chall-P, также данные Capture Token, в которых платежный шлюз запрашивает у ТП ожидаемые им данные от ТП в сообщении Capture Request). Сообщение зашифровывается с помощью сгенерированного для этого симметричного ключа, который в свою очередь закрывается с помощью открытого ключа ТП.

ТП дешифрует симметричный ключ, проверяет цифровую подпись платежного шлюза и формирует сообщение PRes, содержащее Chall-C, подписывая его своим закрытым Signing Key.

Владелец карты, получив сообщение PRes, проверяет цифровую подпись ТП. На этом процесс электронной покупки может быть закончен.

Расчеты между ТП и обслуживающим банком осуществляются либо на основании приведенной ранее схемы электронной покупки, либо на основании дополнительного запроса Capture Request от ТП.

Относительно протокола SET имеют место следующие утверждения.

Теорема 1. Протокол SET является устойчивым протоколом ЭК.

Доказательство этой теоремы следует из приведенного описания протокола.

Таким образом, SET обладает следующими свойствами:

- Мошеннику недостаточно знать реквизиты платежной карты для того, чтобы успешно выполнить SET-транзакцию. Помимо реквизитов карты необходимо иметь закрытый ключ владельца данной карты, а также сертификат соответствующего ему открытого ключа.
- ТП при выполнении SET-транзакции точно знает, что владелец карты, совершающий транзакцию, является подлинным, то есть обладает секретным ключом RSA, для которого открытый ключ сертифицирован банком-эмитентом клиента.
- Клиент точно знает, что ТП, в котором совершается SET-транзакция, является истинным, то есть обладает секретным ключом RSA, для которого открытый ключ сертифицирован обслуживающим банком ТП.

- ОБ точно знает, что владелец карты и ТП являются подлинными, то есть обладают сертифицированными ключами.
- Информация о реквизитах карты не известна ТП.
- ТП и владелец карты имеют заверенные подписями соответственно владельца карты и ТП подтверждения факта совершения транзакции, что делает невозможным отказ от результатов операции ни одного из участников транзакции ЭК.

Теорема 2. Протокол SET является *единственным* открытым (известным) устойчивым протоколом ЭК.

Сегодня не существует никакого другого (кроме SET) опубликованного устойчивого протокола ЭК. Другими словами, на рынке аппаратно-программных решений, реализующих устойчивый протокол ЭК, не существует альтернативы продуктам, реализующим SET. VISA International предполагает в ближайшее время опубликовать спецификации нового глобального стандарта аутентификации, называемого 3D Secure. Однако неочевидно, что этот стандарт будет определять устойчивый протокол ЭК.

Теорема 3. Протокол SET де-факто является *отраслевым стандартом* в области пластиковых карт.

Будучи признанным ведущими международными платежными системами (VISA, MasterCard, Europay, AmEx, Diners Club) в качестве стандарта ЭК, SET де-факто является отраслевым стандартом.

Таким образом, протокол SET является на сегодняшний день единственным открытым и устойчивым протоколом ЭК.

Расширения стандарта SET

Версия 1.0 стандарта SET была принята в 1997 г. С тех пор протокол получил дальнейшее развитие в виде ряда расширений (сегодня их насчитывается 8).

Наиболее существенными расширениями являются:

- Common Chip Extension (использование микропроцессорных карт, удовлетворяющих стандарту EMV, для проведения электронных покупок на базе протокола SET);
- CVV2/CVC2 Extension (передача данных, используемых для верификации карт, в сообщениях Purchase Request протокола SET);
- Track 2 Data Extension (передача некоторых данных 2-й дорожки магнитной полосы эмитенту);

- On-line PIN Extension (возможность передачи PIN-кода от владельца карты к банку-эмитенту в сообщении Purchase Request протокола SET).

Коротко остановимся на каждом из перечисленных расширений.

Описание Common Chip Extension v.1 появилось 29 сентября 1999 г. и носит революционный характер для ЭК (до этого существовало несколько попыток создания стандарта, позволяющего совместить микропроцессорные карты с ЭК). Цель этого расширения — позволить осуществлять SET-транзакции с использованием EMV-карт. Предполагается, что к компьютеру покупателя подключено специальное устройство — карт-ридер, предназначенное для считывания информации с микропроцессорной карты.

Суть расширения состоит в следующем. Приложение клиента на его персональном компьютере (оно называется электронным кошельком, или по-английски wallet) эмулирует функцию POS-терминала в обычных транзакциях покупки по микропроцессорным картам. Оно инициирует EMV-транзакцию, направляя карте команду Select, в которой представляет карте в качестве поддерживаемого приложения приложение, находящееся на карте. Далее приложение клиента передает карте команду Get Processing Options, получая в ответ от карты Application Interface Profile (указания приложению, какие проверки поддерживаются картой) и Application File Locator (указания приложению адресов записей, необходимых ему для процессинга транзакции).

После этого, как в обычном EMV-сценарии, приложение клиента на основании данных Application File Locator с помощью команды Read Record считывает нужные данные и генерирует команду Generate AC, требуя от карты провести транзакцию в режиме on-line. Карта генерирует криптограмму ARQC (Application Request Cryptogram), используя случайное число Unpredictable Number, переданное ей в качестве параметра команды Generate AC, а также другую информацию, связанную с транзакцией (сумма транзакции, тип транзакции, дата транзакции), терминалом (в нашем случае приложением покупателя — код страны, результаты проверки терминала (Terminal Verification Result)) и картой (счетчик транзакции, результаты проверки карты (Card Verification Result), Application Interface Profile и т. п.). Криптограмма ARQC представляет собой перечисленные выше данные вместе с подписью этих данных, сделанной с помощью алгоритма Triple DES, и симметричным ключом, известным только карте и ее эмитенту.

ARQC помещается в раздел PI и далее шифруются в соответствии со стандартом SET. Эти данные передаются банку-эмитенту для аутентификации карты. Банк-эмитент в соответствии со стандартом EMV проверяет ARQC и подготавливает в ответ сообщение ARPC (Application Response Cryptogram), содержащее код авторизации и подпись банка-эмитента.

Таким образом, применение EMV-карты позволяет обеспечить в операциях ЭК взаимную аутентификацию карты и банка-эмитента. При этом приложение клиента сертификат карты не проверяет. С точки зрения безопасности операции ЭК с использованием EMV-карты приравниваются к SET-транзакциям с сертификатами.

On-line PIN Extension содержит два расширения: расширение для случая, когда PIN-код вводится покупателем через Security Device (PIN-Pad), и расширение, когда PIN-код вводится с клавиатуры PC.

Расширения определяют:

- способы идентификации транзакций ЭК, содержащих PIN-код, а также способ идентификации Internet Payment Gateway, который способен транслировать полученный PIN-код в платежную сеть;
- способ передачи PIN-кода в данных PI сообщения PReq;
- способ передачи некоторых дополнительных Discretionary Data, которые могут использоваться эмитентом при вычислении PIN-кода.

Расширение On-line PIN Extension определяет требования к процедуре расшифровывания PIN-block в Hardware Security Module.

Расширение CVV2/CVC2 Extension определяет возможность передачи значений CVC2 (Europay/MasterCard), CVV2 (VISA), FDBC (Four Digit Batch Code — American Express), используемых для верификации карт. Дополнительные данные передаются в специально предназначенном для этого поле раздела PI сообщения PReq протокола SET.

Расширение Track 2 Data Extension позволяет ОБ передавать банку-эмитенту три поля со второй дорожки магнитной полосы: Country Code, Service-Code и Discretionary-Data (содержимое данных Discretionary-Data полностью определяется эмитентом), что является очень важным фактором, поскольку некоторые сети и банки используют эту информацию для маршрутизации транзакций, а также их авторизации. Данные Discretionary-Data передаются в специально предназначенном для этого поле раздела PI сообщения Purchase Request протокола SET.

Другие расширения протокола SET уже не носят столь общего характера (например, одно из расширений связано с использованием протокола в некоторых японских магазинах, другое — позволяет ТП использовать SET для работы с ОБ, независимо от того, в каком виде был подготовлен запрос на покупку клиентом и т. п.).

Сравнение протоколов SSL и SET

В табл. 4.5 приведены результаты сравнения протоколов SET и SSL по отношению к наиболее вероятным типам мошенничества в ЭК, перечисленным ранее.

Таблица 4.5. Результаты сравнения протоколов SET и SSL

Тип мошенничества	SET решает проблему?	SSL решает проблему?
Мошеннические транзакции по «правильным» картам	Да	Нет
Злоупотребления магазинов	Да	Нет
Фиктивные магазины	Нет	Нет
Фиктивные банки	Да	Нет
Компрометация данных	Да	Да

Как видно из табл. 4.5, протокол SSL решает только проблему защиты данных о реквизитах карты.

Важным критерием сравнения протоколов является вычислительная мощность (производительность) компьютеров и серверов владельца карты, ТП и шлюза обслуживающего банка (аппаратно-программного комплекса, конвертирующего сообщения ЭК в стандартные сообщения платежной системы), необходимая для реализации того или иного протокола. Дело в том, что противники SET с самого начала говорили о том, что протокол в силу своей перегруженности применением криптографических алгоритмов обладает плохими операционными показателями. Это, в свою очередь, означает, что для внедрения SET требуются более «мощные» серверы ТП и шлюза обслуживающего банка.

Рассмотрим, каким образом используются криптографические операции на компьютере покупателя. Сразу сделаем оговорку, что рассматриваются только операции асимметричного шифрования, поскольку операции симметричного шифрования на два-три порядка быстрее асимметричных алгоритмов.

Далее перечислены операции, выполняемые на компьютере покупателя и использующие алгоритм RSA:

1. Проверка подлинности сертификата ключа Key-Exchange Key платежного шлюза. Сертификат владелец карты получает от ТП в сообщении PinitR.es.
2. Проверка подлинности сертификата ключа Certificate Signature Key PCA платежного шлюза. Сертификат владелец карты получает от ТП в сообщении PinitRes.
3. Проверка подлинности сертификата ключа Certificate Signature Key GCA, подписавшего сертификат ключа Certificate Signature Key PCA платежного шлюза. Сертификат владелец карты получает от ТП в сообщении PinitRes.
4. Проверка подлинности сертификата ключа Message Signing Key ТП. Сертификат владелец карты получает от ТП в сообщении PinitRes.
5. Проверка подлинности сертификата ключа Certificate Signature Key MCA. Сертификат владелец карты получает от ТП в сообщении PinitRes.
6. Проверка подлинности сертификата ключа Certificate Signature Key GCA, подписавшего сертификат ключа Certificate Signature Key MCA. Сертификат владелец карты получает от ТП в сообщении PinitRes.
7. Проверка цифровой подписи ТП. Подпись ТП владелец карты получает от ТП в сообщении PinitRes.
8. Проверка цифровой подписи BCI, полученной владельцем карты от ТП в сообщении PinitRes.
9. Создание подписи (dual message signature) владельцем карты. Подпись вставляется в сообщение Preq, направляемое владельцем карты ТП.
10. Шифрование некоторых данных открытым ключом Key-Exchange Key платежного шлюза. Зашифрованные данные вставляются в сообщение Preq, направляемое владельцем карты ТП.
11. Проверка цифровой подписи ТП, полученной владельцем карты от ТП в сообщении PRes.
12. Проверка цифровой подписи BCI, полученной владельцем карты от ТП в сообщении PRes.

Из перечисленных здесь операций восемь являются обязательными (номера 1,2,4,5,7,9,10,11), а остальные опционными. Например, one-

рации 3 и 6 используются в том случае, когда соответственно PCA и MCA получают сертификаты своих ключей от Geopolitical Level CA. Кроме того, проверка подписей BCI требуется только в том случае, когда список всех CRL данной платежной системы изменился по отношению к списку, хранящемуся на компьютере покупателя.

Далее отметим, что из 12 перечисленных операций только операция 9 имеет дело с шифрованием закрытым ключом. Все остальные операции представляют собой шифрование открытым ключом. Как мы отмечали в главе «Введение в криптографию», операции на открытом ключе существенно (на порядок) быстрее операции на закрытом ключе. Например, типичное время выполнения операций шифрования с помощью RSA на закрытом ключе с модулем 1024 бита на «рядовом» компьютере с тактовой частотой процессора 200 МГц составляет 0,04 с (25 операций в секунду). Аналогичное время в тех же условиях для операции шифрования на открытом ключе равно 0,002 с, то есть в 20 раз меньше.

Таким образом, время, затрачиваемое персональным компьютером покупателя на криптографические операции при реализации протокола SET, составляет примерно 1,51, где t — время, необходимое компьютеру на выполнение шифрования на закрытом ключе.

При использовании покупателем протокола SSL, как это следует из его описания, асимметричное шифрование используется для проверки сертификата сервера (как правило, сертификат сервера получен от одного из корневых центров сертификации), а также для шифрования данных на открытом ключе сервера. Таким образом, асимметричное шифрование на закрытом ключе на компьютере покупателя не осуществляется совсем. Отсюда следует, что время, затрачиваемое компьютером покупателя на криптографические операции при использовании SSL, на порядок меньше аналогичной величины при применении протокола SET. Однако с учетом абсолютного значения этого времени практической разницы для покупателя от того, используется SET или SSL нет!

Аналогичный анализ можно провести для сервера ТП и платежного шлюза. Такой анализ был выполнен в работе Gartner Group «SET Comparative Performance Analysis». Анализ основан на более грубой модели по сравнению с рассмотренной здесь. В частности, модель не учитывает разницу в вычислительных затратах между шифрованием на открытом и закрытом ключах. Кроме того, предполагается, что в протоколе SSL при совершении покупки используются только авто-

ризационные запросы. Считается, что финансовые сообщения, требующие возмещения средств за выполненный заказ, при использовании SSL не применяются, хотя никакой связи между технологией совершения покупки (Single Message Mode и Dual Message Mode) и применяемым при этом протоколом не существует. В то же время в целом анализ дает представление о том, что разница в стоимости серверов ЭК в зависимости от того, какой протокол используется, начинает возникать только при больших объемах ЭК (более 200 транзакций в секунду на сервер). При нагрузке, равной 200-400 транзакций в секунду, разница в стоимости сервера составляет всего 5 %!

В то же время проблема обеспечения производительности серверов при больших нагрузках является актуальной. В этом направлении значительных успехов добились компании Compaq Atalla и Rainbow Technologies.

Остановимся на криптографических устройствах первой компании. Продукты Atalla используются в крупнейших процессинговых центрах мира, обеспечивая защиту финансовых транзакций. Криптографические модули выпускаются в двух видах: PCI-карты и отдельного устройства. Независимо от внешнего вида модули обязательно удовлетворяют стандарту физической безопасности FIPS 140-1 Level 3. Модули защищены специальным корпусом, взлом которого приведет к самоуничтожению всей памяти. Внутри корпуса расположены датчики удара, температуры и напряжения.

Среди различных моделей криптографических устройств для приложений, связанных с Интернетом, наиболее распространены AXL200 и PayMaster. PCI-карта Atalla AXL200 представляет собой математический ускоритель, содержащий 8 отдельных математических сопроцессоров и позволяющий на несколько порядков повысить производительность Web-сервера, использующего SSL. Производительность карты составляет 240 SSL-подключений в секунду. Модуль AXL200 не хранит ключи и потому не является криптографическим модулем (не поддерживает стандарт FIPS 140-1 Level 3).

Устройство PayMaster обеспечивает ускорение и дополнительную защиту решений, использующих протокол SET. Устройство выпускается в виде либо PCI-карты, либо отдельного модуля, подключенного к компьютеру через Ethernet. Модуль работает в операционных средах Windows NT, Windows 2000, Compaq True64 Unix, Sun Solaris. Устройство позволяет осуществлять 43 операции шифрования RSA с ключом 1024 бита в секунду.

Переходные модели от SSL к SET. Концепция Server Based Wallet

Для платежных систем разработана модель плавного постепенного перехода от наиболее популярного сегодня протокола ЭК — SSL к стандарту SET.

Модель SSL End-to-End Payment

Данная модель соответствует наиболее массовой на сегодняшний день технологии проведения транзакций ЭК, основанной на использовании протокола SSL (рис. 4.2).

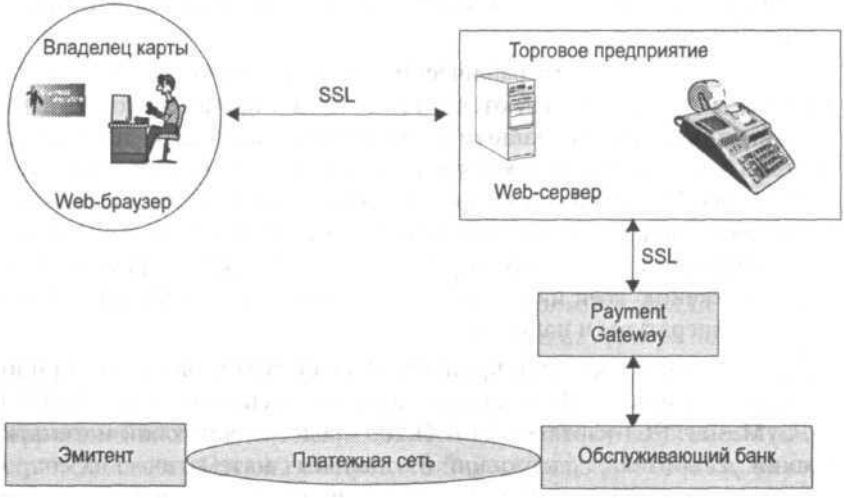

Рис. 4.2. Модель SSL End-to-End Payment

В основе данной модели лежат следующие принципы:

- взаимодействие ТП и покупателя в процессе ЭК осуществляется с помощью протокола SSL;
- взаимодействие ТП и ОБ также происходит с помощью протокола SSL.

Недостатки данной модели с точки зрения безопасности транзакции ЭК подробно обсуждались при описании протокола SSL. Модель рассматривается в качестве отправной точки процесса миграции от SSL к SET.

Модель MOSET (SET 2KP)

Данная модель представляет собой промежуточный этап развития ЭК от SSL к SET (рис. 4.3).

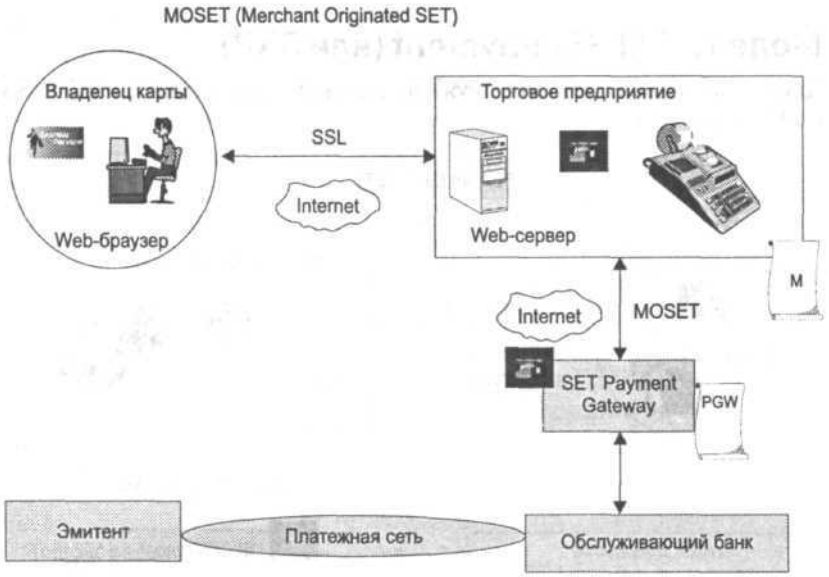

Рис. 4.3. Модель MOSET

В ее основе лежат следующие принципы:

- взаимодействие ТП и покупателя в процессе ЭК по-прежнему осуществляется с помощью протокола SSL;
- взаимодействие ТП и ОБ происходит с помощью протокола SET. При этом ТП и ОБ, представленный в системе ЭК платежным шлюзом, в соответствии с протоколом SET, имеют цифровые сертификаты ключей.

Таким образом, в соответствии с моделью MOSET ТП предает платежному шлюзу сообщения в формате протокола SET (отсюда название модели Merchant Originated SET или 2 Certificate Keepers Model).

Очевидно, внедрять модель MOSET проще, чем «полный» SET, поскольку не требуется решать достаточно сложную задачу распределения клиентского ПО и удаленной сертификации клиентов (для продавцов эта задача не является столь трудной из-за того, что количество их клиентов существенно меньше).

Рассматриваемая модель имеет те же недостатки, что и модель SSL End-to-End Payments. В частности, при ее использовании по-прежнему не гарантирован возврат средств ТП за проведенную в нем операцию электронной покупки.

Модель Full SET Payment (или 3KP)

Данная модель представляет собой конечный этап развития ЭК от SSL к SET (рис. 4.4).

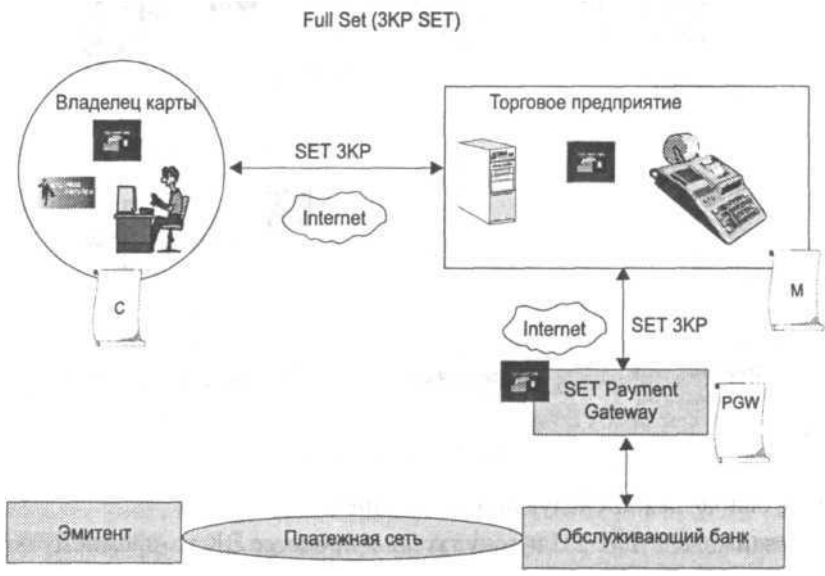

Рис. 4.4. Модель Full SET Payment

В ее основе лежат следующие принципы:

- взаимодействие ТП и покупателя в процессе ЭК осуществляется с помощью протокола SET;
- взаимодействие ТП и ОБ происходит с помощью протокола SET. При этом все субъекты ЭК — покупатель, ТП и ОБ (IPG) имеют цифровые сертификаты ключей (отсюда альтернативное название модели 3KP — Certificate Keepers Model).

Модель 3KP обладает всеми перечисленными ранее преимуществами протокола SET. В частности, в этом случае торговому предприятию гарантируется возврат средств за оказанную им услугу ЭК.

Одна из проблем внедрения протокола SET заключается в сложности задачи распределения клиентского ПО и организации удаленной сертификации клиентов.

Для решения этих задач международные платежные системы рекомендуют банкам-эмитентам использовать в качестве решения для электронного бумажника (Wallet) вместо стандартной модели PC Based Wallet (модель подразумевает установку специализированного ПО на рабочем месте клиента) модель Server Based Wallet.

В соответствии с этой моделью функции SET от лица клиента поддерживаются на отдельном сервере его банка-эмитента (Server Based Wallet). Защищенная связь между банком-эмитентом и клиентом осуществляется с помощью протокола SSL (для надежной идентификации клиента может использоваться любой алгоритм, выбранный банком-эмитентом, например идентификация клиента по User ID+Password). При этом клиент должен иметь ПО Thin Wallet, основные функции которого заключаются в реализации взаимной аутентификации клиента и его банка-эмитента, а также в «переадресации» на сервер эмитента так называемых сообщений wake-up message от ТП. Модель Server Based Wallet показана на рис. 4.5.

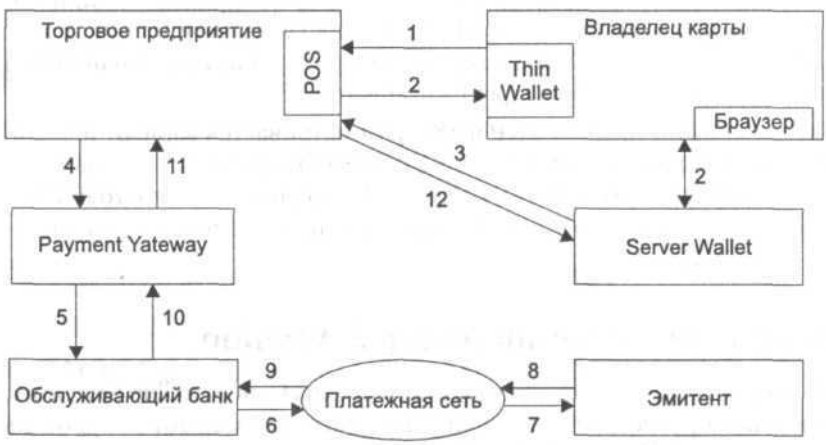

Рис. 4.5. Модель Server Based Wallet

Подход Server Based Wallet имеет ряд важных преимуществ:

- облегчает поставку ПО Wallet клиентам через Интернет; размер бумажника сегодня составляет 2,8-4,5 Мбайт. Это приводит к тому,

что время загрузки ПО довольно велико — 20 минут и более; в то же время ПО Thin Wallet имеет объем до 70 Кбайт со временем загрузки 20 секунд;

- облегчает инсталляцию и использование ПО бумажника (из-за сложности ПО PC Based Wallet по опыту служб поддержки на одну инсталляцию приходится от 2 до 5 звонков клиента);
- повышает безопасность хранения ключевой информации клиента, поскольку решение Server Based Solution использует для хранения закрытых данных специализированные Tamper-Resistant Hardware Security Module;
- упрощает задачу модернизации ПО электронного бумажника (замену текущей версии новой);
- способствует решению задачи совместимости компонентов протокола SET;
- улучшает операционные показатели обработки транзакции ЭК;
- позволяет клиенту использовать различные средства доступа к Интернету (в частности, мобильные телефоны, Set-Top-Box, PDA и т. п.).

Сегодня концепция Server Based Wallet является основной при построении платежных систем ЭК. В частности, эта концепция лежит в основе протокола 3D SET (см. далее), признанного на сегодняшний день основной формой внедрения стандарта SET.

Иногда между моделями 2KP и 3KP рассматривается вариант использования покупателем протокола SET без сертификатов. Этот вариант по своей природе относится к классу 2KP (в данном случае с точки безопасности совершенно все равно, какой протокол использует клиент — SSL или SET).

Модель SET+Common Chip Extension

Эта модель предполагает внедрение расширения Common Chip Extension, описанного ранее. Данное расширение обеспечивает тот же уровень безопасности ЭК, что и Full SET, но помимо того естественным способом решает проблему сертификации открытого ключа покупателя, а также снижает требования к вычислительным характеристикам устройства, поддерживающего электронный бумажник.

Концепция Server Based Wallet, дополненная применением смарт-карт в качестве средства платежа покупателя, является по признанию меж-

дународных платежных систем наиболее перспективной технологией развития ЭК. Смарт-карта является универсальным защищенным средством оплаты товара и может использоваться при проведении транзакции ЭК через все известные на сегодня каналы генерации транзакции, включая PC, STB-устройства, GSM-телефоны.

Важным фактором для распространения использования смарт-карт в ЭК является наличие на рынке дешевых карт-ридеров (считывателей смарт-карт). Сегодня цена такого устройства составляет более $20—30. В рамках международного проекта FINREAD, поддерживаемого банковскими структурами, решается задача разработки относительно дешевого считывателя смарт-карт, стоимость которого не должна превышать $10-15.

Другой важный вопрос — стандартизация интерфейса между смарт-картой и приложением компьютера, использующим смарт-карту. В 1997 г. международной группой компаний (Bull CP8, Gemplus, Hewlett Packard, IBM, Microsoft, Schlumberger, Siemens Nixdorf, Sun Microsystems, Toshiba и VeriFone) были разработаны спецификации PC/SC (Personal Computer/Smart Card). Спецификации определяют среду для использования смарт-карт в персональных компьютерах общего назначения. Они платформонезависимы и могут реализовываться на таких платформах, как Unix, Windows, Mac/OS и т. п.

Модель SSET

Модель SSET будет описана далее и в силу изложенных в том же параграфе причин является наиболее интересной моделью перехода к протоколу SET.

Технологические компоненты электронной коммерции и предлагаемые на рынке решения

Сразу после появления спецификаций протокола SET многие разработчики приступили к созданию реализующего его программного обеспечения. Сегодня на рынке присутствует около 50 программных продуктов, реализующих SET от более чем 20 производителей. Среди лидеров в этом направлении следует назвать компании Globeset (в конце 2000 г. компания была приобретена Trintech), IBM, Hewlett-Packard/VeriFone, Trintech и Brokat.

Все известные сегодня программные продукты ЭК состоят из четырех компонентов: программного обеспечения покупателя — электронного бумажника (Wallet), ТП (POS), платежного шлюза (Payment Gateway) и центра сертификации (Certificate Authority).

Основные функции перечисленных компонентов состоят в следующем:

- Центр сертификации производит регистрацию и сертификацию открытых ключей ТП, владельцев карты и платежных шлюзов. Процедуры удаленной сертификации всех участников транзакции ЭК определены в протоколе SET.
- Электронный бумажник позволяет покупателю выбрать интересующий его товар, произвести его заказ и оплату, а также в дальнейшем получать информацию о статусе выполнения сделанного заказа. Кроме того, электронный бумажник хранит информацию о транзакциях клиента.

Существуют две основные разновидности электронного бумажника — PC-based Wallet и Thin Wallet (клиентская часть в концепции Server Based Wallet). Как уже отмечалось, концепция «тонкого» бумажника сегодня является доминирующей.

Наиболее распространенными платформами для реализации ПО электронного бумажника покупателя являются Windows '95/98/2000, Windows NT 4.0. В табл. 4.6 приведены минимальные и рекомендуемые параметры PC покупателя, необходимые для выполнения электронной покупки.

Таблица 4.6. Минимальные и рекомендуемые параметры компьютера покупателя

Минимальные параметры	Рекомендуемые параметры
* 486 PC	Pentium
* 16 MB RAM	* 32 MB RAM
* 540 MB Hard Disk	* 1 GB Hard Disk
* 14,4 Kb/s Modem	* 28,8 Kb/s Modem
* Colour Monitor	* Colour Monitor

Программное обеспечение ТП обеспечивает оплату товаров по кредитным картам. С одной стороны, это ПО поддерживает связь с электронным бумажником покупателя, а с другой — с платежным шлюзом. Наиболее часто используемые операционные системы для сервера продавца — Windows NT, Unix, OS/2.

Аналогичные платформы используются и для реализации платежного шлюза. Основная функция шлюза состоит в конвертации SET-сообщений в форматы сообщений протокола межхостового обмена ISO 8583, а также в маршрутизации сообщений в процессинговые системы платежных систем и финансовых институтов.

Далее будут рассмотрены решения для системы ЭК таких известных компаний, как IBM, GlobeSet, Hewlett-Packard и ACL

Решение компании ACI

Компания ACI предлагает для организации ЭК использовать программное решение e-24 Commerce Solutions, являющееся объединением решений компании Globeset (в части протокола SET) и ACI (в части протокола SSL).

Решение e-24 Commerce Solutions основано на использовании классической архитектуры системы ЭК. В состав системы входят:

- e24-merchant link, программный компонент, реализующий SET-совместимый интерфейс между электронным бумажником клиента и ТП; компонент инициирует электронный бумажник клиента на проведение оплаты по протоколу SET и обеспечивает проведение оплаты;
- e24-gateway, программная компонента, реализующая интерфейс между платежным сервером (Payment Server) и Acquirer Host; данный компонент осуществляет конвертацию SET-транзакций в формат стандартного межхостового интерфейса ISO 8583;
- e24-wallet, программный компонент, реализующий функции Server Based Wallet;
- e24-registration authority, программный компонент, обеспечивающий генерацию и распределение сертификатов открытых ключей ТП и клиентов банка-эмитента.

Перечисленные выше компоненты дополняются также следующими программными модулями:

- e24-portal, программный компонент, обеспечивающий параллельную обработку транзакций, поступающих от многочисленных ТП, а также доступ ТП к серверам системы ЭК с помощью SSL browser-based-интерфейсов для получения различной информации (например, информации об истории транзакций данного клиента);
- e24-risk, программный компонент, позволяющий обнаруживать мошеннические транзакции ЭК; система является rules-based системой (решение о подозрительности транзакции на мошенничество

принимается на основе проверки предварительно определенного набора критериев), использует несколько критериев анализа транзакции на мошенничество, включая Luhn Check parity-проверку (проверка необходимого условия правильности номера карты), алгоритм VISA Address Verification System, соответствие номера карты имени ее владельца, частотный анализ использования карты, частотный анализ использования отдельных BIN; компонент e24-risk обеспечивает мониторинг транзакций в режиме реального времени, а также предоставляет различные batch-отчеты по результатам мониторинга; ОБ имеют возможность конструировать форму отчетов по своему усмотрению.

Компоненты e24-portal, e24-merchant, e24-risk могут быть реализованы на отдельном сервере, называемом Payment Server. Программный компонент e24-gateway реализуется на другом сервере, называемом Payment Gateway. Наконец, компонент e24-certificate authority реализуется на третьем сервере (также возможно распределение отдельных функций Certificate Authority между серверами электронного бумажника и шлюза).

Решение компании IBM

Компания IBM предлагает для организации системы ЭК использовать аппаратно-программное решение IBM Payment Suite.

Предлагаемое решение является масштабируемым и способно поддерживать систему платежей компании практически любого размера. В состав пакета входят четыре продукта:

- IBM Consumer Wallet;
- IBM Payment Server;
- IBM Payment Gateway;
- IBM Payment Registry.

IBM Payment Server, версия 1.2 (5765-E43) обеспечивает проведение платежей между бумажником покупателя (IBM Consumer Wallet) и ТП через Интернет. Разработанный как составной компонент IBM Payment Suite, сервер платежей IBM Payment Server в то же время работает с различными продуктами в области платежных приложений от других поставщиков, что позволяет создать комплексную систему обработки платежей в Интернете.

Сервер платежей IBM Payment Server управляет записями со сведениями о транзакциях, хранит информацию о платежах и взаимодейству-

ет с финансовыми учреждениями для авторизации платежей, возврате денежных средств, помещении денег на депозиты и прочих финансовых транзакциях.

Сервер IBM Payment Server написан на языке программирования Java и использует модульную архитектуру, что обеспечивает его интеграцию с различными имеющимися у продавцов серверными продуктами и средами деловой обработки данных.

Сервер IBM Payment Server поддерживается на нескольких аппаратных платформах, включая системы IBM AIX, IBM OS/400, IBM OS/390, Microsoft Windows NT и Sun Solaris. Выполненный на базе открытой, основанной на использовании стандартов технологии, сервер IBM Payment Server поддерживает несколько протоколов платежей, включая:

- SET;
- Merchant originated SET (MO SET);
- SSL.

Шлюз **IBM Payment Gateway** (5648-D20 PN И K6384 WebSphere Payment Manager) выполняет функцию посредника между торговыми Web-серверами и финансовыми учреждениями. Payment Gateway поддерживает протоколы SET и Secure Sockets Layer (SSL). Шлюз включает в себя утилиты для преобразования сообщений, поступающих от Интернет-магазинов, в формат ISO 8583. Кроме того, Payment Gateway реализует маршрутизацию сообщений в различные финансовые учреждения.

В основе Payment Gateway лежит комплексное программное обеспечение маршрутизации транзакций, которое использовалось для обработки сообщений в самых различных средах на протяжении более чем десяти лет.

В качестве электронного бумажника покупателя предлагается продукт **IBM Consumer Wallet** (5639-115 PN 11K5996 IBM Consumer Wallet). Бумажник представляет собой приложение, реализующее протоколы SSL и SET, и поддерживает язык ECML, что существенно упрощает для клиента процедуру оформления заказа.

Электронный бумажник позволяет распространять торговую марку любого учреждения с помощью специального настраиваемого процесса работы с торговыми марками.

Бумажник предоставляет простой в использовании графический интерфейс пользователя, содержит встроенные системы справки, поддержки, защиты данных и коммуникации. Бумажник поддерживает различные валюты.

Бумажник предназначается сразу для нескольких пользователей со своими защищенными счетами, каждый из которых может поддерживать различные типы оплаты и торговые марки. Защита счетов обеспечивается с помощью входа в электронный бумажник по паролю и шифрования конфиденциальной информации (например, информации, связанной со счетами пользователей).

Электронный бумажник распространяется на CD-ROM или дискетах.

IBM Payment Registry (5697-C83 IBM Payment Registry 1.2) выполняет функции центра сертификации, поддерживая уровни Geopolitical Certificate Authority, Cardholder Certificate Authority, Merchant Certificate Authority и Payment Gateway Certificate Authority. Решение IBM Payment Registry реализуется на аппаратной платформе RS/6000.

Помимо компонентов, обеспечивающих электронные расчеты, IBM предоставляет решения для Storefront ТП, описанные далее.

IBM Net.Commerce — набор интегрированных между собой программных компонентов, которые представляют собой решение для организации продаж товаров или услуг через Интернет-магазин. Система поставляется с готовыми шаблонами электронных каталогов, мастерами по установке и дополнительными инструментами поддержки каталога, что позволяет создать сайт электронного магазина. Продукт Net.Commerce предоставляет также средства для создания приложений, ориентированных на организацию взаимодействия между компаниями. Семейство IBM Net.Commerce дает возможность:

- управлять процессом регистрации и электронной адресной книгой;
- проверять и обновлять списки товаров;
- контролировать обработку заказов;
- рассчитывать стоимость, налоги и определять конечную цену товара;
- предлагать скидки определенным категориям пользователей;
- отслеживать доставку товара, проверять экспортные ограничения и рассчитывать стоимость грузоперевозок;
- применять различные методы расчета налогов с продаж или стоимость грузоперевозок для различных регионов и международных заказов;
- проверять достоверность платежной информации;
- использовать информацию из локальных баз данных;
- создавать несколько коммерческих серверов на одной **физической** машине.

Продукт **IBM Net.Commerce PRO** является решением для построения Web-сайта крупного электронного магазина. Пакет включает в себя функции IBM Net.Commerce плюс:

- Расширенные инструменты поддержки каталога (Advanced Catalog Tools) позволяют существенно расширить навигацию по каталогу и предоставляют возможность настройки функций просмотра и поиска для отдельных категорий пользователей. Продавец может создать интеллектуальные средства поиска, которые помогут покупателям находить соответствующие разделы каталога.
- Расширенный поиск (Intelligent searching) — позволяет искать с помощью выбора наиболее важных параметров продукта, что очень существенно сужает результаты поиска и сразу отбрасывает все, что не удовлетворяет потребностям покупателя. Покупатель имеет возможность указывать в критерии поиска такие условия, как «равно», «не равно», «диапазон», «больше чем», «меньше чем».
- Средства интеграции — они существенно облегчают процесс интеграции Net.Commerce с такими системами, как Electronic Data Interchange (EDI), IBM CICS, MQSeries, IMS, SAP.

Продукт **IBM Catalog Architect** позволяет управлять каталогом товаров с высокой степенью детализации по сравнению с традиционными способами. Продукт специально спроектирован для поддержки электронной коммерции, основанной на использовании серверного программного обеспечения IBM Net.Commerce. Пакет Catalog Architect может использоваться совместно с IBM Net.Commerce v3.1.2 START или PRO.

Все компоненты решения IBM сертифицированы в SETCo.

Решение компании Hewlett-Packard

Решение компании Hewlett-Packard (HP) Integrated Payment System (IPS) Solution основано на использовании следующих программных компонентов:

- IPS Payment Gateway (функционирует под HP/UX 11.0);
- vPOS (функционирует под Windows NT 4.0);
- vWallet (функционирует под Windows 95, Windows NT 4.0).

Все перечисленные компоненты прошли сертификацию в SETCo и поддерживают специальный Mark Up язык PTML (Payment Transaction Markup Language), созданный на основе языка XML. Язык PTML

позволяет строить эффективное взаимодействие между отдельными компонентами системы, а также обеспечивает развитие системы.

Система IPS полностью соответствует классической модели ЭК, и потому функции ее отдельных компонентов следуют из их названий. В частности, IPS Payment Gateway представляет собой платежный шлюз, vPOS является платежным сервером ТП, а vWallet — PC-based электронным бумажником покупателя.

IPS Payment Gateway для обработки транзакций поддерживает протоколы SET и SSL, выполняет функцию конвертации сообщений из SET/SSL в формат сообщений платежных систем (поддерживаются VISA BASE I, MasterCard ISO 8583, в качестве коммуникационных протоколов используются X.25, TCP/IP), а также функцию маршрутизации транзакций в различные финансовые институты. IPS Payment Gateway способен одновременно обрабатывать до 16 транзакций, что позволяет обеспечить производительность около 300—500 тыс. транзакций в день.

Решение vPOS является полнофункциональным, поддерживая протоколы SSL и SET. Оно легко интегрируется в такие распространенные решения для Storefront, как Microsoft Site Server Commerce Edition, Oracle Merchant Server, iCat и Intershop.

Компания HP не имеет собственного решения для центра сертификации и предлагает решение своего партнера — компании CyberTrust. Данное решение является одним из наиболее полнофункциональных решений для центра сертификации. Центр сертификации CyberTrust поддерживает не только процедуры получения сертификатов, описанные в стандарте SET, но и решает задачи выдачи разнообразных сертификатов для схем SSL, а также для проектов по смарт-картам и т. д.

Компания HP не имеет собственного решения для Server Based Wallet и в качестве такового предлагает решение компании GlobeSet, являющееся по мнению многих экспертов лучшим решением Server Based Wallet в мире.

Решение компании Globeset (Trintech)

Решение компании Globeset основано на использовании следующих программных компонентов:

- центра сертификации Certificate Authority (CA);
- платежного шлюза Payment Gateway;
- платежного сервера ServerPOS;

- сервера эмитента ServerWallet.

Все перечисленные компоненты прошли сертификацию в SETCo.

Центр сертификации Certificate Authority представляет собой SET-приложение для управления сертификатами (генерация, обновления и отзыв сертификатов) торговых предприятий, платежных шлюзов и владельцев карт. Функции GCA (Geopolitical Level в иерархии SET) ЦС не поддерживаются.

Центр сертификации имеет административный интерфейс, позволяющий администраторам получать доступ и конфигурировать CA Databases (поддерживаются БД Oracle, Microsoft SQL Server и Sybase).

Компания Globeset предоставляет пользователям программные модули Software Development Kit (SDK), позволяющие адаптировать центр сертификации под индивидуальные требования банка.

Решение Globeset предлагает пользователям использовать вместе с центром сертификации приложение CA Administration Manager. CA Administration Manager представляет собой Java-приложение, позволяющее:

- стартовать, останавливать и рестартовать сервер центра сертификации;
- конфигурировать лог-файлы сервера, его адреса, порты и БД;
- просматривать лог-файлы сервера;
- добавлять и удалять банки;
- добавлять и удалять карточные продукты.

Центр сертификации поддерживает работу с HSM, использует длины RSA-ключей, равные 1024 и 2048 битов. Центр поддерживает процедуры генерации, обновления и отзыва сертификатов в соответствии с требованиями стандарта SET.

Центр сертификации может функционировать на платформах Windows NT 4.0 и Sun Solaris 2.6.

Платежный шлюз Payment Gateway представляет собой шлюз между платежным сервером и платежной сетью. Шлюз поддерживает протокол SET 1.0 для работы с ServerPOS и несколько различных подключений к хостам обслуживающих банков (допускается, по крайней мере, три соединения по протоколу ISO 8583).

Шлюз Payment Gateway не поддерживает функций мониторинга и контроля безопасности транзакций ЭК. Однако Payment Gateway обеспечивает подключение и адаптацию к службам обнаружения мошенничеств (fraud detection services), поддерживаемых другими приложениями.

Шлюз Payment Gateway поддерживает работу с различными криптографическими ускорителями (cryptographic accelerator) и/или Hardware Security Modules (HSM).

Решение предлагается на платформах NT и Solaris. Имеется поддержка СУБД Oracle, Microsoft SQL Server и Sybase.

Шлюз Payment Gateway поддерживает административный интерфейс, используемый для его конфигурирования, а также для удаленного доступа к функциям Administration Manager. Это позволяет осуществлять запуск, остановку и рестарт сервера, анализировать лог-файлы, конфигурировать порты, БД и т. п.

Компания Globeset предоставляет пользователям программное обеспечение Software Development Kit (SDK), позволяющее адаптировать шлюз под индивидуальные требования банка.

Платежный сервер ServerPOS поддерживает SET 1.0 транзакции. Сервер может функционировать в режиме MOSET, когда в качестве протокола между покупателем и ТП используется SSL.

Сегодня ServerPOS не поддерживает функции мониторинга и контроля безопасности транзакций ЭК (transaction risk detection).

Сервер ServerPOS может функционировать вместе с криптографическими ускорителями и/или Hardware Security Module (HSM).

Сервер ServerPOS поддерживает административный интерфейс, используемый для конфигурирования платежного сервера, а также для удаленного доступа к функциям Administration Manager.

Компания Globeset предоставляет пользователям средства SDK, позволяющие адаптировать платежный сервер под индивидуальные требования банка.

Важнейшее преимущество ServerPOS по сравнению с другими решениями заключается в том, что сервер может обслуживать практически любое количество виртуальных магазинов, сайты которых размещены на различных удаленных серверах. При этом обмен информацией между ТП и ServerPOS может осуществляться через Интернет. Все функции, связанные с реализацией протокола SET, включая получение и хранение сертификатов ключей обслуживаемых ТП, выполняются ServerPOS.

Сервер поддерживает программный интерфейс eLink, позволяющий осуществлять простую интеграцию между merchant storefront и ServerPOS thin-client.

ServerPOS 1.4 поддерживает стандартный набор интерфейсов к системам ТП (merchant adapter):

- Microsoft Site Server Commerce Edition 3.0;
- Vision Factory Cat@log 2.5;
- INTERSHOP4;
- Generic CGI.

Наряду с решением ServerPOS компания Globeset поддерживает решение MPOS, предназначенное для выполнения транзакций ЭК по протоколу SET. Решение предназначено для организации расчетов по транзакциям отдельного электронного ТП.

Компания Globeset предлагает решение Server Based Wallet. ServerWallet может поддерживать и хранить информацию о практически неограниченном количестве карт, а также обрабатывать связанные с этими картами транзакции. Решение допускает распределение входящей нагрузки транзакций ЭК между несколькими серверами.

ServerWallet поддерживает модули HSM и криптографические ускорители для повышения безопасности и производительности операций ЭК. Все криптографические операции выполняются внутри модулей HSM.

С помощью ServerWallet банк-эмитент имеет возможность легко производить модификацию версии тонкого бумажника (thin client), установленного на компьютере владельца карты. Когда клиент для совершения транзакции электронной покупки обращается к ServerWallet, сервер определяет, что поддерживаемая клиентом версия электронного бумажника не соответствует последней, и направляет клиента на специальный сайт за получением новой версии thin wallet.

Сервер ServerWallet использует протокол SSL для защиты коммуникаций между бумажником владельца карты и сервером. Протокол SSL на сервере ServerWallet реализуется с помощью стандартной функции Netscape Enterprise Server или IIS.

Анализ представленных решений

С точки зрения функциональности все рассмотренные решения являются полнофункциональными (поддерживают все компоненты системы ЭК).

Но каждое из предложенных решений обладает своими особенностями.

Только компания Globeset обладает собственным (и, как нам известно из других источников, лучшим на рынке) решением Server Based Wallet.

В решениях HP и ACI в качестве Server Based Wallet используется решение Globeset.

Лучшее и наиболее функциональное решение для центра сертификации предлагает CyberTrust. Как уже отмечалось, это решение может использоваться для решения практически всех известных задач, связанных с PKI.

Что касается платежного сервера, то здесь следует выделить решение Globeset. Концепция «тонкого» клиента, лежащая в основе сервера ServerPOS, обладает теми же преимуществами, что и технология ServerWallet. TIT устанавливает на своем сервере небольшой по размеру программный модуль, обеспечивающий взаимодействие «витрины» магазина с ServerPOS. Вся нагрузка, связанная с реализацией протокола SET, ложится на ServerPOS. В результате ослабляются требования к аппаратным средствам, на которых реализована витрина ТП. Это, а также отсутствие необходимости покупки ПО ТП, реализующего протокол SET, ведет к уменьшению затрат ТП на внедрение SET.

Необходимо также отметить, что концепция «тонкого» клиента для платежного сервера является эталонной в интерпретации компании VISA модели 3D SET, хотя сама по себе концепция трех доменов не требует использования ServerPOS.

Что касается выбора платежного шлюза, то рассмотренные решения для этого компонента ЭК по функциональности примерно одинаковы. Может быть, следует отметить, что по количеству инсталлированных шлюзов мировое лидерство держит компания IBM. Это дает ей при прочих равных некоторое преимущество. Опыт эксплуатации любого программного обеспечения всегда важен для его компании-разработчика с точки зрения учета возможных недостатков, что повышает качество программного обеспечения.

Следует отметить, что среди рассмотренных решений «решения под ключ» (поставка ПО и вычислительных систем) предлагают только HP и IBM. При построении крупномасштабной системы это преимущество может иметь большое значение.

Очевидно, что «лучшее» решение зависит от целей и масштабов проекта. Вполне возможно, что такое решение окажется комбинированным. Например, для крупномасштабного проекта, ориентированного на массового покупателя, решение может быть таким: центр сертификации строится на основе решения CyberTrust, кошелек покупателя — на основе решения Globeset, а остальные компоненты решения и вычислительные средства — на основе решения IBM.

Анализ затрат на создание системы электронной коммерции, окупаемости системы и сроков реализации проекта

Далее приводится приблизительный анализ окупаемости проекта построения полнофункциональной системы ЭК национального масштаба. Очевидно, что окупаемость любого проекта ЭК в масштабе отдельного банка окажется еще более низкой. Поэтому полученные здесь результаты могут рассматриваться как оптимистические оценки окупаемости проекта ЭК.

С организационной точки зрения система ЭК строится на базе двух компаний — Процессинговой компании и Центра сертификации. Приводятся ориентировочные затраты на создание и поддержку функционирования системы ЭК, а также оценки по окупаемости системы. Основные функции Процессинговой компании состоят в следующем:

- в процессинге транзакций, сгенерированных в Интернет-магазинах (захват транзакции и ее доставка соответствующему обслуживающему банку для проведения авторизации);
- в организации подключения Интернет-магазинов к системе ЭК;
- в сопровождении сайтов магазинов (функция Application Service Provider и аутсорсинга на сопровождение электронных магазинов);
- в установке Server-based Wallet для банков-участников системы ЭК;
- в работе с банками по их привлечению в систему ЭК;
- в поддержке аппаратно-программных комплексов ЭК;
- в дистрибуции решений ЭК для торговых предприятий и банков-эмитентов (электронные бумажники, платежные серверы и т. д.).

Примерная структура Процессинговой компании:

- Руководство компании — 1
- Финансовые специалисты — 2
- Юрисконсульт — 1
- Кадры — 1
- Отдел сопровождения прикладного программного обеспечения (ППО) и системных средств — 10
- Отдел по работе с торговыми предприятиями — 15
- Отдел информационной безопасности — 2
- Отдел банковского маркетинга — 4

- Охрана —6

Итого: 42 человека.

Приведем примерный бюджет Процессинговой компании.

Капитальныезатраты:

- построение машинного зала, создание структурированной кабельной сети, приобретение средств связи и телекоммуникаций (LAN/WAN) - $250 000;
- приобретение и инсталляция аппаратно-программных платформ для Internet Payment Gateway, 100 магазинов на 10 Web-сайтах и 5 Server Based Wallet&Certificate Authority - $1 100 000;
- оснащение офисных помещений на 40 человек мебелью, организационной и вычислительной техникой - $80 000;
- PR-акции - $70 000.

Итого: $1 500 000;

Текущиеежемесячныерасходы:

- ФЗП (40 чел. х 900$) - $36 000;
- Налог на ФЗП и подоходный налог - $25 200;
- Плата за поддержку аппаратных средств и программных средств -$10 000;
- Аренда помещений - $10 000;
- Телекоммуникационные услуги - (стоимость канала ежемесячно + трафик) - $3 000;
- Электроэнергия - $500;
- Коммунальные услуги - $200;
- Факсимильная/телефонная связь - $200;
- Канцелярские расходы - $150;
- Реклама, связи с общественностью - $300;
- Накладные расходы (10%) - $6 000;

Итого: - $92 000

Далее рассматривается следующая модель окупаемости системы.

В таблице 4.7 по годам приведены объемы транзакций ЭК, обрабатываемых в системе, а также доходы, получаемые за процессинг (предполагается, что компания оставляет себе 1% от размера транзакции; средний размер транзакций в 2001 и 2002 гг. предполагался равным $ 25,

а та же величина, начиная с 2003 г., в связи с появлением более безопасной инфраструктуры SET, станет равна $50).

Таблица 4.7. Объемы транзакций ЭК

Год	Число тр-й/день	Доход в день,$	Доход за месяц,$
2001	1000	250	7 500
2002	3000	750	22 500
2003	10000	5 000	150 000
2004	15000	7 500	225 000
2005	30000	15 000	450 000

Таблица 4.8. Расходы и доходы компании по годам

Год	Расходы за год, $	Доходы за год, $
2000 (начальные)	1 500 000	-
2001	1 100 000	90 000
2002	1 100 000	270 000
2003	1 100 000	1 800 000
2004	1 100 000	2 700 000
2005	1 100 000	5 400 000
Итого	7 000 000	10 260 000

Как видно из таблицы 4.8, система ЭК окупится в начале 2005 г., а к концу 2005 г. она уже принесет доход в размере $3 млн.

Основные функции Центра сертификации таковы:

- сертификация ключей банков-участников российских платежных систем для проектов ЭК;
- сертификация ключей банков-участников международных платежных систем (от лица этих систем) в проектах ЭК, внедрения чиповых карт, телекоммуникационных проектов;
- сертификация ключей клиентов банка от лица его Центра сертификации.

Примерная структура Центра сертификации компании:

- Руководство компании — 1
- Финансовые специалисты — 1
- Юрисконсульт - 2
- Кадры — 1

- Отдел сопровождения прикладного программного обеспечения (ППО) и системных средств — 3
- Охрана — 6

Итого: 14

Примерный бюджет компании оценивается следующим образом.

Капитальныезатраты:

- построение машинного зала, создание структурированной кабельной сети, приобретение средств связи и телекоммуникаций (LAN/WAN)-$100 000;
- приобретение и инсталляция аппаратно-программных средств ЦС -$850 000;
- оснащение офисных помещений на 14 человек мебелью и вычислительной техникой - $30 000;
- PR-акции - $120 000.

Итого: 1 100 000$

Текущие ежемесячные расходы:

- ФЗП (14 чел. х 1000$)-$14 000
- Налог на ФЗП и подоходный налог - $9 800
- Плата за поддержку аппаратных средств (с учетом амортизации) и программных средств - $10 000;
- Аренда помещений - $5 000
- Телекоммуникационные услуги — (стоимость канала ежемесячно + трафик)-$1000
- Электроэнергия - $300
- Коммунальные услуги - $200
- Факсимильная/телефонная связь - $100
- Офисные расходы - $100
- Реклама, связи с общественностью - $100
- Накладные расходы (10 %) -$2 400

Итого: - $43,000

В табл. 4.9 приведено количество сертификатов, выданных компанией за год, с учетом динамики развертывания системы ЭК и внедрения смарт-карт. В качестве клиентов ЦС рассматриваются только банки-участники платежных систем.

Таблица 4.9. Количество сертификатов, выданных компанией за год

Год	Кол-во сертификатов за год
2001	20
2002	100
2003	200
2004	300
2005	500
2006	700

Таблица 4.10. Расходы и доходы компании по годам

Год	Расходы за год, $	Доходы за год, $
2000 (начальные)	1 100 000	-
2001	520 000	60 000
2002	520 000	300 000
2003	520 000	600 000
2004	520 000	900 000
2005	520 000	1 500 000
2006	520 000	2 100 000
Итого	4 420 000	5 460 000

Как видно из таблицы 4.10, компания, реализующая функции центра сертификации, окупится в середине 2006 г.

Проблемы внедрения SET

Несмотря на технологическое совершенство протокола SET, его внедрение происходит гораздо медленнее, чем предсказывалось экспертами и разработчиками стандарта. Более того, сейчас ведутся настойчивые разговоры по поводу того, что протокол SET уже является вчерашним днем и его шансы на выживание ничтожны.

Такие разговоры начались летом 2000 г., когда VISA International сделала заявление, в соответствии с которым протокол 3D SET (разновидность SET, о которой подробно будет рассказано далее) становится стандартом для стран Евросоюза, Латинской Америки и некоторых других европейских стран, включая Россию. В то же время на самом крупном американском рынке в качестве стандарта был провозглашен протокол 3D SSL (другое название протокола — 3D Payer).

Несмотря на то что ни Europay, ни MasterCard, никакая другая международная платежная система громогласно от SET не отказывались, заявление руководства системы VISA говорит о многом. Понятно, что решение крупнейшей международной платежной системы отказаться от стандарта SET на самом большом рынке ЭК не может не отразиться на решениях других платежных систем.

Очень коротко остановимся на истории SET. Первая транзакция ЭК на базе протокола SET была совершена в декабре 1996 г. через датский межбанковский процессинговый центр PBS. На сегодняшний день в мире насчитывается около 100 000 SET-совместимых карт платежных систем Europay, MasterCard и VISA, а также несколько сотен SET-совместимых ТП. По данным платежной системы VISA проекты по внедрению решения ЭК на базе протокола SET реализованы в 39 странах мира. По данным Europay International на конец 1999 г. в программе по продвижению SET участвовало 55 банков из 17 стран. Общее количество выданных сертификатов составляло 25. SET-платежи принимали 194 торговые точки.

В SET-программе системы MasterCard участвовали 104 банка из 56 стран.

В Европе насчитывается около 50 внедрений протокола SET. Банки и межбанковские организации, включая Euro Kartensysteme (Германия), SSB (Италия), PBS (Дания), Deutche Bank, Dresdner Bank, Credit Agricole и SE Banken потратили приблизительно 50 миллионов евро на имплементацию этого протокола.

Внедрение SET с самого начала сопровождалось возникновением различных проблем. В первые 2-3 года распространения стандарта по миру главной проблемой являлось отсутствие взаимной совместимости (interoperability) продуктов различных поставщиков программных средств, поддерживающих протокол SET. Проблема успешно была решена (и эффективно решается сегодня для новых разработчиков ПО) усилиями компании SETCo и разработчиков ПО. Сегодня на рынке продается около 50 различных решений ЭК, в основе которых лежит протокол SET, более чем от 20 поставщиков программного обеспечения. Компания SETCo организует для поставщиков программных продуктов специальные тесты SET Compliance Testing на совместимость со стандартом SET. Продукты, прошедшие подобное тестирование, получают специальную лицензию SET Mark, свидетельствующую об их совместимости со стандартом. В то же время, совместимость со стандартом не гарантирует совместимости между продуктами, получившими лицензию SET Mark. Список продуктов, успешно прошедших тестирование SET Compliance Testing, можно найти на сайте www.setco.org по

ссылке Derived Products. На том же сайте по ссылке Vendor Status Matrix можно получить информацию о продуктах, находящихся на этапе тестирования SET Compliance Testing.

Проблеме совместимости и сегодня уделяется большое внимание. В ее решении заинтересованы в первую очередь поставщики программного обеспечения, принимающие активное участие в организации тестов на совместимость под эгидой SETCo Technology Advisor Group. Результаты тестирования на совместимость продуктов различных производителей можно также найти на сайте www.setco.org по ссылке Interoperability Database. Тестирование на совместимость продуктов различных производителей проводится на так называемых фестивалях, организуемых SETCo. Во время таких фестивалей, организуемых дважды в год, проводятся попарные тесты на совместимость, результаты которых и заносятся в БД Interoperability Database.

Существуют объективные причины медленного продвижения SET. К ним, в первую очередь, следует отнести высокую стоимость решений, реализующих протокол SET; принимая во внимание наличие уже развитой базы электронных магазинов, применяющих протокол SSL, а также пока приемлемый для торговли уровень мошенничества, магазины не спешат инвестироваться в новое решение. Это хорошо видно на примере Дании, являющейся одним из лидеров по внедрению протокола SET. Уже упоминавшаяся компания PBS при заключении договоров на обслуживание предлагает Интернет-магазинам обе технологии — SSL и SET. На конец 2000 г. PBS заключила 1971 договор на работу по технологии SSL и только 208 договоров на обслуживание по стандарту SET.

Таким образом, в сегодняшних условиях (объемы продаж в ЭК, стоимость продуктов, уровень мошенничеств) в целом продавцы не желают тратить ни время, ни деньги на реализацию решений, обеспечивающих безопасность транзакций ЭК.

В свою очередь, отсутствие инфраструктуры Интернет-магазинов, использующих стандарт SET, сдерживает банки-эмитенты от инвестиций в SET. Кроме того, банки-эмитенты полностью защищены от мошенничеств сегодняшними правилами международных платежных систем (вся ответственность по транзакциям, проведенным не по протоколу SET, лежит на обслуживающем банке). Это также является одной из принципиальных ошибок, допущенных международными платежными системами при внедрении нового стандарта. Только марте 2001 г. до банков дошло решение VISA International, действительное с 1 января

2003 года для стран с базовым протоколом ЭК 3D SET, в соответствии с которым ответственность за мошенничество, совершенное не по SET-карте, в ТП, поддерживающем SET, ложится на банк-эмитент. Такое решение должно серьезным образом стимулировать эмитентов на переход к использованию SET.

Другая ошибка международных платежных систем состояла в том, что для SET-транзакций не были введены специальные значения комиссионных Interchange Fee, выплачиваемых обслуживающим банком в пользу банка-эмитента. Долгое время тарифы оставались такими же, как для неэлектронной операции «покупка» — около 2,5 % от размера транзакции. Только общее уменьшение комиссионных плат в международных платежных системах привело к снижению размера Interchange Fee для электронных покупок (примерно 1,45-1,69 % в зависимости от платежной системы и карточного продукта).

Модели трех доменов

Летом 2000 г. компания VISA объявила о своей поддержке концепции (модели) «трех доменов» (Three Domain Model), суть которой состоит в следующем.

Весь процесс аутентификации, обеспечивающий безопасность транзакций ЭК, разбивается на три домена (области): Issuer Domain, Acquirer Domain и Interoperability Domain (рис. 4.6).

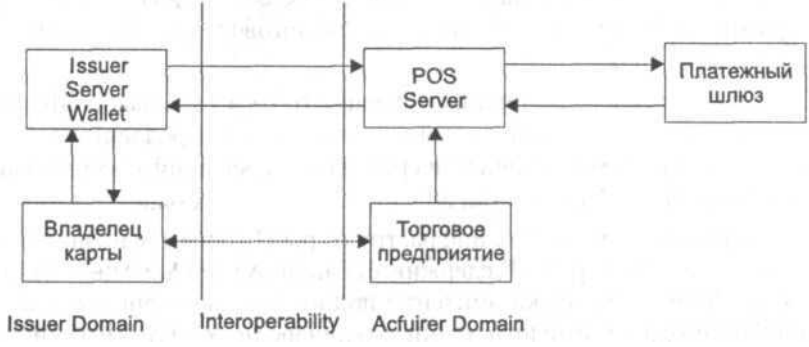

Рис. 4.6. Модель трех доменов (3D)

Назначение Issuer Domain состоит в аутентификации банком-эмитентом своего клиента на основе правил и методов, установленных самим эмитентом.

Назначение Acquirer Domain заключается в том, что обслуживающий банк производит аутентификацию своего ТП на основе правил и методов, установленных самим обслуживающим банком.

Наконец, задача Interoperability Domain состоит в том, чтобы определить правила и процедуры обмена информацией между доменами Issuer Domain и Acquirer Domain, гарантирующие этим доменам взаимную аутентификацию друг друга.

Таким образом, модель трех доменов, разбивая процесс аутентификации участников ЭК на отдельные зоны, сразу ограничивает множество всех протоколов ЭК, определяя лишь некоторое подмножество всех возможных алгоритмов взаимодействия участников транзакции ЭК.

Следует подчеркнуть, что процедуры аутентификации внутри Issuer Domain и Acquirer Domain определяются соответственно банком-эмитентом и обслуживающим банком. Платежная система определяет лишь правила работы в области Interoperability Domain. Таким образом, модель трех доменов ясно определяет ответственность всех участников транзакции ЭК в процессе их аутентификации.

Очевидное преимущество модели трех доменов состоит в том, что эмитент получает возможность производить аутентификацию своего клиента любым удобным ему способом. Например, для этого могут использоваться методы, уже применяемые банком в электронном бэнкинге, или PKI-приложения на смарт-картах.

Недавно компания Еигорау предложила новую оригинальную технологию аутентификации владельца карты, внедрив приложение Wireless Public Key Infrastructure (WPKI) в SIM-карте мобильного телефона. Суть идеи состоит в том, что после того как клиент обратился к серверу своего эмитента для инициализации SET-транзакции, последний организует передачу на мобильный телефон владельца карты SMS-сообщения, содержащего описание товаров, заказанных клиентом. Если клиент согласен с содержимым перечня товаров, он его подтверждает. В результате полученное SMS-сообщение подписывается ключом владельца карты и возвращается на сервер эмитента.

Далее будут рассмотрены два частных случая модели трех доменов: 3D SET и 3D SSL.

Суть модели 3D SET состоит в том, что взаимодействие между доменами эмитента и обслуживающего банка осуществляется по протоколу SET. На практике это означает, что в Issuer Domain реализуется кон-

цепция «тонкого кошелька» с использованием Issuer Server Wallet, который осуществляет аутентификацию клиента по некоторому своему алгоритму и далее направляет в Acquirer Domain сообщения, подтверждающие аутентификацию клиента в формате сообщений протокола SET. В этом случае нет необходимости передачи сертификатов ключей клиентов самим клиентам.

С точки зрения ТП модель 3D SET позволяет ТП выполнить транзакцию ЭК с использованием независимого платежного сервера.

Модель 3D SSL отличается от модели 3D SET тем, что в области Interoperability Domain вместо протокола SET используется протокол SSL. На практике это выражается в том, что после завершения банком-эмитентом процедуры аутентификации своего клиента банк-эмитент подписывает запрос клиента своим секретным ключом и передает его в Acquirer Domain. Тем самым эмитент подтверждает результат аутентификации клиента.

Процедура аутентификации ТП его обслуживающим банком в модели 3D SSL может быть любой (в частности, для этого может использоваться протокол SET или аутентификация ТП может осуществляться по тем же правилам, что и в случае обычной покупки).

Преимущества модели 3D SSL очевидны. Клиенту достаточно использовать обычный браузер для реализации транзакции ЭК. При этом на сервере эмитента Issuer Server не требуется хранение (и тем более распространение) сертификатов ключей клиентов банка. В связи с этим внедрение подобной модели является чрезвычайно простым в сравнении с процедурой внедрения модели 3D SET. В то же время, модель 3D SSL имеет и очевидные недостатки — не обеспечивается конфиденциальность данных о реквизитах карты клиента по отношению к ТП.

Модель 3D Secure

В мае 2001 г. были опубликованы спецификации на стандарт 3D Secure, претендующий на роль глобального стандарта аутентификации в платежной системе VISA. Поскольку рукопись этой книги была передана в издательство примерно в то же время, ниже приводится самое общее описание этого стандарта.

Протокол 3D Secure базируется на концепции трех доменов. Общая схема протокола представлена на рис 4.7.

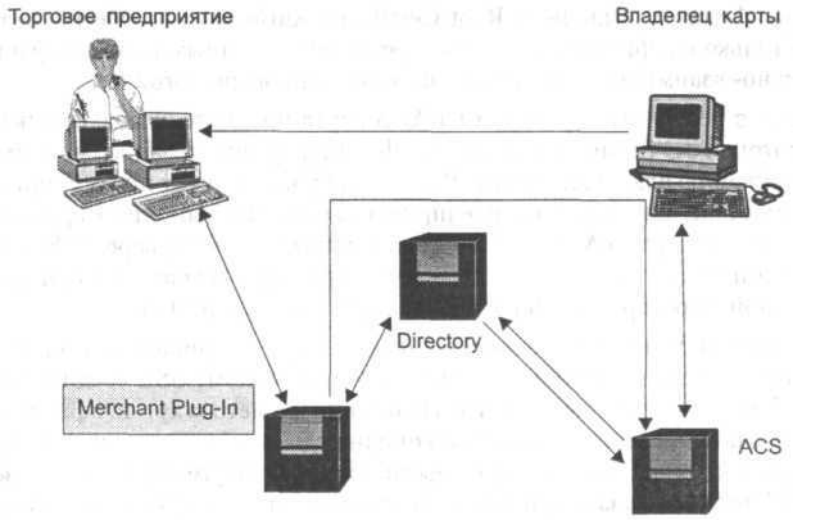

Рис. 4.7. Модель 3D Secure

После того, как владелец карты подтвердил торговому предприятию свою готовность произвести покупку и в защищенной SSL-сессии передал ТП реквизиты карты, приложение ТП инициирует специальное программное обеспечение, устанавливаемое на сервере ТП и называемое Merchant Plug-In.

Программа Merchant Plug-In обращается к серверу платежной системы (Directory) с запросом на проверку поддержки владельцем карты протокола 3D Secure. Данный запрос содержит номер карты, идентификатор торговой точки и ее пароль (опционно). Сервер Directory по идентификатору торговой точки проверяет наличие данного ТП в БД интернет-магазинов, поддерживающих протокол 3D Secure. Кроме того, в случае использования пароля ТП проводится идентификация ТП. После этого сервер Directory по номеру карты покупателя определяет ее принадлежность к диапазону карт, поддерживающих протокол 3D Secure, а также URL сервера эмитента карты, называемого Access Control Server (ACS), и передает по этому URL запрос на поддержку данной конкретной картой протокола 3D Secure. Сервер ACS проверяет поддержку владельцем карты протокола 3D Secure и результат проверки через Directory сообщает программе Merchant Plug-In.

Следует отметить, что диалоги Merchant Plug-In - Directory и Directory - ACS происходят по защищенным SSL-сессиям с использованием SSL-

сертификатов, выданных Root Certificate Authority, что обеспечивает не только конфиденциальность передаваемых данных, но и что крайне важно- взаимную аутентификацию участников диалогов.

Если в результате проверки на ACS карта покупателя поддерживает протокол 3D Secure, то Merchant Plug-In формирует запрос на аутентификацию владельца карты. Данный запрос содержит информацию о сумме покупки, торговом предприятии, специальный идентификатор владельца карты (Account ID), поддерживаемый на сервере ACS, URL ТП и передается на сервер ACS, через браузер покупателя с одновременной переадресацией владельца карты на сервер ACS.

Сервер ACS, получив запрос, производит аутентификацию владельца карты по установленному с клиентом защищенному SSL-соединению. За банком-эмитентом остается свобода выбора метода аутентификации. В частности, владелец карты может однажды получить от эмитента пароль. В этом случае проверка выглядит следующим образом. Сервер ACS подготавливает для покупателя страничку, содержащую логотип банка-эмитента, название ТП, сумму транзакции, специальные позывные (по сути — тот же пароль, но в легко запоминаемой форме), придуманные владельцем карты на стадии его регистрации для участия в программе ЭК банка и хранимые на ACS, а также запрос к покупателю на ввод секретного пароля владельца карты. С помощью позывных сервер ACS идентифицирует себя перед владельцем карты. В ответ владелец карты сообщает серверу ACS свой пароль, идентифицируя себя перед эмитентом.

После успешного завершения аутентификации клиента, сервер ACS подготавливает ответ, подписанный на ключе эмитента. Подпись эмитента используется для решения проблемы потенциального отказа владельца карты от результатов транзакции. Ответ передается на сервер обслуживающего банка с одновременным переключением клиента на этот же сервер. Результат аутентификации передается ACS также на сервер Directory, который выступает в роли третейского судьи в случае возникновения диспута по транзакции. Merchant Plug-In проверяет подпись эмитента и формирует стандартный авторизационный запрос для передачи его в платежную сеть.

Таким образом, протокол 3D Secure удовлетворяет основным требованиям безопасности, предъявляемым к ЭК. В частности, решается проблема аутентификации участников транзакции, отказа от транзакции и т. п. И в то же время говорить о протоколе 3D Secure как об устойчивом протоколе невозможно, поскольку он определяет только часть процесса обработки транзакции (Interoperability Domain), оставляя про-

токолы в зонах Issuer Domain и Acquirer Domain на выбор соответственно эмитента и обслуживающего банка. У протокола 3D Secure имеются следующие очевидные достоинства. Во-первых, в общем случае для совершения транзакции ЭК клиент помимо браузера не должен содержать специального ПО на своем компьютере. Хотя в некоторых случаях наличие электронного бумажника целесообразно. Например, когда эмитент использует более сложные по сравнению с паролями схемы аутентификации владельца карты (например, с помощью смарт-карты и т. п.). Здесь важно, что электронный бумажник предоставляется владельцу карты его эмитентом. Его функционирование никак не регламентируется платежными системами.

Во-вторых, резко упрощается процедура сертификации. В протоколе 3D Secure используется одноуровневая система центров сертификации.

В третьих, и это достоинство всех протоколов, укладывающихся в концепцию трех доменов, процедуры аутентификации ТП и владельцев карты определяются банками и не регламентируются сетью, что дает банкам свободу выбора и возможность интегрирования уже существующих решений (например, в области Интернет-бэнкинга).

Наконец, ПО, устанавливаемое на стороне обслуживающего банка и банка-эмитента, гораздо проще по своей функциональности и потому должно быть существенно дешевле ПО, реализующего SET.

Модель SSET

Как уже отмечалось, ключевыми вопросами для успешного внедрения проекта электронной коммерции являются его стоимость и безопасность операций, обеспечиваемая внедряемой системой. При этом очевидно, что чем выше безопасность системы электронной коммерции, тем выше и ее стоимость.

Использование протокола SET, обеспечивающего высокую степень защиты транзакций ЭК, в мире весьма ограничено (около ста тысяч карт и несколько сотен торговых предприятий). Тому имеется множество причин, решающей среди которых является высокая стоимость внедрения системы ЭК на базе протокола SET (стоимость SET-решения колеблется между $600 и 1500 тыс.).

В результате подавляющее большинство современных систем ЭК используют протокол SSL, обеспечивающий лишь конфиденциальность данных транзакции ЭК при их передаче через сеть общего пользования, но при этом являющийся существенно более дешевым для внедрения.

Как известно, любое SET-решение состоит из четырех программных компонентов — электронного кошелька покупателя, POS-сервера продавца, платежного шлюза обслуживающего банка продавца и центра сертификации (ЦС). При этом наиболее дорогостоящими компонентами решения являются платежный шлюз (от $350 до 500 тыс.) и ЦС (около $200-300 тыс.).

Идея описываемого далее протокола ЭК состоит в исключении из употребления наиболее дорогостоящего компонента решения SET — платежного шлюза и замене его так называемым Интернет-агентом. Основные функции такого Интернет-агента аналогичны функциям платежного шлюза. Однако взаимодействие между Интернет-магазином и шлюзом определяется обслуживающим банком, как это делается при подключении банком к своему центральному компьютеру электронных POS-терминалов. Конечно, на это взаимодействие в значительной степени накладывает отпечаток протокол работы клиента и ТП, о чем еще будет сказано.

Суть идеи заключается в том, чтобы оставить интерфейс между покупателем и продавцом полностью соответствующим стандарту SET, но при этом изменить протокол взаимодействия между торговым предприятием и его обслуживающим банком (такой протокол будет в дальнейшем называться SSET — Simplified SET). Следует отметить, что протокол работы продавца и его банка всегда являлся предметом соглашения продавца и банка и платежными системами фактически не регламентировался (имелись общие требования, реализация которых оставалась предметом договоренности между продавцом и банком). Функции платежной системы всегда состояли в определении интерфейса между банком и платежной сетью.

В случае SET в силу трехстороннего характера этого протокола платежные системы впервые за всю историю своего существования вторглись в область, которую никогда прежде не регламентировали. И в этом состояла одна из главных ошибок. В действительности, было бы достаточно определить формат отдельных элементов сообщений, используемых для обмена информацией между продавцом и обслуживающим банком, для того чтобы остальную часть протокола оставить на усмотрение продавца и его банка. Новые инициативы системы VISA, связанные с провозглашением концепции 3D (трех доменов), является фактически попыткой исправить сделанную ошибку.

Технически протокол SSET выглядит следующим образом. Покупатель передает продавцу сообщение Payment Order и получает в ответ сообщение Payment Response, подтверждающее принятие заказа от поку-

пателя. Весь этот обмен происходит в полном соответствии с протоколом SET и потому на этом этапе производится взаимная аутентификация покупателя и продавца. Позже покупатель может воспользоваться другой SET-транзакцией Purchase Inquiry для того, чтобы узнать статус исполнения сделанного им заказа.

После принятия заказа продавец, вообще говоря, в отложенном режиме (off-line) генерирует сообщение Payment Authorization для отправки его банку-эмитенту (через платежный шлюз и платежную систему) с тем, чтобы получить авторизацию эмитента на проведение безналичной операции продажи товара или услуги покупателю. При этом форматы и алгоритм обмена сообщениями между продавцом и обслуживающим его банком остаются предметом соглашения между продавцом и банком. К информационному обмену между продавцом и его банком предъявляются лишь следующие общие требования:

- сообщение Payment Authorization должно содержать в неизменном виде поля (эти поля без изменения переносятся из сообщения Payment Order), относящиеся к Payment Instructions (эти поля содержат реквизиты карты), и значение dual message signature;
- строго рекомендуется, чтобы сообщение Payment Authorization было подписано продавцом и содержало сертификат открытого ключа продавца;
- ответ на сообщение Payment Authorization должен быть подписан Интернет-шлюзом и содержать сертификат открытого ключа Интернет-шлюза;
- в сообщении от платежного шлюза к ТП должны содержаться список CRL-листов вместе с соответствующими списками отозванных сертификатов.

При выполнении перечисленных требований Интернет-агент сможет извлечь из Payment Instructions реквизиты карты, необходимые ему для формирования сетевого сообщения (сообщения, предназначенного для банка-эмитента), обеспечить целостность передаваемой информации, аутентифицировать покупателя и продавца, а продавец, в свою очередь, сможет аутентифицировать Интернет-шлюз и проверить целостность информации, полученной от Интернет-шлюза.

Транзакция Payment Capture, используемая продавцом для того, чтобы потребовать от обслуживающего банка расчета по транзакции электронной покупки, может быть реализована с помощью механизма предавторизации. В соответствии с этим механизмом транзакция Payment Authorization перед отправкой в платежную сеть преобразуется

в сообщение 0100 (authorization request), которое позволяет «заморозить» сумму, соответствующую покупке, на счете клиента. После выполнения заказа продавец генерирует сообщение 0200 (completion), дебетующее со счета покупателя сумму покупки.

Описанный здесь протокол (точнее, общая схема) SSET с точки зрения безопасности практически эквивалентен протоколу SET (по крайней мере, с точки зрения взаимной аутентификации участников транзакции ЭК и конфиденциальности данных по реквизитам карты для продавца). В то же время, он, благодаря большей свободе, позволяет реализовать взаимодействие продавца и его банка по внутреннему протоколу, что, в свою очередь, существенно уменьшает стоимость внедрения протокола SET.

Протокол SSET очевидным образом позволяет поддержать все известные «расширения» протокола SET 1.0, включая расширение, связанное со смарт-картами (Common Chip Extension).

С точки зрения международных платежных систем транзакция SSET может рассматриваться как транзакция с Electronic Commerce Indicator соответствующим Encrypted Channel, что предполагает, в частности, тот факт, что ответственность за транзакцию в случае возникновения диспута лежит на обслуживающем банке. Однако можно быть уверенным в том, что обслуживающие банки в целях экономии средств на первом этапе будут готовы пойти на использование протокола SSET, понимая, что вероятность мошенничества при его использовании так же мала, как и при использовании SET.

Несколько слов по поводу процедуры управления сертификатами. В первую очередь, необходимо отметить, что для клиентов и ТП эта процедура не меняется никак. Другими словами, как и в случае «чистого» SET эти участники электронной коммерции получают свои сертификаты в режиме реального времени от центров сертификации CCA и MCA, соответственно.

Что касается платежного шлюза, то здесь можно действовать разными способами. Первый способ — оставить все в том же виде, что и в протоколе SET. Второй способ, позволяющий уменьшить программную сложность Интернет-агента (а значит, и его стоимость), — проводить процедуру получения сертификата в режиме off-line. В этом случае платежный шлюз должен получить возможность получения. Второй способ, позволяющий уменьшить программную сложность сертификатов своих ключей в PCA с помощью запросов PKCS#10/PKCS#7. При этом можно получить сертификаты для «запасных» ключей, которые могут

быть оперативно использованы в случае компрометации основной пары ключей.

Функция получения списка BCI и соответствующих ему списков CRL остается без изменений. Эта функция реализуется в режиме off-line и потому не является обременительной с точки зрения сложности программной реализации.

Нужно ли сертифицировать Интернет-агента в компании SETCo на соответствие спецификациям протокола SET. Ответ — нет, если правильно распределить ответственность между участниками транзакции. В частности, если считать, что ответственность за потерю реквизитов карты из-за скомпрометированного ключа платежного шлюза лежит на обслуживающем банке, то сертификации платежного шлюза проводить не нужно.

Что необходимо сделать для того, чтобы протокол SSET можно было использовать? Обслуживающему банку при применении SSET необходимо получить разрешение международных платежных систем на получение сертификата своих ключей на ключах соответствующих систем, а также на выдачу сертификатов ключей продавца и Интернет-шлюза (для Интернет-агента) на своем ключе. Кроме того, платежные системы должны дать разрешение на прием SET-карт в SSET-магазинах. Поскольку ни одно из перечисленных ранее решений платежных систем никоим образом не приводит к какой-либо компрометации конфиденциальных данных участников транзакции ЭК, выдача подобных разрешений является лишь вопросом доброй воли платежных систем.

Каковы преимущества протокола SSET для банков?

- Существенно уменьшаются начальные затраты обслуживающих банков на реализацию протокола SET. За счет этого должна существенно расшириться инфраструктура продавцов, принимающих к оплате SET-карты.
- Расширяется инфраструктура электронных магазинов, обслуживающих SET-карты, что делает интересным для банков-эмитентов эмиссию таких карт.

Предлагаемый протокол является первой ступенькой к реализации протокола SET в полном объеме. С ростом объемов операций обслуживающие банки станут постепенно переходить на SET.

SSET эффективнее альтернативных вариантов, предлагаемых некоторыми платежными системами (например, 3D SSL), поскольку обеспечивает более высокий уровень защиты при разумных затратах на реализацию и допускает в дальнейшем переход на полный SET.

Глава 5. Другие модели построения систем электронной коммерции

Другие аспекты повышения безопасности систем электронной коммерции

Как уже отмечалось ранее, сегодня большинство систем ЭК используют протокол SSL Уровень защиты, обеспечиваемый SSL, таков, что аутентификация владельца карты не производится вообще, а аутентификация электронного торгового предприятия может быть признана с серьезными оговорками. Эффективность ранее обсуждавшихся методов повышения безопасности проведения электронных покупок с использованием протокола SSL (применение различных негатив-файлов, проверка CVV2/CVC2, VISA AVS) является весьма ограниченной.

Что же делать обслуживающему банку, желающему заниматься электронной коммерцией уже сегодня в условиях отсутствия широко распространенных надежных протоколов ЭК? Пожалуй, для нынешнего этапа развития электронного бизнеса существует единственный ответ на поставленный вопрос — руководствоваться набором базовых принципов, выработанных на основе обобщения накопленного опыта работы других банков. Эти принципы носят в основном организационно-административный характер и представлены во многих документах. В частности, в концентрированном виде они изложены в материале компании VISA International «Acquirer Best Practices. Electronic Commerce Fraud Management».

С точки зрения работы обслуживающего банка принципы обеспечения безопасности в электронной коммерции могут быть представлены в виде инструкции по работе банка с ТП. Далее приводится проект подобной инструкции.

В общем случае различаются три этапа работы обслуживающего банка с ТП:

1. Подписание договора с ТП.
2. Контроль функционирования ТП.

3. Разрыв отношений с ТП.

На первом этапе банк получает от ТП заполненную анкету ТП, осуществляет необходимые проверки данных анкеты и принимает решение о подписании договора с торговым предприятием. Заканчивается этап либо подписанием договора на обслуживание ТП банком, либо отказом от сотрудничества с данным ТП. Роль первого этапа является крайне важной. Фактически, только грамотно реализовав этот этап работы с ТП, можно защититься от мошеннических торговых предприятий, создаваемых для «отмывания» украденных реквизитов карт.

На втором этапе производятся регулярное инспектирование ТП, мониторинг показателей, характеризующих его электронные продажи, на основе учета статистики по объему операций и отказов от платежей (chargeback), вычисление размеров страховых депозитов и дополнительные расследования по случаям подозрительных транзакций, а также поддержка различных негатив-файлов (файлов, содержащих информацию о параметрах транзакции, считающихся достаточными для того, чтобы ее отвергнуть). В зависимости от результатов наблюдений за работой ТП, в случае «отклонения» характеристик транзакций от некоторых типовых значений могут приниматься решения о приостановке отправки финансовых сообщений (презентментов) по отдельным подозрительным транзакциям до выяснения причин наблюдаемого «необычного» поведения трафика ТП. На этом же этапе поддерживаются процедуры периодического перевычисления страховых депозитов на основе новых статистических данных о работе ТП, а также принимается решение о возможной приостановке работы ТП.

Наконец, на третьем этапе реализуется процедура расторжения договора с ТП.

Рассмотрим подробнее каждый этап работы обслуживающего банка с ТП.

Этап 1. Рассмотрение заявки на регистрацию электронного торгового предприятия и заключение договора

На данном этапе банк получает от ТП комплект документов, включающий в себя:

- нотариально заверенные копии учредительных документов и Устава, свидетельств о регистрации в МРП и постановке на учет в налоговых органах, а также лицензий/разрешений ТП на заявленные виды деятельности;

- ксерокопии паспортов руководства ТП (директор, главный бухгалтер) и основных учредителей (в случае наличия в составе учредителей физических лиц), а также ксерокопии трудовых книжек вышеуказанных лиц;
- бухгалтерский баланс с отметкой инспекции МНС;
- анкету ТП, заверенную руководством ТП.

Рекомендуется, чтобы анкета ТП содержала следующие сведения:

- торговую марку ТП;
- название юридического лица, выполняющего функции ТП;
- паспортные данные руководителей ТП (директор, главный бухгалтер);
- при наличии «физического» магазина, являющегося основой для электронного бизнеса, фактический адрес ТП;
- URLTn;
- E-mail и контактные телефонные номера для обслуживания клиентов ТП. Контактные телефоны и E-mail ответственных менеджеров, в том числе по вопросам технического функционирования ТП и безопасности;
- IP-адрес сервера, на котором расположен сайт ТП;
- данные о компании-владельце хостинга и его учредителях;
- краткую историю бизнеса ТП (в частности, необходимо указать, работало ли ранее торговое предприятие через другие банки и если да, то почему оно меняет обслуживающий банк);
- подробный перечень предоставляемых товаров и услуг с указанием для каждой услуги или товара разброса в ценах;
- если данное предприятие является биллинговой компанией (через нее обслуживаются несколько ТП, в иностранной литературе также используется термин merchant aggregator), то требуется указать данные по предыдущему пункту для каждого обслуживаемого биллинговой компанией ТП. В идеале банк должен заключать прямой договор на обслуживание с каждой торговой точкой;
- если ТП уже ранее функционировало, указывается средний размер транзакции, количество транзакций, количество chargeback, процент объемов chargeback к общему объему покупок, время функционирования ТП;
- если ТП ранее не функционировало, указываются ожидаемые значения оборотов и количества транзакций;

- наличие (отсутствие) в ТП собственной системы безопасности, системы защиты БД карт клиентов (если таковая ведется), а также системы анализа транзакций на потенциальное мошенничество (предоставляется краткое описание архитектуры системы, используемых алгоритмов и критериев);
- наличие в ТП собственной службы безопасности с указанием ее контактных адресов;
- предложения по предоставлению дополнительных поручительств физических лиц либо иных структур за ТП.

Банк, получив вышеуказанный комплект документов, проводит проверку фирмы по следующим направлениям:

1. Подтверждение факта регистрации фирмы в РФ.
2. Проверка действительности паспортных данных руководителей ТП.
3. Проверка руководства ТП на предмет наличия ликвидного имущества в личной собственности, регистрации на их имя других юридических лиц.
4. Проверка наличия претензий со стороны правоохранительных и налоговых органов к ТП либо к близким к ТП структурам.
5. Проверка наличия лицензий и разрешений на осуществляемую ТП деятельность.
6. Проверка адресов электронной почты и контактных телефонов для обслуживания клиентов.

Банк, получив анкету ТП, выполняет следующие действия:

1. Проверяет соответствие URL и IP-адреса хоста.
2. Устанавливает юридическое лицо, на которое зарегистрировано доменное имя и IP-адрес сервера для сайта магазина (по БД РосНИИРоса).
3. Если ТП торгует физическими товарами, проверяет наличие физического офиса ТП.
4. Если ТП использует услугу хостинга для организации своего Web-сайта, производится проверка информации о компании-владельце хостинга.
5. Проверяет наличие криптографической защиты соединения между владельцем карты и ТП во время ввода данных о реквизитах карты, а также данных о реквизитах карт (требования к защите информации указаны ниже при описании необходимых разделов в договоре банка и ТП).

6. Сравнивает списки продаваемых услуг или товаров из анкеты ТП и по электронной витрине ТП.
7. Классифицирует ТП на предмет его степени риска. К высоко рискованным предприятиям априори относятся Adult Entertainment (развлечения для взрослых), игры в реальном масштабе времени/лотереи (gambling/lottery), магазины, торгующие информацией и ПО, магазины, работающие по схеме ребиллинга (то есть магазины, безакцептно дебетующие на регулярной основе счета своих клиентов, например некоторые биллинговые компании, ISP-провайдеры), предприятия, торгующие дорогостоящей аудио- и видеоаппаратурой и другими товарами, легко реализуемыми мошенниками в реальном мире за наличные, предприятия, оказывающие услуги со значительной задержкой от момента совершения оплаты (например, подписка на различные услуги). По данным исследования компании Gartner Group вероятность возникновения chargeback в таких ТП в среднем составляет 15 %, достигая в отдельных электронных магазинах 30 %. Наоборот, к низкорискованным ТП относятся продажа билетов, книг, CD/DVD-дисков и т. п.
8. Проверяет информацию о ТП по БД международных платежных систем MATCH и NMAS (данные БД содержат информацию о мошеннических и подозрительных ТП).
9. Проверяет наличие на сайте ТП ссылок на «подозрительные» сайты (например, на сайты Adult Entertainment).
10. Проверяет полноту описания потребительских характеристик продаваемых продуктов с тем, чтобы недостаток описания товара/услуги не мог стать причиной для chargeback (например, при описании электротоваров рекомендуется указывать, какие значения напряжения требуются для работы данного товара).
11. Проверяет, ясны ли покупателю процедуры заказа товаров и их оплаты по карточкам. Проверяет наличие на Web-сайте ТП ясной информации о сроках доставки товара.
12. Проверяет наличие на сайте описания процедур возврата покупателю товаров/денежных средств, контактных данных ТП (адрес электронной почты, телефона) для покупателя, описания способов доставки товаров, экспортных ограничений и страны регистрации ТП.
13. Проверяет наличие на сайте ТП информации, объясняющей покупателю процедуры безопасного хранения частной информации о покупателе, а также процедуры, гарантирующие покупателю

невозможность компрометации данных его карты при проведении транзакции.

14. Проводит пробную транзакцию для оценки времени доставки товара и проверки содержимого электронного чека, предоставляемого владельцу карты в качестве подтверждения выполнения транзакции. В электронном чеке должны присутствовать номер заказа, ясный для покупателя идентификатор ТП (это очень важно, поскольку практика показывает, что частой причиной отказа клиента от транзакции является неузнаваемость имени магазина на электронном чеке и в стейтменте о транзакциях), совпадающий с именем сайта ТП, имя покупателя, дата транзакции, размер транзакции и код валюты, код авторизации (Approval Code), контактные телефоны и адреса электронной почты для обращения клиента в случае возникновения вопросов, перечень покупаемых товаров и услуг, тип транзакции (покупка). Требования к электронному чеку хорошо изложены в VISA International Operating Regulations, Volume 1 — General Rules, Exhibit 71 «Electronic Transaction Receipt».

На основе полученных результатов банк принимает одно из следующих решений:

- отказать на запрос торгового предприятия по его обслуживанию в банке;
- разрешить ТП работу с банком с указанием схемы проведения транзакции (ограничений на способ выполнения транзакции) в зависимости от размера транзакции (см. далее) и определением схемы поддержания страхового депозита ТП в банке (в зависимости от степени риска данного ТП).

Возможно применение различных схем проведения транзакций.

Ниже в порядке убывания степени защиты от мошенничества приведены возможные схемы проведения транзакции ЭК:

- Транзакция с реализацией надежной процедуры аутентификации владельца карты, принятой в банке-эмитенте карты. Схема, очевидно, может использоваться только для карт, эмитированных банками, реализующими надежные протоколы ЭК.
- Транзакция, совершаемая в отложенном режиме (то есть в режиме off-line), с проверкой следующих данных: номера карты, срока действия карты, имени владельца карты, CVV2, номера паспорта. Транзакция считается успешной, если эмитент по отдельности подтверждает правильность представленных в запросе обслуживаю-

щего банка данных. В противном случае, даже если эмитент присылает общее подтверждение, транзакция отвергается. В запросе должна специально оговариваться необходимость предоставить результат проверки по каждому элементу реквизитов транзакции. Запрос в банк-эмитент может передаваться разными способами, например с помощью принятой в международных платежных системах так называемой телексной авторизации.

- Транзакция с обязательной проверкой CVV2/CVC2.
- Транзакция с переходом на отложенную авторизацию и обязательным подтверждением номера карты, срока ее действия и имени клиента (проверка CVV2/CVC2 запрашивается, если карта содержит этот параметр, но наличие результата проверки необязательно; в то же время, если в ответе эмитента утверждается, что значение CVV2 неверно, транзакция отклоняется).
- Транзакции с обязательной проверкой только номера карты и срока ее действия.

Для каждого ТП на основании «профиля» торгового предприятия определяются значения X_1 X_2, X_3, X_4, суть которых состоит в следующем:

- если размер транзакции превышает значение X_4, то обязательным является проверка по схеме 1;
- если размер транзакции лежит в диапазоне (X_3,X4, то минимально возможный уровень защиты — схема 2;
- если размер транзакции лежит в диапазоне (X_2,X_3], то минимально возможный уровень защиты — схема 3;
- если размер транзакции лежит в диапазоне (X_1X_2], то минимально возможный уровень защиты — схема 4;
- если размер транзакции меньше X_1, то возможно использовать любой способ (схему) проведения транзакции.

В договоре банка с ТП необходимо отразить следующие аспекты:

1. Должен быть указан профиль магазина (виды продаваемых товаров и услуг). Оформляется в виде приложения к договору, являющемуся его неотъемлемой частью. Должна предусматриваться возможность оперативного удаленного доступа сотрудников обслуживающего банка к БД товаров или описанию номенклатуры предлагаемых товаров и услуг.
2. Обязательство ТП предупреждать обслуживающий банк об изменении «профиля» магазина (появление принципиально отличаю-

щихся по цене и видам товаров). Всякое такое изменение должно оформляться в виде дополнительного приложения к договору.

3. Должна иметься статья, указывающая на то, что ТП обязано проводить любую транзакцию ЭК в режиме реального времени (Floor Limit=0).
4. Должны быть оговорены персональные гарантии учредителей ТП с одновременным заключением отдельного договора поручительства для покрытия расходов, связанных с мошенничествами по ЭК.
5. Должна быть четко оговорена схема поддержания страхового депозита для данного ТП. В соответствующей статье договора должны быть слова о том, что если финансовые потери превышают размер страхового депозита, то банк оставляет за собой возможность замораживания средств из текущих поступлений на счет магазина даже в случае банкротства ТП.
6. Должна оговариваться возможность для банка разрыва договора в одностороннем порядке в случае превышения порога мошеннических операций, совершенных в ТП.
7. В договоре или приложении к нему должен быть указан MCC ТП.
8. В отдельном пункте договора должна оговариваться полная ответственность ТП за хранение реквизитов карт.
9. Должно быть отмечено, что для хранения данных о реквизитах карт могут использоваться симметричные алгоритмы шифрования с длиной ключа не менее 128 битов и/или асимметричные алгоритмы с длиной ключа не менее 1024 битов. Сервер, хранящий данные о картах, может быть подключен к Интернету только через специальные средства защиты сетевого доступа Firewall.
10. Должна быть оговорена процедура защиты данных карты при их передаче между ТП и хостом банка. Необходимо потребовать, чтобы сервер ТП при вводе данных о реквизитах карты поддерживал с покупателем защищенную сессию, организуемую с применением симметричного шифрования с длиной ключа не менее 128 битов; в случае использования для защиты реквизитов карты SSL-сессии ТП должно контролировать размер ключа, поддерживаемого браузером покупателя, и, если последняя меньше 128 битов, отказывать покупателю в проведении транзакции, указывая ему адрес сервера, с помощью которого он может модернизировать свой браузер, обеспечив поддержку симметричного шифрования на ключе длиной не менее 128 битов. При использовании асимметричных алгоритмов шифрования длина ключа должны быть не менее 1024 битов.

11. Должно быть предъявлено требование, чтобы на сайте ТП имелись четкие разъяснения для покупателя по процедурам безопасного хранения частной информации о покупателе, а также процедурам, гарантирующим покупателю невозможность компрометации данных его карты при проведении транзакции. По правилам системы VISA этот пункт должен быть включен во все договоры обслуживающего банка с его Интернет-магазинами до 1 января 2002 г.
12. Должен оговариваться режим регулярных инспекций ТП со стороны обслуживающего банка и всяческая помощь банку в осуществлении таких проверок со стороны ТП.
13. Должны быть определены сроки и механизм предоставления дополнительной информации о проведенных транзакциях по запросу обслуживающего банка.
14. Должна предусматриваться возможность инициализации торговым предприятием расследования по подозрительным с точки зрения ТП транзакциям.
15. Должна быть предусмотрена оплата услуг по мониторингу транзакций ТП. Технология мониторинга должна сообщаться ТП.
16. Должна быть оговорена возможность замораживания средств ТП (задержки платежей в сторону ТП) по транзакциям, находящимся в состоянии проверки специалистами обслуживающего банка.

В договоре или приложении к нему должны быть указаны имена и контактные телефоны (адреса электронной почты) ответственных менеджеров, в том числе по вопросам технического функционирования ТП и безопасности.

Этап 2. Контроль функционирования ТП

I. В целях осуществления контроля за деятельностью ТП необходимо проводить регулярные инспекции ТП специалистами банка.

   Содержание инспекции:

   1. Проверка ассортимента предоставляемых ТП услуг и товаров с использованием ранее сохраненных электронных копий (HTML Source) страниц сайта данного ТП, связанных с описанием продаваемых товаров-услуг.
   2. Проведение специалистами банка контрольных покупок в ТП с целью оценки уровня качества предоставляемых услуг (соответствие описания товара его реальному качеству, сроков поставки товаров, стоимость товара и дополнительных услуг

и т. п.), а также проверки использования торговым предприятием методов защиты данных о карточке во время выполнения транзакции.

3. Создание электронных копий (HTML Source) для новых страниц сайта ТП, содержащих описание продаваемых товаров, услуг.
4. Проверка наличия средств защиты БД карточек ТП и обеспечения защищенности соединений между ТП и владельцем карты.

Результаты инспекции оформляются в виде акта с перечислением нарушенных ТП требований банка и используются банком для осуществления акций, предусмотренных договором с ТП (предупреждение, штраф, разрыв договора и т. п.), либо для получения официальных письменных объяснений руководства ТП.

II. Мониторинг транзакций ЭК на предмет выявления подозрительных транзакций и ТП. По подозрительным случаям банк инициирует и проводит специальные расследования.

III. Подготовка еженедельных статистических данных, необходимых для анализа функционирования ТП (как минимум, количество и объемы операций с разбивкой по платежным системам, уровень chargeback). Ведение негатив-файла (файла исключений) по картам и некоторым другим данным владельцев карт (телефон, e-mail, адрес), для которых имели место сообщения chargeback с Reason Code 83, 79 (VISA) и 37 (Europay).

IV. Ведение БД ТП, с которыми была приостановлена работа, с указанием причины расторжения договора и реквизитов, которые могут быть полезны для распознавания ТП при попытке повторного заключения договора (IP-адрес, URL сайта, Ф.И.О. директоров и учредителей и т. п.). Проведение расследования по подозрительным транзакциям.

V. Расследование инициируется либо по результатам анализа клиринговых файлов международных платежных систем (chargeback), статистических данных по ТП, данных мониторинга транзакций ЭК, либо по запросу ТП.

Причины, по которым может инициироваться расследование:

1. Карта эмитирована иностранным банком, и ее владелец делает покупку в российском ТП, используя российский IP-адрес.
2. Большое количество транзакций по одной карте в день.

3. Большой размер транзакции по отношению к ценовому ассортименту ТП.
4. Маленький размер транзакции по отношению к ценовому ассортименту ТП.
5. Большое количество транзакций по данному префиксу.
6. Слишком высокая активность ТП в терминах количества транзакций.
7. Слишком высокая активность ТП в терминах объема операций.
8. Слишком высокий процент отвергнутых эмитентами транзакций от общего количества транзакций, совершенных в ТП.
9. Высокий уровень chargeback по ТП.

По причинам 1-5:

- банк предупреждает ТП о начале расследования по некоторым транзакциям (если это еще возможно, ТП по этим транзакциям приостанавливает выполнение заказа) и запрашивает у ТП дополнительную информацию для выполнения расследования (имя клиента, адрес доставки, IP-адрес, с которого делалась транзакция); кроме того, банк инициирует обращение ТП к клиенту с извинениями по факту задержки доставки товара;
- банк «замораживает» средства на страховом депозите ТП, если презентмент по транзакции уже был отправлен в сеть; в противном случае — временно задерживает отправку презентмента до окончания расследования;
- банк формирует запрос в банк-эмитент с данными о транзакции (включая полученные от ТП имя клиента, номер карты, размер транзакции и идентификатор ТП, адрес доставки) и просьбой связаться с клиентом для подтверждения правильности транзакции в ограниченные сроки (как правило, не более 10 дней со дня отправки запроса).

По причинам 6-9 банк предпринимает следующие действия:

- выясняет причины роста трафика (банк обращается за разъяснениями в ТП — возможно, ТП запустило новую услугу, пользующуюся спросом, и таким образом рост транзакционного трафика объясним);
- принимает решение по ужесточению схемы проведения транзакции (уменьшение параметров, для которых минимально обязательными становятся более защищенные методы авторизации);

- изменяет страховой депозит ТП и замораживает средства ТП для формирования нового значения страхового депозита.

Расследование может дать следующие результаты:

- банк-эмитент подтверждает факт проведения транзакции его клиентом. В этом случае банк оповещает ТП о возможности выполнения заказа, если он еще не был выполнен, и размораживает сумму транзакции на страховом депозите ТП, если эта сумма ранее была заморожена;
- банк-эмитент отрицает факт проведения транзакции его клиентом. В этом случае банк оповещает ТП о невозможности выполнения заказа, если он ранее не был выполнен. Если презентмент уже был отправлен в сеть, банк подготавливает кредитовый презентмент на сумму транзакции;
- банк не получает ответа от банка-эмитента в пределах отведенного для этого времени. В этом случае, если размер транзакции больше некоторой величины Z, банк принимает решение отвергнуть транзакцию. Об этом оповещается ТП. В случае необходимости банк выполняет действия по формирования кредитового презентмента.

Если размер транзакции меньше величины Z, но больше Y, решение по результату выполнения операции перекладывается на ТП, но при обязательном «замораживании» суммы транзакции на страховом депозите ТП на срок 120 дней (срок, в течение которого эмитент может отправить банку chargeback).

Если размер транзакции меньше величины Y, то решение перекладывается на ТП без замораживания суммы транзакции. Значения Z и Y определяются банком на стадии подключения ТП к системе ЭК.

VI. Вычисление на регулярной основе новых значений страховых депозитов по каждому ТП на основе последних статистических данных о функционировании ТП.

VII. Обновление критериев анализа статистических данных по электронной коммерции на основе информации о текущих требованиях международных платежных систем к деятельности ТП.

Этап 3. Прекращение договора с ТП

Если банк принимает решение о прекращении договора между банком и ТП, то он должен выполнить следующие мероприятия:

- внести ТП в базу данных торговых предприятий, с которыми были разорваны договорные отношения;

- изменить значения параметров в программе мониторинга ТП;
- в случае необходимости сообщить о разрыве договорных отношений с ТП в международную платежную систему.

Виртуальные карты

Идея виртуальной карты основана на том, что во время проведения CNP-транзакции пластиковая карта как физический объект не применяется. Используются лишь реквизиты карты, и совсем необязательно, чтобы они были нанесены на пластик. Поэтому можно выделить отдельные предназначенные специально для ЭК номера карт с сопутствующими им реквизитами и «привязать» к таким виртуальным картам счета с небольшим остатком. В этом случае клиент будет застрахован от крупных потерь, связанных с риском мошенничества в ЭК.

Таким образом, смысл виртуальной карты заключается в том, чтобы психологически «раскрепостить» клиента при совершении электронных покупок. Действительно, карта, которой пользуется покупатель, связана с небольшим по размеру счетом, и потому весь риск покупателя ограничен потерей средств на этом счете.

Использование виртуальной карты удобно для клиента в случае, когда банк-эмитент дополнительно предоставляет ему услуги Интернет-бэнкинга для управления своими счетами. В этом случае клиент в удаленном режиме при помощи только персонального компьютера, подключенного к Интернету, может в режиме реального времени перевести средства со своего «главного» счета на счет, связанный с виртуальной картой, в количестве, необходимом для совершения намеченных электронных покупок.

Требования к виртуальным картам состоят в следующем:

- виртуальная карта должна иметь номер (система MasterCard требует, чтобы номер карты состоял из 16 цифр) и срок действия;
- система MasterCard требует, чтобы с виртуальной картой была связана величина CVC2 (VISA оставляет вопрос использования величины CVV2 для виртуальной карты на решение эмитента карты);
- к виртуальным картам применяются те же правила, что и к обычным картам, за исключением правил, которые связаны с физическими характеристиками карт;
- эмитенты должны понятным для клиента образом передать ему номер карты, ее срок действия и т. п., а также способ ее использования;

- эмитенты должны утвердить выпуск виртуальных карт в соответствующих департаментах сертификации карт международных платежных систем;
- эмитент должен ясно объяснить владельцу виртуальной карты, что она не может использоваться в режиме Dual Mode, когда авторизация производится по виртуальной карте, а презентмент сформирован по обычной карте, привязанной к тому же счету, что и виртуальная карта.

Для того чтобы передать клиенту реквизиты виртуальной карты, эмитент может использовать некоторый физический носитель информации о реквизитах карты (Reference Device — RD). RD по своим физическим характеристикам должен явным образом отличаться от обычной карты. В частности, RD не должен иметь тех же размеров и пропорций, что и обычная карта, содержать голограмм платежных систем, а также магнитной полосы и чипа.

В то же время на физическом носителе должен находиться логотип платежной системы, размеры и цвет которого определяются правилами платежной системой. Дизайн физического носителя, а также иные средства доведения информации о реквизитах карты и правилах ее использования должны пройти обязательную сертификацию в платежной системе.

Другое важное требование международных платежных систем заключается в том, что виртуальная карта может быть выдана:

- владельцу «физической» карты;
- клиенту, не имеющему «физической» карты платежной системы, но имеющему возможность получить ее по его первому требованию.

Эти условия по замыслу платежных систем должны сформировать столь же серьезное отношение банка-эмитента к виртуальной карте, как и к обычной, поскольку ответственность банка за своего клиента-владельца виртуальной карты не меняется по сравнению со случаем владельца обычной карты.

Гута Банк стал первым российским банком, который приступил к эмиссии виртуальных карт платежной системы VISA, получивших название VISA E-c@rd и специально предназначенных для осуществления платежей в Интернете. Проект был запущен летом 2000 г. после того, как компания VISA International завершила сертификацию VISA E-c@rd и официально санкционировала их эмиссию Гута Банком.

Карты VISA E-c@rd предназначены для оплаты через Интернет любых видов товаров и услуг в любых электронных магазинах во всем мире, в том числе для оплаты услуг операторов сотовой связи, Интернет-провайдеров, туристических компаний, предприятий гостиничного бизнеса и т. д. Для проведения других операций (расчетов в обычной торговой сети, получения наличных денежных средств) карта VISA E-c@rd не предназначена.

Платежи при помощи VISA E-c@rd осуществляются следующим образом. Выбрав товар в электронном магазине, держатель карты, находясь в защищенной сессии с сервером ТП, вводит в компьютер номер пластиковой карты и срок окончания ее действия. Далее транзакция обрабатывается по тем же законам, что и любая другая (не ЭК) транзакция.

Пополнять счет, связанный с картой VISA E-c@rd, клиенты могут путем внесения наличных денежных средств через кассы в филиалах Гута Банка, через систему Интернет-бэнкинга Телебанк, посредством перевода средств с других счетов (в том числе и карточных) в Гута Банке, а также через перевод средств со счетов в других банках.

Карта VISA E-c@rd Гута Банка выдается сроком на 6 месяцев. Стоимость обслуживания карты составляет $2 за полгода.

Еще одним участником проекта является один из ведущих российских Интернет-провайдеров компания «МТУ-Информ». «МТУ-Информ» будет обеспечивать распространение карт VISA E-c@rd среди своих клиентов. При помощи карты VISA E-c@rd клиенты «МТУ-Информ» могут в режиме реального времени оплачивать услуги доступа в сеть Интернет, аренды программного обеспечения, Интернет-телефонии и т. д.

Виртуальную карту Eurocard/MasterCard Virtual в системе MasterCard эмитирует и другой российский банк — Альфа-Банк. Открытие карты в этом банке обходится ее владельцу в $2, стоимость годового обслуживания карты равна $3. Минимальный первоначальный взнос при открытии карты составляет $20.

Технология Eurocard-MasterCard Virtual Card реализуется в 40 банках, расположенных в 8 странах. Среди банков, использующих эту технологию, два крупнейших испанских банка — La Caixa и BSCH, турецкие банки Citibank и Garanti Bank, португальский банк Unicre и другие.

Ключевым фактором в реализации программ виртуальных карт является небольшое время, необходимое международным системам и банкам-эмитентам для их запуска. Сегодня это время оценивается в две недели.

Близкой по своей идее к виртуальной карте является скрэтч-карта. Скрэтч-карта представляет собой предоплаченный продукт, предназначенный для оплаты услуг того или иного провайдера. Приобретая такую карту, клиент может постепенно тратить денежную сумму, предоплаченную им при покупке карты, в различных целях. Для этого, очевидно, должен существовать авторизационный центр, контролирующий расход средств, связанных со скрэтч-картой.

В виду отсутствия универсальной инфраструктуры приема скрэтч-карт эмиссионный центр скрэтч-карт должен заключать договоры с торговыми предприятиями, которым он должен гарантировать возмещение средств за покупки по скрэтч-картам.

Для обеспечения расчетов с торговыми предприятиями эмиссионный центр должен сотрудничать с кредитными организациями.

Виртуальные номера карт

Идея виртуальной карты получила развитие в технологии виртуального номера карты (используются также термины pseudo card number и proxy card number). Суть этой технологии заключается в том, что при заполнении формы торгового предприятия во время операции ЭК владелец карты вместо реального номера карты сообщает Интернет-магазину некоторый случайный номер. После того как транзакция поступает в систему эмитента для авторизации, производится обратное преобразование виртуального номера карты в реальный номер. В результате при выполнении операций ЭК реальный номер карты никогда не передается в платежную сеть и остается в системе эмитента. Таким образом, вероятность компрометации реальных номеров карт, а также вероятность успешного совершения транзакции ЭК мошенником становятся близкими к нулю.

Технически идея виртуального номера карты может быть реализована следующим образом. Клиент для оплаты электронных покупок с помощью технологии виртуального номера карты должен установить на свой компьютер специальное ПО. После того как клиент получает от Интернет-магазина для заполнения форму, содержащую информацию о реквизитах карты, ПО клиента инициирует обращение к системе своего эмитента. Эмитент генерирует для клиента виртуальный номер карты и возвращает его клиенту. При этом эмитент контролирует в некотором смысле уникальность сгенерированного номера карты, а также принадлежность префикса карты к выделенному для эмитента диапазону значений BIN.

После этого транзакция выполняется обычным образом. Клиент направляет Интернет-магазину заполненную форму, в которой в качестве номера карты фигурирует виртуальный номер. В результате выполнения стандартных процедур обработки транзакции в системе обслуживающего банка и платежной системы из последней в систему эмитента поступает авторизационный запрос, содержащий виртуальный номер карты. Эмитент, получив авторизационный запрос, устанавливает соответствие между данными, сгенерированными при инициализации транзакции, и данными авторизационного запроса. Соответствие ищется по целому ряду параметров. Например, система MasterCard к обязательным параметрам относит номер карты, срок ее действия, имя магазина (Merchant Name), идентификатор магазина (Merchant ID), сумму транзакции и валюту транзакции. Эмитент определяет реальный номер карты, выполняя обратное преобразование, проводит с его использованием авторизацию транзакции и результат возвращает в платежную сеть, предварительно вновь подставив в авторизационный ответ виртуальный номер карты.

Если в платежной системе используется технология Single Message System (авторизационный запрос является одновременно и финансовым сообщением, требующим от эмитента возмещения средств), то процесс на этом завершается. В случае применения технологии Dual Message System (процедуры авторизации и расчетов разделены) система эмитента будет обязана также обработать клиринговое (финансовое) сообщение, связанное с рассматриваемой транзакцией. При обработке клирингового сообщения требуется выполнить необходимую подстановку реального номера карты вместо виртуального номера.

Достоинство идеи виртуального номера карты уже отмечалось. Вероятность мошенничества при реализации идеи эмитентом практически равна нулю. При этом технология работы платежной системы никак не затрагивается, начиная с уровня торговой точки — те же протоколы, форматы сообщений и т. п.

В то же время, идея виртуальных номеров карт имеет и ряд недостатков.

Во-первых, как уже упоминалось, владелец карты должен установить на своем компьютере специальное ПО, называемое электронным кошельком. Обычно это делается путем «скачивания» кошелька с некоторого Web-сервера. Для некоторой категории клиентов такая процедура сама по себе представляет проблему.

Во-вторых, эмитент должен предложить клиенту процедуру его аутентификации во время обращения клиента за виртуальным номером в систему эмитента. Как правило, используется система паролей —

клиент в защищенной сессии с системой эмитента сообщает последней свой идентификатор и кодовое слово (пароль). Здесь существуют несколько подходов к решению задачи. Наиболее надежным является получение клиентом своих идентификатора и пароля непосредственно в банке (в крайнем случае письмом из банка, причем идентификаторы клиента должны распечатываться в PIN-конверте для того, чтобы сделать информацию закрытой для банковского персонала).

Этот подход является неудобным для клиента. Поэтому на практике находит применение другой, менее надежный метод. Клиент получает свои идентификаторы во время первой сессии с системой эмитента. Он идентифицирует себя, представляя эмитенту реквизиты карты, а также дополнительную информацию, запрашиваемую эмитентом (например, номер паспорта, девичью фамилию матери и т. п.). В ответ в случае положительного результата аутентификации клиент получает свой идентификатор и пароль. Весь обмен информацией между клиентом и системой эмитента происходит в защищенной сессии. Логическое соединение с системой эмитента обеспечивается кошельком клиента. Более низкая защищенность этого метода связана с тем, что в процессе идентификации клиента могут быть различные подставки со стороны мошенников, имитирующих работу эмитента.

В-третьих, помимо виртуального номера карты система эмитента в некоторых случаях должна в режиме реального времени генерировать значения CVC2/CVV2. Напомним, что в системе MasterCard использование CVC2 в транзакциях ЭК коммерции является обязательным.

Конечно, эмитент, применяющий технологию виртуальных номеров карт, может и не проверять значения CVC2. В этом случае в платежную сеть может направляться любое случайное значение CVC2. Однако при таком подходе эмитент лишается возможности использовать резервную авторизацию (авторизацию Stand-in), предоставляемую в его распоряжение многими платежными системами на случай отказа в работе системы эмитента. В режиме резервной авторизации платежная сеть от лица эмитента в соответствии с параметрами, установленными эмитентом, производит авторизацию транзакции. В системе резервной авторизации существует общий параметр для всех префиксов карт, определяющий действие эмитента на случай неверного значения CVC2/CVV2 — отклонить транзакцию сразу или продолжить другие проверки. Если такой параметр установить равным значению, означающему «не отклонять», то и по всем другим операциям и префиксам будет приниматься то же решение, что наверняка противоречит интересам эмитента.

В-четвертых, применение технологии виртуальных номеров карт повлечет за собой проблемы для тех Интернет-магазинов, которые сохраняют номера карт клиентов, уже однажды обращавшихся в торговое предприятие за услугами, чтобы не заставлять клиента набирать свои реквизиты при следующих обращениях в ТП. Очевидно, что при массовом применении технологии виртуальных номеров карт БД таких магазинов быстро переполнятся, что повлечет за собой операционные проблемы в их функционировании.

У Интернет-магазинов имеются и другие проблемы. Например, если клиент совершил в одном и том же магазине в течение относительно короткого интервала времени две транзакции на одинаковую сумму, то при необходимости провести операцию «возврат покупки» будет неясно, какой номер карты подставлять в транзакцию возврата. Это связано с тем, что в системах торгового предприятия в качестве ключа для поиска транзакции, как правило, используется номер карты и сумма транзакции. Поэтому, если клиент не может назвать точное значение номера карты, существует вероятность того, что при формировании возврата будет подставлено неправильное значение номера карты и в учетной системе магазина появится неправильная запись — будет «возвращен» не тот товар со всеми вытекающими последствиями для подсистемы управления запасами магазина и т. п.

Наконец, использование виртуальных номеров карт влечет за собой и проблемы в системах эмитента. Необходимость хранения информации обо всех используемых номерах карт — одна из них.

Впервые идея виртуального номера карты в статическом варианте была реализована банком First Virtual, который предлагал своим клиентам для транзакций ЭК использовать идентификатор VirtualPIN. Этот идентификатор вводился клиентом вместо номера карты и Интернет-магазин передавал его на сервер First Virtual, который преобразовывал идентификатор в соответствующий номер, и дальше транзакция обрабатывалась стандартным способом. Таким образом, реализовывалась ограниченная защита номера карты от магазина-мошенника. В технологии First Virtual магазин не знает настоящего номера карты. При этом он может использовать идентификатор клиента для проведения транзакций ЭК из торговых предприятий, поддерживающих эту технологию.

Сегодня технология виртуальных номеров карт получила распространение среди ряда крупных банков. Например, четвертый по размеру американский эмитент пластиковых карт Discover предлагает 50 мил-

лионам своих клиентов услугу Discover DeskShop. В основе Discover DeskShop лежит технология виртуальных карт в реализации ирландской компании Orbiscom (www.orbiscom.com). Решение этой компании O-power используется не только в Discover, но и в банках MBNA (система MBNA Shopsafe, создается для пользования 45 млн владельцев карт), HFC (английский филиал компании Household International) и Allied Irish Banks.

Система O-power для случая 16-цифрового номера карты и 6-цифрового BIN карты генерирует до 1 млрд различных значений виртуальных номеров карт (в терминах Orbiscom — Controlled Payment Number). Период повторного использования виртуального номера карты в системе — 9-12 месяцев.

Для банка Discover система O-power реализована на базе высокопроизводительных серверов E450 компании Sun Microsystems, технологии Oracle и известного программного обеспечения для «свитча» платежной системы Oasis. Клиенту DeskShop достаточно ввести свой пароль для того, чтобы система эмитента заполнила для клиента платежную форму магазина (для этого необходимо, чтобы магазин участвовал в проекте Discover).

Компания Orbiscom не поставляет решений для электронного кошелька клиента. Внедрение технологии виртуальных номеров карт на стороне клиента остается задачей банка-эмитента. При этом может применяться уже используемый электронный кошелек.

Другое известное на рынке решение Nexus-1 предлагается американской компанией Appletix (филиал компании по разработке программных продуктов располагается в Израиле). Клиентами этой компании являются крупнейший канадский банк CIBC (4 млн владельцев карт на начало 2001 г.) и процессинговая компания VISA Israel Credit Cards. Решение Nexus-1 предлагает двухфакторную аутентификацию клиента — аутентификацию клиента по его паролю и аутентификацию компьютера клиента по некоторому специальному алгоритму.

Решение на основе виртуальных номеров карт предлагает также компания Cyota (www.cyota.com).

В конце первого квартала 2001 г. платежная система Maestro (оператор дебетовых карт Maestro) объявила о том, что банки, эмитирующие эти дебетовые карты, могут использовать для реализации систем ЭК технологию виртуальных номеров карт (e-Wallet Maestro solution). Карты Maestro начнут приниматься некоторыми наиболее известными Интернет-магазинами начиная с третьего квартала 2001 г.

Требования к технологии виртуальных номеров карт при использовании карт Maestro состоят в следующем. Эмитент должен генерировать 16-цифровые номера карт (при этом виртуальный номер карты может совпадать с реальным номером карты), а также проверять соответствие между данными, сгенерированными при инициализации транзакции, и данными авторизационного запроса. Как указывалось ранее, соответствие ищется как минимум по номеру карты, сроку ее действия, имени магазина (Merchant Name), идентификатору магазина (Merchant ID), сумме транзакции и валюте транзакции.

Отличительная особенность решения для карт Maestro заключается в том, что владелец карты не должен устанавливать на своем компьютере никакого специального ПО (электронного бумажника). Транзакция выполняется следующим образом. После того как владелец карты сообщил ТП о готовности платить с использованием карты Maestro, Интернет-магазин отправляет на сервер эмитента (e-Wallet в терминах Maestro), хранящий информацию о реквизитах своих карт, специальное сообщение. Это сообщение содержит информацию о ТП (Merchant Name, Merchant ID), о сумме и валюте покупки, идентификатор транзакции в системе ТП и т. п. Одновременно сервер магазина переключает владельца карты на сервер эмитента.

Сервер эмитента устанавливает с владельцем карты защищенное соединение и направляет клиенту форму для проведения его аутентификации. Например, эмитент может запросить у владельца карты ранее предоставленные ему идентификатор и пароль.

После того как владелец карты аутентифицирован сервером эмитента, последний формирует запрос на сервер ТП, содержащий сгенерированный эмитентом виртуальный номер карты. Далее транзакция производится способом, описанным в начале этого параграфа.

По решению Maestro имеется несколько вопросов, ответы на которые явно не следуют из официального описания схемы. Во-первых, не определено, каким образом ТП узнает адрес сервера эмитента карты Maestro. В простейшем случае ТП знает адреса серверов эмитента для некоторого ограниченного набора префиксов (локальное решение). В общем случае необходимо создавать некоторую централизованную директорию адресов, и в этом случае ТП должно обращаться к серверу директории, который уже маршрутизирует запрос на сервер эмитента.

Второй вопрос связан с необходимостью определения спецификации интерфейса между ТП и сервером эмитента. Речь идет о семантике и синтаксисе сообщений, которыми обмениваются ТП и сервер эмитента.

Распределение ответственности при возникновении диспута по транзакции ЭК ничем не отличается от того, каким образом оно производится при использовании модели трех доменов.

Другие решения по расчетам на базе пластиковых карт

О некоторых других схемах проведения транзакций ЭК, повышающих безопасность платежей, говорилось ранее. Безусловный интерес представляет идея применения ПИН2, реализованная для банков-участников платежной системы STB CARD. Идея проста в реализации и эффективна с точки зрения защиты электронных платежей от мошенников.

Об идее системы банка First Virtual также уже коротко говорилось в предыдущем параграфе. Суть идеи состоит в том, чтобы вместо реального номера карты ее владелец при инициализации транзакции ЭК представлял некоторый код, называемый VirtualPIN, которой, в свою очередь, на платежном сервере First Virtual заменяется на реальный номер карты. В результате ТП не видит реального номера карты и не хранит его в своих БД, что понижает шансы мошенников на успех. Кроме того, даже если мошенникам удастся украсть БД VirtualPIN, это не будет иметь для эмитентов карт столь серьезного значения, поскольку эту БД можно просто обновить — перевыпускать карты клиентам не понадобится. Более того, обновление БД VirtualPIN целесообразно для повышения безопасности электронных платежей.

Для реализации схемы от клиента ничего не требуется, кроме того, что он должен запомнить свой VirtualPIN. Процедура эмиссии и периодического обновления VirtualPIN может строиться различным образом. Например, при первом обращении в систему клиент может быть предупрежден о том, что в следующий раз ему для проведения покупок через Интернет нужно использовать определенное значение VirtualPIN.

Идея VirtualPIN реализует защиту транзакции ЭК со стороны обслуживающего банка. Это снижает область ее применения только Интернет-магазинами, обслуживаемыми только этим обслуживающим банком. С другой стороны, от клиента, как правило, использование такой защиты не требует больших усилий. Другими примерами повышения безопасности транзакций ЭК со стороны обслуживающего банка являются системы CyberCash и VeriFone. Поскольку системы во многом напоминают друг друга, расскажем подробнее об одной из них, а именно о системе CyberCash.

Общая схема функционирования системы показана на рис. 5.1.

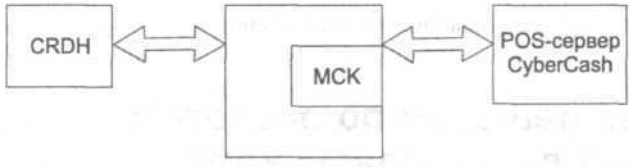

Рис. 5.1. Система CyberCash

Основная идея системы CyberCash заключается в организации виртуального POS-сервера для подключения к нему Интернет-магазинов. В этом случае ТП на своем сервере должно имплементировать небольшое приложение, называемое Merchant Connection Kit (MCK), с помощью которого устанавливается надежное соединение с POS-сервером CyberCash, называемым также CashRegister. Весь трафик между MCK и POS-сервером шифруется с помощью алгоритма Triple DES, что обеспечивает защищенную передачу реквизитов карты и данных транзакции через Интернет. С другой стороны, POS-сервер подключен к платежным системам в соответствии со стандартными протоколами межхостовых соединений.

Системы расчетов, не использующие технологию пластиковых карт

Системы электронной наличности

Идея электронных наличных появилась более 10 лет назад. В 1980-х годах голландец Давид Шаум (David Chaum, после переезда в США чаще именуемый на англо-американский манер Дэвидом Чомом) получил патенты на разработанные им криптографические алгоритмы «слепой подписи», которые закладывали фундамент для альтернативы всем существовавшим системам платежей. Протоколы Чома позволяли создавать виртуальные электронные монеты, которые могли циркулировать подобно деньгам в онлайновой среде, абсолютно никак не раскрывая личности своих хозяев.

Сначала в Нидерландах, а потом и в США Чом основал компанию DigiCash, предназначенную для распространения технологии электронной наличности. В 1995 г. были запущены первые реальные проекты, когда систему электронных наличных лицензировал американский

банк Mark Twain, а также несколько крупных банков и компаний в Европе, Австралии и Японии.

Сама идея электронных наличных очень проста. Система электронных наличных оперирует электронными монетками, каждая из которых представляет собой файл-обязательство эмитента системы, подписанное цифровой подписью эмитента. Клиент обращается к эмитенту, отдает ему некоторое количество реальных денег и получает взамен некоторый файл-монету, который подтверждает тот факт, что эмитент должен клиенту соответствующую сумму денег. При наличии авторитетного эмитента такой файл ничем не хуже обычных денег. Более того, схема электронных наличных обладает грандиозным преимуществом перед обычными деньгами. Файл-монету можно передать по Интернету (или другим способом, например на дискете), осуществляя платеж, и получатель может обналичить его у того же эмитента или его доверенного лица.

Хотя система Чома сама по себе не использовала систем клиринга, схема, применявшаяся в банке Mark Twain, позволяла продавцу пересылать электронные наличные обратно в банк, чтобы гарантированно оградиться от двойной траты электронных монет. Во время клиринга банк аннулировал электронные деньги и переводил на счет продавца соответствующую сумму денег.

Несмотря на высокий интерес к новой системе, проявившийся в основном среди специалистов-криптографов и активистов-правозащитников, усмотревших в полностью анонимных расчетах DigiCash весьма мощный инструмент обеспечения приватности, коммерческий успех компании не сопутствовал. В условиях отсутствия спроса на предлагаемую технологию и недостатка финансирования в ноябре 1998 г. компания DigiCash была вынуждена объявить о своем банкротстве.

По мнению аналитиков, сама по себе идея электронных денег весьма привлекательна и в конечном итоге может быть принята крупнейшими мировыми финансовыми рынками. Однако в период ее внедрения, в 1996—1997 гг. пользователи Интернета еще не были в достаточной степени мотивированы заботой о своей анонимности, чтобы породить тот спрос на технологию, которого ожидали ее создатели.

В случае с DigiCash покупателям по сути дела не предоставлялось никаких финансовых стимулов к переходу на новую систему. Наоборот, электронные монеты в отличие от банковских счетов не приносили их владельцам никаких процентов. Более того, существовала постоянная угроза компрометации «бумажника» клиента на его персональном компьютере. Повышенный риск ощущали и продавцы, поскольку су-

шествовала угроза двойной траты электронных монет, хотя клиринговая система банков обещала свести потери от этого к минимуму.

Сегодня преемником дела DigiCash стала компания eCash Technologies, выкупившая все активы обанкротившейся фирмы и в марте 2000 г. объявившая о намерении продолжить внедрение электронных наличных.

Коротко остановимся на технологических аспектах применения электронной наличности. Еще раз повторим, что электронная наличность — это цифровые данные (последовательность бит) специального вида, эмитируемые банком. Цифровые данные включают в себя идентификатор электронной монеты (купона), денежный номинал монеты и цифровую подпись банка, эмитировавшего монету.

Процедура эмиссии цифровой монеты в общих чертах выглядит следующим образом. Клиент, имеющий счет в банке, направляет в банк запрос об эмиссии ему монеты определенного номинала взамен соответствующей суммы денег, находящихся на его счете. Для этого клиент генерирует некоторую случайную цифровую последовательность, представляющую собой идентификатор монеты, и добавляет к ней номинал монеты. Получившуюся в результате последовательность (обозначим ее a) клиент с помощью некоторой хэш-функции h(x) преобразует в значение h(a). Далее на своем компьютере клиент вычисляет значение $R=h(a)\times b^e \pmod N$, где e — экспонента открытого ключа его банка (банк для подписи использует алгоритм RSA с модулем N, экспонентой закрытого ключа d, экспонентой открытого ключа e), b — случайное число. Число b называют «слепым множителем» (blinding factor). Полученное в результате значение R клиент направляет в банк вместе с запросом на эмиссию монеты определенного номинала.

Банк, получив запрос клиента, списывает с его счета значение номинала монеты (и, возможно, комиссионные), зашифровывает R своим закрытым ключом, то есть вычисляет значение $R^d \pmod N$, и полученное значение возвращает клиенту.

Нетрудно видеть, что имеет место равенство $R^d \pmod N = h(a)^d \times b \pmod N$ Поэтому, получив от банка значение $R^d \pmod N$, клиент легко освобождается от известного ему «слепого множителя» b (это делается с помощью алгоритма Евклида нахождения наибольшего общего делителя чисел b и N) и получает значение подписи последовательности a, равное $h(a)^d \pmod N$. Последовательность $(a, h(a)^d \pmod N)$ и является цифровым выражением электронной монеты.

Таким образом, клиент получает электронную монету $(a, h(a)^d \pmod N)$, которая может быть предъявлена клиентом банку. При этом банк

не сможет идентифицировать, кому была выдана эта монета. Благодаря «слепому множителю» b, банк непосредственно сам никогда не подписывал a. Все, что известно банку, — это значение $h(a)^d \times b \pmod N$, которое благодаря «слепому множителю» b представляет собой просто случайное число. В то же время банк, проверив цифровую подпись в электронной монете, сможет легко установить, что данная монета была эмитирована именно им.

Таким образом, реализуется одно из важнейших свойств обычных денег — анонимность. Безопасность банка в схемах электронной наличности основывается на стойкости алгоритма RSA. Применение хэш-функции h(x) в описанной здесь конструкции необходимо ввиду известного свойства мультипликативности RSA: если s_1 и s_2 — подписи для m_1 и m_2 соответственно, то $s_1 \times s_2 = (m_1^d) \times (m_2^d) \pmod N$ — подпись для $m_1 \times m_2$ Поэтому, если в качестве электронной монеты использовать последовательность $(a, a^d \pmod N)$, то, имея две электронные монеты, легко изготовить третью.

Очевидно, что электронная наличность помимо анонимности обладает и другими важнейшими свойствами денег:

- возможностью обмена на товары и услуги;
- единовременностью и окончательностью расчетов с их использованием (здесь требуется оговорка, связанная с необходимостью использования в некоторых случаях клиринговых систем или авторизации в реальном масштабе времени принятой наличности в банке, эмитировавшем эту наличность);
- делимостью суммы.

Приведенная выше технологическая схема является лишь одним из методов реализации электронной наличности. Таких методов достаточно много. Все они отличаются способом маскировки начальной последовательности, идентифицирующей электронную монету, алгоритмами подтверждения эмиссии монеты и т. д. В то же время у всех схем эмиссии существуют общие проблемы. Проиллюстрируем их на описанной ранее схеме.

Первая фундаментальная проблема состоит в том, каким образом банк-эмитент, получив от клиента запрос на эмиссию замаскированной монеты, может быть уверен в том, что в последовательности a указан номинал именно той монеты, которую запрашивает клиент. Действительно, банк-эмитент «не видит» a, и потому клиент имеет возможность обмануть эмитента, вставив в последовательность a номинал, существенно больший запрашиваемого.

Существует несколько способов решения этой проблемы. Один из них состоит в следующем. Клиент направляет эмитенту М (М — достаточно большое число) последовательностей $R=h(a)\times b^e \pmod N$ с разными значениями а и Ь, но с одним и тем же номиналом монеты. Банк случайным образом выбирает (М-1) последовательностей и запрашивает у клиента соответствующие значения а и Ь. Таким образом, банк проверяет, насколько «искренен» был клиент в выбранных им для проверки случаях. Легко видеть, что описанное решение обеспечивает защиту банка от обмана клиента с вероятностью 1—1/М.

Другая фундаментальная проблема состоит в возможности повторного использования монеты (double-spending). Классическим решением проблемы является применение единого авторизационного центра. Использованная однажды монета заносится в «черный список» и при попытке повторного применения опознается как использованная.

С проблемой повторного использования тесно связана и проблема выбора длины последовательности а, идентифицирующей монету. С одной стороны, она должна быть достаточно большой, чтобы вероятность совпадения с идентификатором ранее использованной монеты была невысокой. С другой стороны, ее размер желательно ограничить для уменьшения трафика в системах электронной наличности.

Не такой простой оказывается на практике и задача поддержания анонимности цифровых монет. Эта задача не сводится только к анонимности эмиссии монеты, как многие считают. Анонимность должна поддерживаться и на этапе использования монеты. В частности, иногда нетривиальной оказывается задача обеспечения анонимности при возврате электронной наличности на счет клиента, о чем будет рассказано немного позже.

Существуют также проблемы обеспечения эффективных процедур размена монет, мультивалютности, реализации встроенных в монеты контрактов и т. п. Все эти схемы закрыты многообразными патентами, число которых постоянно растет.

Рассмотрим одну из них, изложенную в основополагающей работе Чома. Система основана на использовании алгоритма RSA. Будем обозначать $a^{(1/t)} \pmod N$ вместо $a^d \pmod N$, где $d\times t \equiv 1 \pmod{(p-1)\times(q-1)}$, $N=p\times q$, и называть эту величину корнем t-й степени из а.

Рассматривается бесконечный ряд простых чисел c(1)=3, c(2)=5, c(3)=7, c(4)=11,... Устанавливается следующее соглашение: номиналу 2^1 кибердолларов (КД) соответствует корень степени c(i+1), где i>0, из хэш-функции h(a). Таким образом, одному КД соответствует монета

$(a, h(a)^{(1/3)} (\mathrm{mod}\ N))$, 4 КД — монета $(a, h(a)^{(1/7)} (\mathrm{mod}\ N))$ и т. д. В общем случае для монеты достоинством S КД необходим корень степени, равной произведению всех простых чисел, соответствующих единицам в двоичном представлении S.

Все банкноты, выдаваемые банком, имеют одинаковое достоинство. Для простоты изложения будем считать, что оно равно 15 КД. Тогда подпись банкноты должна представлять собой корень степени $w=3\times5\times7\times11$ хэш-функции h(a). Таким образом, клиент получает от банка монету $(a, h(a)^{(1/w)} (\mathrm{mod}\ N))$. Очевидно, что для того, чтобы корень степени w существовал, необходимо и достаточно, чтобы w и $(p-1)\times(q-1)$ были взаимно простыми. Для этого достаточно, чтобы простые сомножители, на которые раскладываются числа (p-1) и (q-1), были достаточно большими (больше максимального сомножителя в разложении w). Если w и (p-1)x(q-1) — взаимно простые числа, существует такое 1, что $w*l \equiv 1 \ (\mathrm{mod}\ (p-1)\times(q-1))$. Более того, число 1 вычисляется с помощью известного алгоритма Евклида для нахождения наибольшего общего делителя двух целых чисел. На реализацию этого алгоритма требуется не более $O(\log_2 (p-1)\times(q-1))$ элементарных операций.

Очень важно также отметить, что корень степени w может вычислить только банк, поскольку для нахождения 1 требуется знать секретные значения простых чисел p и q. Поэтому эмитировать монету никто, кроме банка, не сможет.

Процедура получения клиентом монеты $(a, h(a)^{(1/w)} (\mathrm{mod}\ N))$ аналогична схеме, описанной ранее. Разница состоит только в том, что клиент направляет в банк вместо $h(a)\times b^e (\mathrm{mod}\ N)$ число $h(a)\times b^w (\mathrm{mod}\ N)$. В этом случае процедура освобождения от «слепого множителя» не меняется — достаточно полученную подпись банка «разделить» на число b.

Рассмотрим теперь, как в схеме Чома осуществляются покупка и возврат электронной наличности. Начнем с покупки. Предположим, клиент, имея монету номиналом 15 КД, хочет потратить 5 КД. Для этого он вычисляет $(a, h(a)^{(1/(3*7)}) (\mathrm{mod}\ N))$, возведя подпись имеющейся монеты в 55-ю степень. Кроме того, клиент создает электронную копилку. Для этого он генерирует случайное число a,, вычисляет $h(a_1)\times b_1^{55} (\mathrm{mod}\ N_1)$, где N, — другой модуль схемы RSA, используемый эмитентом электронной наличности для копилки. Платеж состоит в передаче продавцу значений $(a, h(a)^{(1/(3*7)}) (\mathrm{mod}\ N))$, $h(a_1)\times b_1^{55} (\mathrm{mod}\ N_1)$, а также значения платежа 5 КД. Продавец, в свою очередь, передает всю эту информацию банку клиента.

Банк легко проверяет, что последовательность $(a, h(a)^{(1/(3*7)}) (\mathrm{mod}\ N))$ представляет собой монету достоинством 5 КД. Кроме того, он прове-

ряет по специальному списку, что монета с идентификатором a ранее не использовалась. Если проверки закончились успешно, банк увеличивает счет продавца на 5 КД и возвращает клиенту сдачу в размере 10 КД через копилку: $h(a_1)^{(1/55)} \times b_1 \pmod{N_1}$

В транзакции возврата электронной наличности покупатель отправляет в банк копилку $(a_1, h(a_1)^{(1/55)} \pmod{N_1})$. Банк проверяет ее так же, как и электронную монету, и если копилка подлинная и ранее не использовалась, кредитует счет клиента на 10 КД.

Если бы все платежи, производимые клиентом, делались на сумму 15 КД, рассмотренная выше схема обеспечивала бы безусловную анонимность клиента. Транзакции возврата электронной наличности в банк (клиент обналичивает имеющуюся в его распоряжении копилку) могут нарушить анонимность клиента. Действительно, банк запоминает все платежи, а значит, и все сдачи покупателям. Поэтому если клиент совершил покупку на уникальную или достаточно редкую сумму, то и сдача также будет иметь уникальное значение. Следовательно, при возврате сдачи в банк, когда личность клиента устанавливается по его счету, банк может «вычислить», кто делал покупку на уникальную сумму, то есть анонимность покупок клиента нарушается.

Эта проблема может быть частично решена за счет многократного использования копилки в транзакциях платежа, когда сдачи от электронных монет клиента, возникающие в результате совершаемых им покупок, фиксируются в одной и той же копилке клиента. Если количество клиентов в платежной системе достаточно велико и копилка используется каждым клиентом до тех пор, пока накапливаемая в ней сумма не превысит некоторого фиксированного уровня, а после достижения уровня сразу проводится операция возврата суммы копилки на счет клиента, то шансы банка на «вычисление» клиента не велики.

Рассмотренные ранее примеры относятся к классу так называемых централизованных систем электронной наличности, отличительная черта которых состоит в необходимости участия банка во всех платежах. Гораздо привлекательнее выглядят автономные системы электронных платежей, в которых продавец самостоятельно, без обращения к банку, проверяет подлинность полученной от покупателя электронной наличности. Обращение к банку в централизованных системах электронной наличности требуется для предотвращения повторной траты одной и той же электронной монеты. Вместо этого автономные системы обеспечивают идентификацию нарушителя после проведения транзакции платежа. В общих чертах опишем конструкцию автономной системы электронной наличности, базирующейся на применении схемы аутентификации Шнорра.

Напомним, что в схеме Шнорра операции производятся в поле GF(p), где p — большое простое число. Рассматривается также подгруппа мультипликативной группы поля простого порядка q с образующим элементом g. Каждый клиент банка обладает секретным ключом x, содержащим идентификатор клиента, и открытым ключом $y=g^x \pmod p$.

В транзакции снятия со счета с целью эмиссии электронной монеты клиент выбирает случайное число k и вычисляет $r=g^k \pmod p$. Электронная монета состоит из некоторой строки, содержащей y и r, а также подписи банка для этой строки.

Для совершения транзакции платежа клиент предоставляет продавцу электронную монету. Продавец проверяет подлинность подписи банка и, если она корректна, генерирует случайное число e, которое направляется клиенту. Клиент вычисляет $s=k-x\times e \pmod q$ и возвращает s продавцу. Продавец, получив s и зная e, r, y, проверяет соотношение $r=(g^s)\times(y^e) \pmod p$. Как известно, если рассматриваемое соотношение верно, клиент действительно обладает закрытым ключом x, соответствующим открытому ключу y.

В транзакции возврата электронной наличности на счет клиента продавец отправляет в банк электронную монету, а также числа e и s. Если продавец обнаруживает, что монета с параметрами y, r уже ранее использовалась, то есть у банка имеются две пары (e_1,s_1) и (e_2,s_2), удовлетворяющих проверочному соотношению схемы Шнорра, то банк легко вычисляет секретный ключ x, решая систему двух линейных уравнений

$$s_1=k-x*e_1 \pmod q$$
$$s_2=k-x*e_2 \pmod q$$

относительно x. Зная x, банк может идентифицировать клиента, нарушившего правило системы.

Таким образом, автономные системы позволяют однозначно идентифицировать нарушителя. Но в таких системах банк идет на определенный риск, поскольку в момент обнаружения повторной траты электронной монеты на счету нарушителя может не оказаться суммы, достаточной для покрытия перерасхода.

Электронная наличность может иметь и другие формы представления. Кроме электронных монет получили определенное распространение и электронные чеки. Электронному чеку присущи те же особенности, что и бумажному. Он также является указанием покупателя банку перечислить деньги и так же, как и бумажный чек, выдается получателю платежа, который предъявляет его в банк для получения наличных.

В то же время, у электронного чека имеется масса достоинств. Во-первых, его можно передать для оплаты товаров или услуг через Интернет (или другую телекоммуникационную среду) с компьютера покупателя на компьютер продавца. Во-вторых, схемы электронных чеков используют протоколы, позволяющие надежно осуществить взаимную аутентификацию покупателя и продавца. Наконец, электронные чеки позволяют скрыть номер счета покупателя, например, зашифровав его открытым ключом банка.

За рубежом получили популярность системы электронных чеков, разработанные компаниями CyberCash и FSTC (Financial Services Technology Corporation).

Преимущества схем электронной наличности перед системами пластиковых карт состоят в следующем:

- Наличие надежных средств аутентификации участников транзакции ЭК. Безусловно, протокол SET предоставляет не менее надежные средства обеспечения безопасности, но из-за того, что эти средства должны быть адаптированы для предоставления транзакции ЭК в конечном счете в платежную сеть, стоимость решения SET выше стоимости решений для схем электронной наличности.
- Себестоимость транзакции ЭК с использованием схем электронной наличности в несколько раз ниже аналогичного параметра в транзакции с использованием пластиковых карт. Главная причина здесь та же — при использовании пластиковых карт помимо среды Интернет применяются выделенные телекоммуникационные системы, увеличивающие стоимость транзакции. Себестоимость транзакции ЭК с использованием схемы электронной наличности составляет несколько центов.
- Комиссионные, выплачиваемые обслуживающим банком банку-эмитенту карты, в платежной системе на базе пластиковых карт имеют структуру «X %, но не менее $Y». В результате небольшие платежи (размер платежа сравним с Y) становятся невыгодными. То же самое верно и для крупных платежей, но по другой причине. Если размер транзакции достаточно большой, что характерно для схем B2B, то комиссионные X % могут попросту «съесть» маржу продавца, сделав расчет за покупку через платежную систему невыгодным. В случае применения схем электронной наличности в силу низкой себестоимости транзакции можно рассчитывать на то, что оба параметра X и Y будут значительно ниже значений, характерных для систем на основе пластиковых карт.

В то же время, главный недостаток схем электронной наличности заключается в отсутствии международных стандартов на протоколы, лежащие в основе функционирования подобных систем. Очевидно, что мировое сообщество должно инвестировать миллиарды долларов в создание инфраструктуры электронной наличности, аналогичной существующей инфраструктуре пластиковых карт. Без создания такой инфраструктуры надеяться на широкое распространение технологии электронной наличности вряд ли приходится.

Схемы электронной наличности получили распространение и в России. Сегодня известны две системы — PayCash и WebMoney Transfer.

Проект PayCash является совместной разработкой банка «Таврический» (С.-Петербург) и группы компаний «Алкор-Холдинг». Система PayCash реализует цифровой эквивалент чека. Электронные деньги появляются у пользователя в момент перевода денег с его счета на его платежную книжку (эквивалент чековой книжки) в электронном кошельке (программа, работающая на компьютере пользователя). Использование цифровой подписи позволяет пользователям платежной системы получать электронные денежные обязательства, которые позже не могут быть не признаны банком пользователя.

В системе используется концепция слепой электронной подписи, что делает применение электронной наличности при покупках анонимным.

Специальная процедура, используемая в PayCash, позволяет расходовать электронную наличность (денежные обязательства банка) по мере необходимости. Клиент может пополнять электронную книжку в банке и использовать ее для платежей на любую сумму в пределах находящихся на ней средств, не задумываясь о необходимости их размена.

Процедура покупки в системе PayCash происходит следующим образом.

Кошелек продавца посылает кошельку покупателя требование об оплате, содержащее подписанный электронной цифровой подписью (ЭЦП) текст договора.

Если покупатель собирается платить, то его кошелек отправляет кошельку продавца электронные деньги и подписанный покупателем текст договора. Продавец отправляет электронные деньги в банк для авторизации.

Банк, получив электронные деньги, проводит авторизацию (проверяет подлинность электронного чека и остаток средств в рамках этого чека). Результаты авторизации передаются продавцу вместе с электронной квитанцией для покупателя. В случае успешной авторизации деньги переводятся на счет продавца.

Продавец передает покупателю электронную квитанцию банка и приступает к выполнению своих обязательств по оказанию соответствующих договору услуг покупателю.

В системе PayCash предполагается участие неограниченного числа банков, каждый из которых может выпустить собственные электронные деньги.

Комиссионные платежной системы за процессинг транзакции составляет 1-2 % от ее размера.

В систему PayCash деньги можно ввести одним из следующих способов:

- наличными через один из 6 банков-партнеров системы;
- наличными, вызвав курьера на дом;
- банковским переводом;
- почтовым или телеграфным переводом;
- с помощью предоплаченной карты.

Вывести деньги из системы можно:

- почтовым или телеграфным переводом;
- переводом на счет в российском банке;
- наличными в офисе фирмы в Санкт-Петербурге.

Электронной наличности в системе PayCash придается статус предоплаченных финансовых продуктов в рамках указаний ЦБ РФ №№ 276,277 (подробнее об этом сказано чуть позже). В связи с этим система PayCash работает только с рублями.

На январь 2001 г. в системе были зарегистрированы 30 магазинов и 11 тысяч пользователей. Ежедневно к системе подключалось около 60 пользователей.

Теперь несколько слов о системе WebMoney Transfer. Система предоставляет возможность пользователю Интернета осуществлять безналичные расчеты в масштабе реального времени с использованием электронной наличности WEBMONEY (WM).

Клиентами системы являются продавцы и покупатели товаров и услуг. С одной стороны, это Web-магазины, с другой — любой пользователь Интернета, не имеющий возможности или не желающий использовать традиционные методы расчетов (кредитные карточки и т. п.).

Стать клиентом системы пользователю позволяет клиентское программное обеспечение — WEBMONEY KEEPER. С помощью этой программы пользователь получает возможность фиксировать определенные суммы для расчетов, контролировать движение собственных или перечисленных ему средств.

С помощью программы WEBMONEY KEEPER возможно:

1. В любое время принять или отказаться от WM, переведенных пользователю любым другим клиентом системы по сети Интернет.
2. Перевести по сети Интернет любое количество WM любому другому клиенту системы. Такими клиентами могут быть как частные лица, так и компании, принимающие WM в качестве средства платежа за товары и услуги, предлагаемые в сети Интернет.
3. Перевести свои WM на любой банковский счет банка системы с последующим (автоматическим или по запросу) переводом их в доллары США, российские рубли (или любую другую валюту).
4. Перевести доллары США, российские рубли (другую валюту) в WM с последующим использованием их в расчетах в рамках системы WebMoney Transfer.

WEBMONEY KEEPER является свободно распространяемым программным продуктом, в котором реализованы универсальные решения как для покупателей, так и для продавцов услуг или товаров в Сети.

WEBMONEY KEEPER в виде самораспаковывающегося инсталляционного архива можно бесплатно получить на Web-сервере системы.

Если у клиента есть необходимость оплатить товар или услугу, предоставляемую Интернет-магазином (или получить оплату за свои товары или услуги), он может это сделать через систему WebMoney Transfer. Чтобы стать участником системы, достаточно:

- для всех пользователей: скачать и инсталлировать программу WEBMONEY KEEPER;
- для покупателей: перевести денежные средства (например, доллары США, российские рубли) с любого банковского счета банка системы WebMoney Transfer в WM с зачислением последних на спецсчета-кошельки. Реквизиты перевода можно получить с помощью программы WEBMONEY KEEPER (функция Пополнить кошелек).
- для продавцов: открыть (бесплатно) спецсчета-кошельки, в адрес которых будут поступать WM в счет оплаты их товаров и услуг, а также настроить свои Web-магазины на ведение расчетов в WM.

В рамках системы WebMoney Transfer пользователь может тратить WM в любом магазине, который принимает их в качестве оплаты товаров или услуг. Для этого не нужно предварительно открывать в нем свой специальный счет.

Так как WM имеют эквивалентную денежную ценность, то по совершению оплаты магазины, использующие систему WebMoney Transfer,

немедленно обеспечивают клиенту доставку товаров или услуг. Система WebMoney Transfer предлагает также решение для превращения Web-сервера в виртуальный магазин. Для этого необходимо установить WEBMONEY KEEPER и настроить его под предлагаемые товары.

Далее рассмотрены некоторые методы обеспечения безопасности, примененные в WebMoney Transfer.

Для входа в программу WEBMONEY KEEPER необходимо знание уникального 13-значного идентификатора пользователя, его личного пароля, а также местоположение в памяти компьютера файлов с секретным ключом и кошельками.

Идентификатор генерируется автоматически, уникален для каждой установленной программы WEBMONEY KEEPER. Это анонимное имя клиента в системе. Идентификатор необходим для входа в программу WEBMONEY KEEPER и осуществления сделок в системе WebMoney Transfer.

Пароль определяется лично клиентом и необходим для входа в программу WEBMONEY KEEPER и осуществления сделок в системе WebMoney Transfer.

Внутри каждой установленной программы WEBMONEY KEEPER денежные средства WM хранятся в кошельках.

Кошельки могут поддерживать только один тип валюты. Например:

- Z-кошельки можно пополнить только долларами США. С Z-кошелька можно отправить безналичный банковский перевод только в долларах США. На Z-кошельке 1WM=1USD.
- R-кошельки можно пополнить только российскими рублями. С R-кошелька можно отправить безналичный банковский перевод только в российских рублях. На R-кошельке 1WM=1RUR.

Перевод и получение денежных средств осуществляется только между однотипными кошельками клиентов системы.

Для осуществления сделок необходимо сообщить партнеру номер кошелька. При этом он сможет только отправить деньги на другой кошелек (клиент может отказаться от их принятия), и никто не сможет снять деньги из клиентского кошелька с удаленного компьютера.

Более того, можно создавать отдельный кошелек для разовой сделки и после ее завершения удалять его.

Все номера кошельков программы WEBMONEY KEEPER хранятся в файле, который может находиться на отдельной дискете. Поскольку

при входе в программу WEBMONEY KEEPER требуется указать расположение данного файла, очевидна проблематичность для постороннего лица войти в программу без согласия пользователя.

Вся информация о сделке как на уровне ресурсов компьютера пользователя, так и в линиях сети Интернет кодируется с помощью ключа. Файл с ключом хранится пользователем на отдельной дискете. Поскольку при входе в программу WEBMONEY KEEPER требуется указать расположение данного файла, решить эту задачу постороннему лицу без согласия пользователя практически невозможно.

Все сообщения в системе передаются в закодированном виде с использованием алгоритма защиты информации подобного RSA с длиной ключа более 1024 битов. Для каждого сеанса используются уникальные сеансовые ключи. Поэтому в течение сеанса (времени осуществления транзакции) никто, кроме пользователя, не имеет возможности определить назначение платежа и его сумму.

Также невозможно совершить денежную операцию, основываясь на реквизитах прошлых сделок клиента. Для каждой сделки используются уникальные реквизиты, и попытка использовать их вторично немедленно обнаруживается и предотвращается.

Всем участникам системы гарантируется анонимность расчетов. При желании пользователь может не указывать никаких сведений о себе (имя, фамилия, адрес, почтовый адрес, номера банковских счетов и т. п.) при получении программы WEBMONEY KEEPER с сервера системы, при ее инсталляции, при осуществлении операций в системе WebMoney Transfer.

Все услуги и поставки товаров осуществляются в «адрес» оплатившего их кошелька. Можно создавать кошельки для разового использования и непосредственно после совершения сделки удалять их. По постоянному идентификационному номеру пользователя невозможно определить номера используемых им кошельков. Аналогично, номер кошелька не несет информации об идентификаторе пользователя. Кроме того, можно инсталлировать на своем компьютере любое число версий WEBMONEY KEEPER под разными идентификаторами и входить в систему для осуществления сделок с любого из них.

В системе реализовано два типа платежей:

1. Обычный платеж. Покупатель производит оплату. При этом с его кошелька списывается, а в кошелек продавца зачисляется сумма в размере стоимости товара. После чего продавец осуществляет доставку товара.

2. Двухфазный платеж (платеж с протекцией торговой сделки). Магазин определяет товары, по которым возможен двухфазный платеж и сроки их доставки. После чего указанный товар можно оплатить только двухфазным платежом.

   Клиент производит оплату товара и определяет (самостоятельно) пароль транзакции. При этом на кошельке покупателя резервируется сумма в размере стоимости товара. Продавец получает уведомление о том, что денежная сумма, эквивалентная стоимости товара, зарезервирована, а также инструкции по доставке. На этом первая фаза платежа завершается.

   Возможны различные варианты заключительной стадии двухфазного платежа:

   1. Если продавец осуществляет доставку в указанный им срок и качество товара соответствует заявленному в магазине, то покупатель получает товар и сообщает продавцу код транзакции. Продавец производит сверку кода транзакции через программу WEBMONEY KEEPER, после чего денежная сумма с кошелька покупателя переводится в кошелек продавца.
   2. Если продавец не осуществляет доставку в указанный им срок, то по истечении срока доставки товара зарезервированная денежная сумма разблокируется и становится доступной для других операций.
   3. Если качество товара не соответствует требованиям покупателя и он отказывается принять товар от продавца, то по истечении срока доставки товара зарезервированная денежная сумма разблокируется и становится доступной для других операций.

На этом двухфазный платеж считается завершенным.

В системе WebMoney Transfer приняты следующие тарифы.

Система не устанавливает никакой платы за использование клиентского программного обеспечения WEBMONEY KEEPER, которое предоставляется бесплатно с WEB-сервера системы.

За совершение каждой транзакции (за исключением операций с кошельками одного идентификатора) с кошелька пользователя взимается тариф в размере 0,8 % от суммы платежа, но не менее 0,01 единицы WM.

За все операции, связанные с движением WM из системы, взимается плата в размере 0,8 % от суммы платежа, но не менее 0,01 единицы WM. Ввод денег в систему производится бесплатно.

Система WebMoney Transfer официально действует (имеет представительства) кроме России в США, в Чехии, на Украине и в Казахстане. Сегодня в системе официально предусмотрен обмен на WM и обратно долларов США, чешских крон, российских рублей, казахских тенге и украинских гривен через обменные пункты на территориях этих стран. Все остальные валюты могут конвертироваться в WM и обратно через шлюз в банке 1MB (Черногория).

Деньги на свой кошелек в системе WebMoney Transfer можно поместить одним из следующих способов:

- обычным банковским переводом;
- почтовым или телеграфным переводом;
- переводом через систему Western Union;
- путем обмена наличных на WM в обменном пункте (в четырех странах);
- через покупку предоплаченной карты;
- через шлюз в черногорийском банке 1MB в любой валюте.

Вывести деньги из системы можно следующим образом:

- перевести WM со своего кошелька на счет в любом российском или зарубежном банке;
- обменять WM на наличные в одном из обменных пунктов системы;
- переслать на свой домашний адрес почтовым или телеграфным переводом;
- перевести их кому угодно через систему Western Union.

Оценить надежность систем PayCash и WebMoney Transfer сегодня невозможно, поскольку обе системы не предоставляют полных данных по технологии своей работы и деталям реализации. В отсутствие стандартов на электронную наличность системы, основанные на использовании криптоалгоритмов в протоколах взаимодействия многих участников, безусловно, должны проходить соответствующий аудит и сертификацию в авторитетных компаниях, специализирующихся в области защиты информации.

Развитие электронных платежных систем в Интернете находится под пристальным вниманием как государственных органов различных стран, так и международных консультационных организаций в области финансов и права. Среди последних — Базельский комитет по банковскому надзору (Basle Committee on Banking Supervision). В разработке документов Базельского комитета принимают участие ведущие

специалисты центральных банков стран ЕС. Эти документы имеют статус рекомендаций национальным банкам европейских стран при рассмотрении различных вопросов финансовой деятельности. Существует несколько документов, выпущенных комитетом и содержащих рекомендации по эмиссии, обращению и контролю электронной наличности. К таким документам относятся:

- Risk Management for Electronic Banking and Electronic Money Activities;
- Implications for Central Banks of the Development of Electronic Money;
- Security of Electronic Money.

В преамбуле первого документа перечислены преимущества, получаемые банками от операций с электронной наличностью. В частности, в нем говорится: «В более широком плане развитие электронной коммерции может внести вклад в повышение эффективности банковских платежей и снижение расходов по операции в национальном и международном масштабах. Покупатели и продавцы смогут повысить эффективность и скорость проведения платежей и увеличить рынки сбыта товаров и банковских услуг».

ЦБ РФ также выпустил документы, регулирующие эмиссию и обращение электронной наличности, или как сказано в них, «предоплаченных ЦБ финансовых продуктов, выпущенных в электронной форме». Это указания ЦБ России от 3 июля 1998 г. № 276-У «О порядке выдачи разрешений кредитным организациям-резидентам на распространение платежных карт или предоплаченных финансовых продуктов других эмитентов» и № *211-У* «О порядке выдачи регистрационных свидетельств кредитным организациям-резидентам на осуществление эмиссии предоплаченных финансовых продуктов».

В соответствии с этими документами кредитные организации на территории России могут выпускать денежные обязательства (в том числе и в электронной форме) на основании разрешения, выдаваемого ЦБ РФ. Под предоплаченными финансовыми продуктами понимаются «денежные обязательства кредитной организации, заменяющие в процессе их обращения требования юридических и/или физических лиц по оплате товаров и услуг, и в том числе денежные обязательства, составленные в электронной форме».

Некоторые специалисты в области права предлагают рассматривать электронную наличность в России в качестве условной денежной единицы, в которой выражено денежное обязательство эмитента, погаша-

емое в рублях по первому требованию держателя электронной наличности. Внедрение электронной наличности в этом случае возможно в порядке, предусмотренном договорами между участниками расчетов на основании положения ГК РФ (п. 2 ч. 1 ст. 317). «В денежном обязательстве может быть предусмотрено, что оно подлежит оплате в рублях в сумме, эквивалентной определенной сумме ... в условных денежных единицах ... В этом случае подлежащая уплате в рублях сумма определяется по официальному курсу ... условных денежных единиц на день платежа, если иной курс или иная дата его определения не установлены законом или соглашением сторон». При этом электронная наличность представляет собой денежные обязательства физического или юридического лица, подписанные его электронной цифровой подписью.

Важно отметить, что оба изложенных здесь обоснования использования электронной наличности действуют только в том случае, когда продавец, получив от покупателя электронную наличность, не распоряжается ею далее в качестве платежного средства, а сразу получает в обмен на полученную наличность ее денежное покрытие. Использование электронной наличности в качестве платежного средства продавцом не соответствует действующему в настоящее время российскому законодательству, в соответствии с которым единственным законным платежным средством на территории России является рубль (п. 1 ст. 140 ГК, а также ст. 29 Федерального закона «О Центральном Банке Российской Федерации (Банке России)»).

Понятие предоплаченного финансового продукта используется для обоснования статуса электронной наличности в системе PayCash.

Система WebMoney Transfer для обоснования WM придает последним статус некого объекта права, обладающего определенной ценностью. Выразить эту ценность можно в любой допускаемой законом форме. В одном случае это может быть долговое обязательство на предъявителя, в другом — паевой взнос, в третьем — ценная бумага, наделяющая ее владельца определенными правами.

Другие системы, не использующие пластиковые карты

Другой тип системы ЭК, в общем случае не использующий для расчетов пластиковые карты, иллюстрирует система Earthport. В основе системы находится сервер Earthport, выполняющий функцию многопользовательского электронного бумажника.

В самом начале работы через систему Earthport клиент должен зарегистрироваться на сервере Earthport и открыть на нем свой бумажник. Пользователь в защищенной сессии предоставляет серверу информацию о себе, включая имя, адрес, телефон, а также средства расчета за покупку. В качестве средств расчета может быть либо номер счета в банке, либо реквизиты пластиковой карты.

В результате регистрации в системе покупатель получает номер своего бумажника, идентификатор в системе и пароль для доступа к своему защищенному бумажнику.

Процедура покупки в системе выглядит следующим образом. Покупатель собирается произвести покупку некоторых товаров в ТП, поддерживающем систему Earthport. После того как он подтверждает свое согласие с условиями покупки (обычно покупатель нажимает кнопку Покупаю на соответствующей страничке сайта магазина), он автоматически переадресуется на сайт Earthport. Для того чтобы получить доступ к своему бумажнику, покупатель набирает свои идентификатор и пароль. С помощью бумажника покупатель легко заполняет данные, необходимые для совершения покупки (адрес доставки, способ оплаты и т. п.), и окончательно подтверждает транзакцию. Далее покупатель может вернуться на сайт магазина.

После завершения транзакции система Earthport в отложенном режиме пытается произвести расчеты между клиентом и ТП. Если расчет произведен, транзакция считается успешной.

Достоинства технологии очевидны. Фактически сервер Earthport является посредником в расчетах ТП и покупателя. Он удобен в использовании (клиент только однажды предоставляет данные о себе и далее пользуется ими при совершении покупок). Во время покупки производится аутентификация клиента системой, причем данные аутентификации клиенту ТП не известны, а личные данные клиента хранятся в защищенном месте. Это повышает безопасность операций покупки через систему Earthport.

Невысокими являются и риски магазина. ТП выполняет заказ, убедившись в том, что платеж выполнен.

Недостаток технологии заключается в замкнутости системы Earthport (ограниченное количество ТП).

Пример другой технологии расчетов без пластиковых карт — российская система EACCESS (www.eaccess.ru). Эта система ориентирована на микроплатежи (до $10) в Интернете, связанные с покупкой нематериальных товаров и услуг.

Суть технологии чрезвычайно проста. Покупатель заходит на сайт ТП, работающего в системе EACCESS, выбирает интересующие его товары и подтверждает покупку. После этого клиент получает специальный код для платежа и номер телефона, по которому он должен позвонить. В результате в телефонном счете клиента, регулярно получаемом им на ежемесячной основе, появляется сумма покупки. Таким образом, покупка оплачивается только в момент оплаты телефонных услуг.

Для реализации описанной схемы EACCESS подписал договор с Ростелекомом. Планируется заключить аналогичные договоры с операторами сотовой связи.

Недостатки указанной системы с точки зрения бизнеса очевидны. Система EACCESS расплачивается с ТП в короткое время после совершения покупки, в то время как сама получает возмещение от покупателя по истечении гораздо большего времени. Кроме того, нет гарантий оплаты счета. Таким образом, EACCESS берет на себя риски, связанные с невозмещением покупателем средств за совершенную им транзакцию.

Глава 6. Законодательство, правила и стандарты

Правила международных платежных систем в области электронной коммерции

CNP-транзакции рассматриваются в платежных системах как транзакции повышенного риска. В связи с этим все CNP-транзакции выполняются только в режиме реального времени (значение величины floor limit, определяющей верхний размер транзакции, которая может быть проведена в режиме off-line, для CNP-транзакций определено равным нулю).

По правилам международных платежных систем обслуживающие банки имеют право на обслуживание ТП, расположенных в его зоне Area of Use, которая определена лицензией, выданной данному банку платежной системой. При этом адрес ТП определяется по адресу, указанному в договоре между обслуживающим банком и ТП.

В соответствии с теми же правилами обслуживающие банки имеют право обслуживать торговые предприятия, расположенные вне зоны Area of Use, но только по транзакциям владельцев карт, чьи банки-эмитенты расположены в зоне Area of Use обслуживающего банка.

Рассмотрим теперь правила, определяющие ограничения по использованию дебетовых и кредитных карт, а также распределение ответственности между участниками транзакции ЭК. Эти правила на настоящий момент времени отличаются в системах VISA и Europay-MasterCard.

Начнем с системы VISA. Транзакции ЭК в этой системе разрешены как по кредитным, так и по дебетовым картам независимо от используемого протокола ЭК (еще совсем недавно транзакции ЭК по дебетовым картам разрешались только в случае применения протокола SET; ситуация изменилась летом 2000 г.). В настоящее время системой VISA в качестве надежных протоколов ЭК признаются 3D SET, 3D SSL и 3D Secure. Каждый из перечисленных протоколов однозначным образом определяет зону ответственности всех участников транзакции ЭК (все

протоколы базируются на концепции трех доменов). Поэтому в случае возникновения диспута по транзакции «виновник» конфликта определяется однозначным образом. В частности, в случае возникновения самого распространенного в электронной коммерции диспута, при котором клиент утверждает, что не совершал данной транзакции ЭК, ответственность лежит на банке-эмитенте.

В настоящее время протокол 3D SET является базовым для стран Европейского Союза и Латинской Америки, 3D SSL — для США, а 3D Secure претендует на роль глобального стандарта аутентификации. Переход на стандарт 3D Secure планируется начать в октябре 2002 г., начиная со стран Азиатско-Тихоокеанского региона, США и Канады.

Кроме того, система VISA планирует ввести изменение в распределении ответственности за результат транзакции ЭК, начиная с 2003 г. В соответствии с этим изменением, если эмитент не поддерживает протоколов 3D Secure или 3D SET, а обслуживающий банк поддерживает, то при возникновении диспута по транзакции ЭК ответственность будет переложена на эмитента.

В системе Europay-MasterCard операции по дебетовым картам (Maestro) разрешаются только при использовании протоколов 3D SET и виртуальных номеров карт (Pseudo Card Number). В этом случае ответственность при возникновении диспута лежит на эмитенте за исключением единственного случая, когда покупатель не получил оплаченной услуги/товара.

Электронные покупки по кредитным картам разрешаются независимо от применяемого протокола электронной коммерции. Однако если используется протокол, отличный от 3D SET, ответственность в случае возникновения диспута ложится на обслуживающий банк.

По правилам международных платежных систем обслуживающий банк должен иметь прямое соглашение на обслуживание Интернет-магазина (агентские организации в случае ЭК не разрешаются).

Платежные системы рекомендуют обслуживающим банкам посещать Web-сайты ТП для проверки выполнения правил платежных систем. К числу таких правил относятся:

- отсутствие дискриминации в отношении карт, обслуживаемых ТП в соответствии с договором между ТП и обслуживающим банком;
- отображение логотипа платежной системы, участником которой является обслуживающий банк;
- запрет использования логотипа платежной системы в целях рекламы продаваемой продукции;

- запрет использования магазином лимитов на размер транзакции (относится как к максимальной, так и к минимальной величине транзакции);
- ТП не имеет права ни в каком виде предоставлять третьей стороне информацию о реквизитах карты (номер карты, срок ее действия и т. п.) и деталях выполненных транзакций за исключением случая, когда эта третья сторона является агентом ТП по проведению транзакций между ТП и обслуживающим банком либо компетентным правительственным органом;
- данные о картах, которые более не будут использоваться ТП, должны уничтожаться способом, гарантирующим невозможность их восстановления.

Кроме того, международные платежные системы сформулировали набор правил, которые они назвали «Best Practices to Help Electronic Commerce Merchants» и которые активно предлагаются к использованию ТП под патронажем обслуживающего банка. Этот набор правил содержит следующие требования:

- хранение всех данных о реквизитах карт должно осуществляться в зашифрованном виде;
- хранение всех резервных (back-up) файлов, содержащих информацию о картах, должно производиться в закрытом виде;
- все секретные ключи, используемые для шифрования данных, должны храниться с использованием устройств Hardware Tamper-Resistant Security Module;
- все операции шифрования должны производиться внутри Hardware Tamper-Resistant Security Module;
- информация о ключах должна распределяться между несколькими служащими системы безопасности;
- для шифрования данных должны использоваться ключи длиной не менее 128 битов;
- ограничивать доступ к информации о картах только персоналом, имеющим отношение к этим данными по долгу своей службы;
- защищать доступ к серверам ТП;
- периодически инспектировать сервер и его приложения;
- физически разделять сервер БД и серверы, работающие с сетью;
- информация о картах по мере утраты необходимости ее использования должна уничтожаться.

Компания VISA разработала документы Acquirer Best Practices, Merchant Best Practices, Cardholder Best Practices, описывающие правила и рекомендации по повышению безопасности транзакций ЭК.

Для обеспечения транзакций ЭК международные платежные системы Europay и MasterCard утвердили следующие правила (в том числе ввели определенные изменения) для форматов своих сообщений (0100 — Authorization Request, 0120 — Authorization Advice, 0121 — Authorization Advice Repeat):

- значение DE 003 (Processing Code) полагается равным «000000», что соответствует «Покупке товаров и услуг»;
- значение DE 022 (POS Entry Mode) должно иметь вид «81x»;
- поле Field #4 (POS Cardholder Presence Indicator) в DE 061 (POS Data) должно принимать значение «5» (Cardholder Not Present, electronic order);
- поле Field #5 (POS Card Presence Indicator) в DE 061 (POS Data) должно принимать значение «1» (Card Not Present).

Private Data Sub-element (PDS) 42 (Security Level Indicator) в Data Element (DE) 048 (Additional Data, Private) должно принимать следующие значения в зависимости от протокола, используемого для проведения транзакции:

- Not Applicable;
- 05 SET transaction with cardholder certificate;
- 06 SET transaction without cardholder certificate;
- 07 Channel- encrypted (e. g. SSL, etc.);
- 08 No security;
- PDS 40 (Certificate Serial Numbers) в DE 048 (Additional Data, Private) должно содержать серийный номер сертификата клиента (этот элемент должен присутствовать в сообщении только, если PDS 42 в DE 048 имеет значение «05») и опционно-серийный номер сертификата ТП;
- DE 055 должно содержать минимальный набор EMV-данных, передаваемых от ОБ банку-эмитенту.

В клиринговых сообщениях подэлемент Sub Element 7 (Card Data Input Mode) в DE 022 (POS Data Code) должен принимать значение T, если используется протокол SET с сертификатами, значение S — в остальных случаях. В соответствии с ECCSS Release 00.1 (начинает действовать с 10 июня 2000 г.) этот подэлемент должен принимать значение T,

если используется протокол SET с сертификатами, S — для протокола SET без сертификатов, значение V для случая encrypted channel и V — в остальных случаях.

Международные платежные системы не будут выделять специальные значения кодов Merchant Category Code для транзакций ЭК.

Аналогичные изменения форматов авторизационных и клиринговых сообщений справедливы и для системы VISA. Для сообщений BASE I и VISA SMS имеют место следующие изменения.

- Point of Service Condition Code — Field 25. Значение поля для транзакций электронной коммерции должно быть равно 59.
- Electronic Commerce Indicator — Field 60, Positions 9 and 10. Аналог Security Level Indicator в сети EPS-Net. Принимает те же значения, что SLI в сообщениях Europay (см. выше).
- SET Certificate Serial Numbers — Field 126.6/7. Поле используется для передачи серийного номера SET certificate клиента и ТП от ОБ к банку-эмитенту. Используется только для SET-транзакций.
- XID and TranStain — Field 126.8/9. Величина XID является идентификатором транзакции, используемым для вычисления величины TransStain. Величина TranStain вычисляется с использованием XID и секрета владельца карты (случайная величина, известная только владельцу карты и его банку-эмитенту).

В сообщениях BASE II указывается значение. Положение индикатора в сообщениях BASE II указаны в табл. 6.1.

Таблица 6.1 - Положение Eectronic Commerce Indicator в сообщениях BASE II

Name	TCR	Position
Draft Data	TCR 1	Position 116
Data Capture Advice (TC 57)	TCR 0	Position 111
Fraud Advice (TC 40)		
BASE I Advice (TC 48) ISO Enriched	TCR 0	Position 165–166

Кроме того, для уменьшения расходов эмитента платежные системы Europay/MasterCard разрешают эмитенту группировать некоторые chargeback в одну запись клирингового сообщения (single combined 1442 chargeback record). Это правило распространяется на операции, выполненные в торговых предприятиях с MCC 4816 (Computer Network Inbound Telemarketing) и 5967 (Direct Marketing/Inbound Telemarketing) и касается сообщений chargeback с двумя значениями Reason Code: 37

(ECCF 4526 «Fraudulent Transaction — No cardholder authorization») и 41 (ECCF 4544 «Cancelled Recurring Transaction»).

Наконец, необходимо рассказать о программе Excessive Chargeback Programme for Electronic Merchants, предназначенной для наказания ТП (через обслуживающий банк), превышающих некоторые пороговые значения мошенничеств. Программа касается ТП с MCC 4816 и 5967 (туристические агентства, заказ такси и автомобилей, компьютерные сети и различные информационные услуги, агентства приема заказов по каталогам (mail-order houses), клубы (membership clubs)).

В соответствии с правилами Europay/MasterCard ТП, для которых в течение двух календарных месяцев зафиксировано одно из двух:

- количество chargeback составляет не менее 1% от всех операций покупки;
- объем операций, по которым были сгенерированы chargeback, составляет не менее 2,5 % от всего объема продаж ТП,

объявляются excessive chargeback merchant и могут подвергнуться штрафу в размере:

- $25,000 в месяц в течение 3-5 месяцев;
- $50,000 в месяц в течение 6-7 месяцев;
- $75,000 в месяц в течение 8-9 месяцев;
- $100,000 в месяц, начиная с 10-го месяца.

Обслуживающий банк имеет возможность прекратить договор с ТП в случае превышения указанных выше порогов.

Кроме того, в соответствии с программой Excessive Chargeback Programme for Electronic Merchants банки-эмитенты могут собирать с обслуживающих банков компенсационные платы (Recovery Fee) за каждую транзакцию, по которой был сгенерирован chargeback, в размере:

- $25 за транзакцию в течение 3-5 месяцев;
- $50 за транзакцию в течение 6-7 месяцев;
- $75 за транзакцию, начиная с 8-го месяца.

Помимо этого, за нарушение правил, связанных с обработкой транзакций ЭК торговыми предприятиями, платежные системы дополнительно наказывают обслуживающие их банки. В частности, за отображение торговым предприятием на своем сайте знака MasterCard Mark или логотипа MasterCard с целью повышения статуса ТП, за взимание дополнительных плат с клиента, использование ограничений на размер транзакции, система MasterCard может сделать соответствующему

обслуживающему банку предупреждение, потребовав от него исправления ситуации в течение 30 дней и наложив штраф в размере до $2 тысяч.

Если в течение 12 месяцев с момента первого предупреждения будет отмечено второе аналогичное нарушение, обслуживающий банк наказывается штрафом до $5 тыс. Наконец, если в рамках все того же 12-месячного периода будет отмечено третье нарушение, обслуживающий банк наказывается штрафом до $25 тыс. и MasterCard требует прекращения работы такого ТП в своей системе.

Еще более жесткие правила применяются системой MasterCard к обслуживающему банку за нарушения, связанные с передачей ТП информации о реквизитах карты и деталях транзакций. В частности, при первом предупреждении платежная система может наказать ОБ на сумму до $5 тыс., а в случае повторного нарушения в течение следующих с момента предупреждения 12 месяцев — штрафом в размере до $45 тыс.

Если переданная ТП информация привела к компрометации карт, обслуживающий банк должен предоставить в платежную систему всю имеющуюся у него информацию и в дальнейшем пройти процедуру сертификации по безопасности для обслуживаемой им сети ТП в системе MasterCard.

В соответствии с правилами VISA, определенными в Global Merchant Chargeback Monitoring Program, ТП объявляется excessive chargeback merchant, если зафиксировано одновременное выполнение двух условий:

- количество международных chargeback (отказы по транзакциям, выполненным по картам иностранного банка-эмитента) по этому ТП за месяц составляет не менее 100 сообщений;
- количество операций, по которым были сгенерированы международные chargeback, составляет не менее 5 % от всего количества международных продаж ТП.

Торговое предприятие, признанное excessive chargeback merchant, подвергаются штрафу в размере $100 за каждый chargeback. Из них $30 остаются в системе VISA, а $70 передаются банку-эмитенту для покрытия расходов на формирование отказа от платежа.

В соответствии с Global Merchant Chargeback Monitoring Program еще более жесткие правила применяются к высокорискованным ТП (MCC 5962,5966,5967,7995). Для таких Интернет-магазинов ТП объявляется excessive chargeback merchant, если зафиксировано одновременное выполнение трех условий:

- количество chargeback по ТП за месяц составляет не менее 100;
- количество международных электронных покупок по ТП за месяц составляет не менее 100;
- отношение общего количества chargeback к количеству международных продаж превышает 2,5 %.

Высокорискованнное торговое предприятие, признанное excessive chargeback merchant, подвергаются штрафу:

- в размере $100 за каждый chargeback с 1-го по 3-й месяцы работы ($70 передаются эмитенту, остальные остаются в платежной системе);
- в размере $150 за каждый chargeback с 4-го по 6-й месяцы работы ($120 передаются эмитенту, остальные остаются в платежной системе).

После 6 месяцев система VISA может дисквалифицировать ТП и запретить ему прием карт этой платежной системы.

Стандарты в области электронной коммерции

На страницах этой книги уже рассказывалось о таких стандартах в области протоколов ЭК, как SET, 3D SET, 3D SSL, 3D Secure.

Помимо стандартов, определяющих авторизационно-расчетную часть общего процесса ЭК, появляются стандарты, описывающие процессы сбора данных в области торговли и обмена данным между ТП и клиентом. Так, в июне 1999 г. такими лидерами в области ЭК, как America Online, American Express, Compaq, CyberCash, IBM, MasterCard, Microsoft, SETCo, Sun Microsystems, Transactor Networks, Trintech и VISA USA, был объявлен стандарт ECML (Electronic Commerce Modelling Language). Это открытый стандарт, позволяющий любой торговой организации принять и обработать данные от электронного бумажника. Он также позволяет владельцу бумажника быстро заполнить поля бланка своими данными (имя, адрес, реквизиты карты и т. п.) и автоматически передает введенные данные в ТП. Пользователю бумажника для этого достаточно выбрать функцию autofill (автоматическое заполнение). Такой подход принято называть One Click Shopping. Клиенту достаточно выбрать только логотип платежной системы, заполнение остальной части формы автоматически производится электронным бумажником.

Средствами ECML также легко реализуется заполнение формы по отказу от уже осуществленной транзакции. При этом форма автоматически заполняется на основе данных уже сделанной транзакции. Следует отметить, что простота заполнения форм заказа является чрезвычайно важным фактором в ЭК. Исследования показывают, что около 35-40 % всех транзакций так и не рождаются из-за того, что покупателю не удается заполнить и отправить форму торгового предприятия правильным образом.

Поставщики программного обеспечения уже поставляют на рынок продукты, совместимые со стандартом ECML (например, электронный бумажник Consumer Wallet фирмы IBM).

Необходимо также отметить широкое применение при написании программного обеспечения для ЭК языка XML (Extensive Mark-up Language), представляющего собой сокращенный вариант наиболее универсального языка описания информации SGML (Standard Generalized Mark-up Language — ISO 8879). В частности, широко известный язык HTML является лишь одним из документов, создаваемых с помощью XML. Вероятно, в ближайшее время XML займет центральное место в написании приложений для ЭК.

XML является тэговым языком, позволяющим быстро и удобно описывать новые данные на основе правил Document Type Description, что, в свою очередь, позволяет ускорять и делать более точными поиски в Web, автоматически загружать необходимые данные, расширять возможности ЭК на новые устройства, включая сотовые телефоны.

Другим важным стандартом в области ЭК является Internet Open Trading Protocol (IOTP), определяющий общую логическую архитектуру (модель) системы ЭК (версия 1.0 этого стандарта появилась в октябре 1999 г.). Протокол IOTP не зависит от схемы платежей и позволяет использовать для расчетов через Интернет различные платежные инструменты, включая SET, Mondex, DigiCash, CyberCash, GeldCarte и т. п. Протокол на основе модели обычной торговой сделки определяет логические субъекты последней и процессы взаимодействия этих субъектов (процессы определения участников сделки, способа платежа, метода доставки товара и т. д.). Описываемая стандартом IOTP модель отображает процесс совершения покупки, совершаемой по обычной «бумажной» технологии. Стандарт широко использует язык XML для описания структуры и содержимого сообщений, применяемых для предложений по продаже, соглашения сторон совершить покупку, сообщений о платежах, доставке товаров и их получении, о разрешении конфликтов.

Наконец, следует сказать о стандарте JEPI G°i[nt; Electronic Payment Initiative), явившемся результатом усилий, координируемых консорциумом World Wide Web Consortium и компанией CommerceNet. JEPI обеспечивает интерфейс, позволяющий Web-браузеру и электронному бумажнику использовать различные протоколы платежей (SSL, SET, электронные чеки, электронные деньги и т. п.). JEPI полезен тем, что позволяет покупателю и продавцу применять единый интерфейс для выбора различных средств оплаты товара, предпочитаемых покупателем.

Правовые аспекты использования электронной коммерции

Некоторые вопросы, связанные с правовым обеспечением электронной коммерции, уже обсуждались при рассмотрении проблем защиты информации от несанкционированного доступа и использования электронной наличности для расчетов за электронные покупки.

Сегодня существует ряд юридических проблем, затрудняющих использование Интернет-коммерции.

Во-первых, до 1 января 2001 г. существовал юридический казус, связанный с тем, что в соответствии с законом «О банках и банковской деятельности» операции с пластиковыми карточками не отнесены к банковским, а значит, могут подпадать под налогообложение. И только юридические ухищрения, связанные с возможностью расширительного толкования банковских операций на основе некоторых прецедентов, дают возможность вывести их из-под налогообложения.

1 января 2001 г. вступила в действие вторая часть Налогового Кодекса РФ, исправившая ситуацию с налогообложением операций по пластиковым картам.

Во-вторых, существует Положение ЦБ РФ №23-П «О порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием», позволяющее совершать торговые операции через Интернет с оплатой товаров с помощью пластиковой карточки. В Разделе 1 этого Положения допускается составление «документа по операциям с использованием банковских карт» не только с использованием самой банковской карты, но и ее реквизитов, как это и происходит при покупках через Интернет.

Однако реквизиты банковской карты, сообщаемые ее владельцем торговому предприятию, не могут претендовать на роль аналога собствен-

норучной подписи владельца карты. Поэтому при совершении электронной покупки нарушаются требования к форме расчетного документа, который в соответствии с действующим гражданско-правовым законодательством должен быть заверен собственноручной подписью покупателя или ее аналогом (абз. 1 п. 1 и п. 2 ст. 160 ГК — Гражданского Кодекса).

Положение ЦБ РФ №23-П не предусматривает того, что нарушение формы документа по операциям с использованием банковских карт влечет его недействительность, равно как и не предусматривает иные последствия такого нарушения. Следовательно, их нужно искать в общегражданском законодательстве.

ГК устанавливает, что последствиями нарушений простой письменной формы сделки является невозможность в случае спора ссылаться в подтверждение ее (сделки) и ее условий на свидетельские показания, но не недействительность сделки как таковой. При этом за сторонами сохраняется право ссылаться на письменные и другие доказательства (п. 1 ст. 162 ГК). Такими доказательствами могут быть подписанное держателем карточки уведомление о вручении ему товара или другие документы, подтверждающие его доставку. Однако если таких документов нет, факт совершения сделки доказать будет невозможно.

Поэтому товары заказчику рекомендуется посылать заказным почтовым отправлением и сохранять подписанные им квитанции о доставке в течение некоторого времени. Только в таком случае можно выиграть спор либо в арбитражном суде платежной системы, либо в общегражданском суде. При торговле же виртуальными товарами ситуация представляется в рамках существующего законодательства неразрешимой.

Ситуация меняется при применении протоколов электронной коммерции, использующих аналоги собственноручной подписи (например, SET). Применение аналогов собственноручной подписи при совершении операций через Интернет приведет эти операции в соответствие с требованиями действующего законодательства.

Поскольку любой платеж — это исполнение денежного обязательства, то к платежам в Интернете должны применяться нормы о безналичных расчетах, содержащиеся в главе 46 Гражданского Кодекса РФ (далее — ГК). Данная глава оперирует понятием «форма безналичных расчетов», определение которого ГК не дает. По смыслу использования этого понятия становится ясно, что формой безналичных расчетов является определенный способ исполнения денежного обязательства, который обеспечивается свойственным только ему комплексом обязательственных отношений.

Таким образом, та или иная модель платежей в Интернете является специфической формой безналичных расчетов, которая может быть принципиально новой или соответствовать уже существующим формам.

В соответствии с п. 1 статьи 862 ГК форма безналичных расчетов считается законной, если она либо предусмотрена законом и установленными в соответствии с ним банковскими правилами, либо подпадает под категорию «применяемого в банковской практике обычая делового оборота».

Остановимся подробнее на этих двух основаниях. Первое кажется более очевидным. Под «банковскими правилами», установленными в соответствии с законом, следует понимать нормативные акты ЦБ РФ как компетентного органа, устанавливающего правила осуществления расчетов в России.

Единственный вопрос, который может возникнуть в связи с этим основанием, — насколько правомерна форма безналичных расчетов, если она установлена нормативными актами Банка России, а соответствующий закон еще не принят? Ответ на него дает практика российского нормотворчества, в соответствии с которой в качестве временной меры допускается регулирование подзаконными актами отношений, которые должны быть урегулированы законом.

Более трудным является анализ второго основания существования форм безналичных расчетов — «применяемого в банковской практике обычая делового оборота». Под «обычаем делового оборота» действующее законодательство понимает «...сложившееся и широко применяемое в какой-либо области предпринимательской деятельности правило поведения, не предусмотренное законодательством, независимо от того, зафиксировано ли оно в каком-либо документе» (п. 1 ст. 5 ГК). Приведенное определение содержит три существенные черты. Обычай делового оборота — это такое правило поведения в сфере предпринимательской деятельности, которое:

- сложилось, то есть постоянно и достаточно определено в своем понимании;
- широко применяется;
- не предусмотрено действующим законодательством.

Поскольку приведенные критерии являются слишком общими, в каждом конкретном случае может быть трудно установить наличие или отсутствие обычая делового оборота. В этом случае практика большое значение придает закреплению потенциального обычая в актах отечественных и особенно международных торговых палат и иных авторитетных в данной области организаций.

На данный момент можно с уверенностью сказать, что под определение «применяемого в банковской практике обычая делового оборота» подпадают операции с платежными картами, также являющиеся особой формой безналичных расчетов.

И последнее, что представляется важным отметить в связи с общими положениями о безналичных расчетах, — это правило части 3 статьи 861 ГК, в соответствии с которым «безналичные расчеты производятся через банки, иные кредитные организации, в которых открыты соответствующие счета, если иное не вытекает из закона и не обусловлено используемой формой расчетов». В соответствии с действующим законодательством, помимо кредитных организаций, расчеты могут осуществляться:

- путем зачета взаимных требований;
- с использованием векселей.

Первый способ не применим к платежам в Интернете, а что касается второго, то статья 4 Федерального закона «О простом и переводном векселе» устанавливает, что любой вексель должен быть составлен только на бумажном носителе.

Таким образом, с использованием электронных технологий расчеты могут осуществляться только через кредитные организации. В соответствии с п. 2.1 Положения ЦБ РФ «О проведении безналичных расчетов кредитными организациями в Российской Федерации» «расчеты в безналичном порядке между кредитными организациями, филиалами могут производиться через:

- расчетную сеть Банка России;
- кредитные организации по корреспондентским счетам «ЛОРО» и «НОСТРО»;
- небанковские кредитные организации, осуществляющие расчетные операции;
- внутрибанковскую расчетную систему (счета межфилиальных расчетов).

По общему правилу, существование расчетного документа в электронной форме возможно при соблюдении следующих условий: заверения документа способом, являющимся аналогом собственноручной подписи уполномоченного лица (уполномоченных лиц), и существования предварительного (письменного) соглашения о порядке его использования.

Поскольку, как об этом говорилось ранее, электронные расчеты возможны только через кредитные учреждения, то они должны иметь со-

ответствующую банковскую лицензию, как это определено Законом «О банках и банковской деятельности» и нормативными актами ЦБ РФ.

В случае использования моделей, основанных на логике ценных бумаг, что в соответствии с частью 1 пункта 1 статьи 149 ГК будет считаться бездокументарной ценной бумагой, возникает необходимость получения дополнительно специальной лицензии, дающей право на электронную фиксацию прав, закрепляемых ценной бумагой. Также следует заметить, что электронная фиксация прав, закрепляемых ценной бумагой, возможна только в случаях, определенных законом или в установленном им порядке.

Очевидно, что основная цель платежей в Интернете, — ускорение гражданского оборота и придание дополнительных удобств его субъектам. Однако эта цель не может быть достигнута без адекватного механизма разрешения возможных споров. Существующая система гражданских и арбитражных судов не может справиться с этой задачей и по причине больших сроков разбирательства дел, и по причине неподготовленности судей к такого рода процессам.

Естественный выход из этой ситуации — создание специальных третейских судов, не имеющих указанных недостатков. Однако этому препятствует несовершенное гражданско-процессуальное законодательство России. В соответствии с существующим порядком третейские суды для разбирательств споров между гражданами могут быть созданы только для рассмотрения конкретного спора после его возникновения и только на безвозмездной основе. Но самым главным недостатком законодательства является то, что оно не предусматривает возможности рассмотрения третейским судом спора между физическим и юридическим лицом.

В связи с вышеизложенным возникает необходимость внесения изменений в законодательство.

При обсуждении протоколов электронной коммерции в этой книге не раз делался вывод о том, что без создания инфраструктуры центров сертификации невозможно построить систему электронных платежей, обеспечивающую необходимый уровень безопасности электронных покупок. Вот почему так важно принятие закона об электронно-цифровой подписи (ЭЦП), который бы гарантировал признание ЭЦП законодательством и российскими органами власти.

Нужно отметить, что закону об ЭЦП уделяется достаточное внимание (к середине 2001 г. различными комитетами Государственной Думы вынесены на рассмотрение три различных проекта этого закона) и есть шанс того, что к концу 2001-началу 2002 г. закон будет принят.

Существуют также проекты закона об электронной коммерции (в России они чаще называются законами об электронной торговле). Государственные органы власти в последнее время проявляют к проблемам развития ЭК в России устойчивый интерес. В частности, в начале 2000 г. был обнародован проект программы развития электронной торговли в России, подготовленный совместно Минсвязи, Минторгом, ФАПСИ и РАСУ. Программа рассчитана на период с 2001 по 2006 гг. и предполагает расходы в размере 54 млн рублей из федерального бюджета. В соответствии с программой развития электронной торговли в России предполагается, что к 2003 г. в России будет сформирована необходимая нормативно-правовая база ЭК, гармонизированная с рекомендациями и правилами международных организаций.

Анализ действующего законодательства России позволяет сделать вывод о том, что правовой аспект при разработке различных моделей платежей в Интернете имеет большое значение, поскольку не все модели будут правомерны. Вместе с тем следует отметить положительную по отношению к электронному документообороту тенденцию как в общегражданском законодательстве, так и в нормативных актах Банка России. По состоянию на сегодняшний день наиболее соответствующей законодательству является модель платежей в Интернете с использованием реквизитов платежной карты. Они являются правомерными и с точки зрения форм безналичных расчетов, и с точки зрения лицензирования.

Основные выводы

В мире уже сейчас существует и быстро развивается в перспективе колоссальный по своим размерам рынок электронной коммерции. В России этот рынок станет представлять серьезный коммерческий интерес примерно через 3-5 лет.

Ни у кого не возникает сомнений в том, что банки, активно занимающиеся обслуживанием предприятий торговли и сервиса по покупкам, совершаемым с использованием пластиковых карт, в ближайшее время возьмут на вооружение технологию электронной коммерции.

Несомненно также, что на первых этапах развития электронной коммерции пластиковые карты будут играть доминирующую роль в качестве инструмента для безналичных расчетов по электронным покупкам. В ближайшие годы платежные системы на основе пластиковых карт будут оставаться единственной универсальной инфраструктурой безналичных расчетов, гарантирующих возврат средств продавцу за оказанные им услуги и проданные товары.

Очень важно отметить существование международных стандартов в области электронной коммерции. Наличие стандартов обеспечивает совместимость программных средств разных производителей и тем самым является необходимым условием для начала широкомасштабного внедрения новой технологии.

К сожалению, в области стандартизации протоколов проведения расчетов по пластиковым картам еще будут происходить изменения. Это связано и с неудачным опытом внедрения протокола SET, и с появлением нового стандарта 3D Secure, претендующего на роль глобального стандарта аутентификации, и с влиянием новых технологий в области средств доступа в Интернет. Видимо, пройдет еще некоторое время, прежде чем появится стандарт, признанный и поддерживаемый всеми крупнейшими международными платежными системами. Очень важно, чтобы этот стандарт избежал ошибок, допущенных при внедрении SET. В этом смысле представляются высокими шансы протокола 3D Secure. Протокол дешев в реализации и оставляет немало степеней свободы эмитентам и обслуживающим банкам для реализации процедур аутентификации соответственно покупателей и продавцов.

Очевидно, что пластиковые карты с магнитной полосой не являются идеальным средством расчетов в Интернет-коммерции. На смену им придут микропроцессорные карты, реализующие надежные алгоритмы динамической аутентификации владельца карты. Другое направление развития расчетов в электронной коммерции — электронная наличность.

Многое предстоит сделать и в области законодательства. Для России большое значение будет иметь принятие законов об электронно-цифровой подписи и об электронной торговле, позволяющих на юридической основе решать всевозможные диспуты, время от времени возникающие при совершении электронных покупок.

Несмотря на то что электронная коммерция находится в самом начале своего развития, накопленный опыт и разработанные протоколы позволяют уверенно утверждать, что уже сегодня можно приступать к реализации широкомасштабных проектов, обеспечивая при этом необходимый уровень безопасности проведения транзакций.

Алфавитный указатель