ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

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

Минск БГУИР 2009

УДК 681.326.7 : 336.71 (075.8)
ББК 32.973.26-018.2+65.262 я73
З-40

Р е ц е н з е н т ы :
проректор по учебной работе УО
«Академия управления при Президенте Республики Беларусь»,
доцент, доктор физико-математических наук В. А. Богуш;
кафедра «Автоматизированные системы управления»
УО «Военная Академия Республики Беларусь»

А в т о р ы :
Л. М. Лыньков, Т. В. Борботько, Н. И. Мухуров,
Б. И. Беляев, Л. В. Катковский

Защита информации в банковских технологиях: учебно-метод. пособие / З-40 Л. М. Лыньков [и др.]. – Минск : БГУИР, 2009. – 198 с.

ISBN 978-985-488-352-6

В пособии рассмотрена специфика электронной коммерции. Особое внимание уделено современным технологиям, широко используемым в банковской деятельности, а также методам и средствам обеспечения их безопасности. После каждого раздела предложен ряд вопросов для самоконтроля студентов.

УДК 681.326.7 : 336.71 (075.8)
ББК 32.973.26-018.2+65.262 я73

ISBN 978-985-488-352-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение безопасного информационного обмена является важнейшей задачей современности, которая тесно взаимосвязана с различными сферами жизнедеятельности человека. Особое внимание сегодня уделяется защите прав собственника информационных ресурсов, систем, технологий и средств их обеспечения, что реализуется в правовых, организационных и технических методах защиты, широко применяемых на практике.

В процессе информационного обмена задействуется большое количество различного оборудования, связанного как с обработкой информации, так и с ее доставкой потребителю. Современные телекоммуникационные системы позволяют в короткие промежутки времени обеспечить доставку сообщений в любую точку мира. Таким образом, путь, который проходит единичное сообщение, как правило, имеет значительную протяженность, что не может не сказываться на безопасности тех данных, которые передаются таким путем.

Современные информационные технологии активно внедряются в банковской сфере, что позволяет банкам предоставить клиентам широкий спектр услуг, в том числе обеспечить возможность проведения удаленных транзакций, и тем самым увеличить число клиентов. Несомненные удобства таких взаимодействий, с одной стороны, порождают проблему аутентификации и авторизации клиента и обеспечения банковской тайны и защищенного информационного обмена, – с другой. Поэтому проблема обеспечения информационной безопасности банковских систем является весьма актуальной.

1. ДЕНЬГИ И ПЛАТЕЖНЫЕ СИСТЕМЫ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

1.1. Механизмы классических денег

Развитие натурального товарного обмена (иначе говоря, бартера) привело к выделению из массы товаров одного, который стал играть роль всеобщего эквивалента. Сначала роль этого эквивалента стали играть драгоценные металлы, в основном золото и серебро. Следующий этап – появление чеканных из металла монет. Металлические деньги делятся на полноценные (номинальная стоимость которых равна стоимости содержащихся в них драгоценных металлов) и неполноценные (номинальная стоимость которых выше стоимости содержащихся в них драгоценных металлов). На смену металлическим деньгам пришли «знаки» денег, роль которых взяли на себя бумажные деньги. Бумажные деньги являются «представителями» полноценных денег, самостоятельной стоимости они не имеют, но наделяются принудительным курсом, назначаемым государством. Сегодня стоимость денег соответствует нарицательной стоимости, не зависящей от материала, из которого они изготовлены [1].

Бумажное денежное обращение создает много проблем, которые имеют место во всех странах, даже высокоразвитых. Бумажные деньги неустойчивы, подвержены инфляции. Велика вероятность их подделки. Поэтому возникла необходимость их замены более надежным платежным средством. Появились векселя – долговые бессрочные письменные обязательства должника об уплате определенной суммы через положенный срок; депозиты – вклады на счетах в банках и сберегательные вклады; чеки – письменные приказы владельца счета в банке о выплате определенной в чеке суммы его предъявителю. Наконец, появились пластиковые карточки и электронные деньги, о которых и будет идти речь в настоящей книге.

Деньги выполняют следующие функции:

– средство обращения (средство платежа);

– мера стоимости;

– средство накопления;

– мировые деньги.

Деньги как средство обращения. Когда деньги используются как средства осуществления оплаты за товары и услуги, говорят, что они используются в качестве средства обращения. Значение денег как средства обращения невозможно преувеличить, так как они позволяют уйти от бартерной формы торговли.

Замена бартера денежным обменом отделяет акт продажи от акта покупки. Если существуют деньги, то продавец должен лишь найти того, кто хочет купить его товар.

Деньги, хорошо выполняющие функции средства обращения, с готовностью должны приниматься каждым. Деньги, имеющие широкое распространение, предоставляют их владельцу некую всеобщую покупательную способность. Использование денег позволяет осуществлять гибкий выбор типов и количества покупаемых товаров, выбор времени и места совершения покупки, а также партнеров для сделки. При этом если некоторое средство обращения используется достаточно долго, то его приемлемость становится достаточно стабильной.

Хотя использование денег обычно снижает издержки совершения сделок, бартер все же сохраняется, в некоторых случаях даже возрождается в новых формах. Например, в странах с очень высоким уровнем инфляции торговля с помощью бартера может быть более предпочтительной, чем использование наличных денег. В нормальных экономических условиях примером бартера могут являться всякого рода дополнительные выплаты, такие, как медицинское страхование или страхование пенсий.

Деньги как мера стоимости. В дополнение к функции средства обращения деньги также функционируют в качестве меры стоимости (unit of account),

иначе говоря, денежной единицы, используемой для измерения и сравнения стоимостей товаров и услуг.

Правительство каждой страны устанавливает свою меру стоимости (масштаб цен). В Беларуси мерой стоимости является белорусский рубль, в США – доллар, в Германии – евро и т. д. С помощью меры стоимости стоимость товаров и услуг измеряется так же, как измеряются вес или длина.

Деньги как мера стоимости однородны, что очень важно для вычислений и ведения записей о совершаемых сделках. Выражая цены в денежных единицах, можно сопоставлять и сравнивать стоимости различных товаров немедленно и без особых усилий.

Деньги как средство накопления. Третья функция денег – быть средством накопления (store of value), т. е. особого рода активом, сохраняемым после продажи товаров и услуг и обеспечивающим его владельцу покупательную способность в будущем. Деньги подходят для выполнения этой функции, поскольку им присуща ликвидность. Ликвидным называется такой актив, который может быть использован как средство платежа (или легко превращен в средство платежа) и сохраняет свою номинальную стоимость неизменной.

Итак, термином «деньги» обозначают средство, которое может быть использовано для определения количества каких-либо предметов в системе координат, обычной для всех участников сделки [1]. Деньги определяют покупательную способность в отношении товаров и услуг. Деньги служат стандартом для сравнения различных товаров и услуг. Эти значения субъективны и находятся под влиянием множества факторов, в том числе колебания курсов валют. Деньги являются средством обмена, промежуточной формой в процессе продажи товаров и, таким образом, заменяют бартер. Деньги служат «хранилищем» покупательной способности. Они позволяют производить отсрочку реализации продукции или услуг. Такая сберегательная функция сохраняется при условии, что некоторый общий уровень цен остается стабильным или совсем незначительно увеличивается.

Денежная единица – это знак, обладающий действительной платежеспособностью и принимаемый в качестве платежа в определенном географическом регионе [1]. Платежеспособность основана на юридическом понятии (политическом решении), совмещенном с социальным явлением принятия денег обществом. Денежный знак должен удовлетворять следующим условиям:

– позволять формировать различные суммы;

– должен быть конвертируемым в другие платежные средства;

– должен быть легко распознаваемым в открытом сообществе;

– существовать благодаря тому, что его эмитент пользуется доверием членов сообщества;

– должен быть принудительно защищен законодательством.

Как следствие денежными знаками, имеющими реальную платежеспособность, являются только банкноты установленного образца, выпущенные центральным банком, или монеты, отчеканенные государственным монетным двором. Такие банкноты, иначе называемые ***фидуциарными деньгами*** (fiduciary money), являются всеобщим законным платежным средством на определенной территории, обычно – внутри национальной границы (евро – исключение из правил). Несмотря на то что номинал денежного знака соответствует нарицательной стоимости, отпечатанной на банкноте или монете, реальное значение номинала целиком зависит от эмитента. Однако отметим, что расчет монетами может быть ограничен законодательством.

Банк или любая другая кредитная организация может сделать доступным определенное количество платежных средств для нефинансового агента в обмен на проценты или долю прибыли, пропорциональные рискам и продолжительности операции. Такие деньги называются ***скриптуальными*** (scriptural money); это денежные знаки, основанные на авторитете эмитента в экономической сфере. Если банк выпускает скриптуальные деньги, их покупательная способность целиком зависит от степени доверия к банку и системы гарантий со стороны государственной власти (например центрального банка) при их ис-

пользовании. Заметим, что коммерсант вправе принимать или не принимать платежи скриптуальными деньгами, но обязан принимать фидуциарные деньги. Отметим также, что скриптуальные деньги легко можно отследить, в то время как фидуциарные – практически невозможно.

Материал, из которого изготавливаются классические деньги, должен удовлетворять следующим требованиям:

– простота распознавания;

– относительно стабильная номинальная стоимость;

– прочность;

– простота транспортировки и использования;

– незначительная стоимость производства в сравнении с номинальной стоимостью.

Вся мощь денег может быть передана от одного торгового агента другому с помощью платежных средств.

1.2. Платежные средства

Платежные средства способствуют обмену товаров и услуг и отвечают специфическим требованиям. Каждое средство имеет свою социальную и технологическую историю, определяющую их использование в специфических областях. На сегодняшний день банки предлагают большое количество платежных средств, связанных с автоматической обработкой транзакций и постепенной дематериализацией денег, отличающихся по способу применения в разных странах.

Можно выделить следующие виды платежных средств:

– наличные (cash) (в форме металлических монет или бумажных банкнот);

– чеки (checks);

– кредитные переводы (credit transfers);

– прямое дебетование (direct debits);

– межбанковские переводы (interbank transfers);

– векселя (bills of exchange или negotiable instruments);

– пластиковые карты (payment cards) (кредитные или дебетовые).

Развивающиеся виды платежных средств основаны на дематериализованных деньгах, хранящихся в смарт-картах, электронных или виртуальных кошельках.

Некоторые из таких платежных средств являются всего лишь изобретениями банков и имеют неофициальный статус. К примеру, во Франции кредитные переводы и межбанковские платежи регулируются только Французским комитетом по организации и нормализации банковской деятельности и межбанковскими организациями.

Наличные (cash). В любой стране наличность представляет собой фидуциарные деньги, которые выпускаются центральным банком и государственным казначейством в форме банкнот и монет. Это платежное средство бесплатно для населения. Банки покрывают свои затраты на обслуживание платежей, выдачу наличности в пунктах выдачи наличности или снятие денег с банкоматов путем начисления комиссии за свои услуги, если им приходится обрабатывать большие объемы банкнот или монет и производить соответствующие расчеты и сортировку.

Наличные – самое распространенное средство платежа при сделках, совершаемых физическими лицами (face-to-face commerce). В странах Запада существует тенденция к использованию наличности для сделок на относительно небольшую сумму и скриптуальных инструментов – для средних и больших сделок. Французский комитет потребителей определяет микроплатеж как «платеж, особенно в случае его совершения физическим лицом, для которого, при отсутствии каких-либо специфических ограничений, наличность является наиболее предпочтительным видом платёжного средства» [1].

Так как фальшивые деньги не могут быть обменены на настоящие, то использование наличности основывается на обоюдном доверии сторон. Для поддержания этого доверия власти применяют различные меры безопасности. В частности, защита банкнот основана на использовании специальной бумаги,

которую трудно воспроизвести. Меры защиты применяются в течение всего срока жизни денег, начиная от компонент, используемых при их производстве, и заканчивая уничтожением как ветхих, так и фальшивых банкнот.

Чеки (checks). Чек – денежный документ установленной формы, содержащий безусловное распоряжение чекодателя кредитному учреждению о выдаче держателю чека указанной в нем суммы. Общая стоимость обработки одного чека колеблется между 0,2 и 1 долл. США. Эта сумма включает в себя стоимость полного комплекса мер по выпуску и обслуживанию чека: печать, защита, распространение, процедуры, выполняемые при возврате (сортировка, сверка подписи, сбор вписанных данных, отбраковка и т. д.), архивация, а также стоимость украденных и испорченных чеков, что составляет порядка 1 % от общего их количества. Чек – наиболее дорогое средство платежа, и не только для банков, но и для крупных потребителей.

Денежные переводы (credit transferts). Денежный перевод – это движение средств по счетам по инициативе плательщика. Это платежное средство требует знания плательщиком реквизитов получателя платежа – банка-бенефициара (beneficiary's bank) и номера счета. Денежные переводы используются при массовых платежах (например для выплаты заработной платы или пенсий).

Прямое дебетование (direct debit). Прямое дебетование используется для периодических платежей (например оплата счетов за электроэнергию). Для инициализации прямого дебетования плательщик оформляет длительное поручение на оплату будущих счетов. Поручение может быть оформлено в электронном виде с использованием, например, системы TEP (Titre Electronique de Paiement – система электронных платежей) во Франции или системы Интернет Сервис Банк (ИСБ), разработанной Автобанком, в России. Источники больших счетов, такие как телекоммуникационные компании, находят подобные инструменты очень удобными, но их развитие затруднено общественным недоверием к подобным системам.

Межбанковские переводы (interbank transfers). Система межбанковских переводов Tip впервые была представлена во Франции в 1988 г. Система отличается от обычных переводов тем, что для каждого платежа требуется подпись на специальной форме, поставляемой кредитором. Она легко интегрируется в различные системы удаленных платежей, использующих компьютеры или телефоны. В случае если кредитор все еще пользуется почтовой системой доставки счетов, то с помощью компьютера или телефона клиент может оплатить и подписать счет. Существует две версии системы:

– tele-Tip – подпись передается по каналам Minitel;

– audio-Tip – пользователь аутентифицируется после ввода специального кода по телефону.

Векселя (bills of exchange). Вексель – это платежное средство, предназначенное для профессиональных торговых отношений, предоставляющее должнику (дебитору) или кредитору инициативу платежа. Если дебитор является инициатором платежа, то инструмент называется «простым векселем», или долговым обязательством; если платеж инициирует кредитор, то это тратта. В любом случае кредитор передает документы в банк, который затем пересылает вексель в банк дебитора. Тратта похожа на чек с гарантией платежа и возможностью получения скидки (дисконта) для бенефициара.

Пластиковые карты (payment cards). В зависимости от предлагаемых услуг существует несколько видов пластиковых карт:

– карты гарантии чека (check guarantee cards);

– карты для выдачи наличности (card withdrawal cards);

– банковские платежные карты (bank payment cards);

– дебетовые карты, по которым снятие денег со счета происходит в момент совершения транзакции;

– карты отложенных платежей, по которым платеж происходит в указанную дату, например, в конце месяца;

– кредитные карты;

– карты ограниченного использования (restricted usage cards);

– кредитные карты, такие как American Express или Diner's Card, которые позиционируются как «международные карты отложенных платежей» и отличаются от банковских карт тем, что выпускаются кредитными организациями, имеющими широкую международную сеть филиалов;

– частные карты (private fidelity cards), выпускаемые торговцами для удержания клиентов и предлагающие набор кредитных услуг (с помощью кредитных организаций); одно из применений таких карт – сбор информации о потребителе для проведения маркетинговых кампаний;

– карты для различных потребностей бизнеса;

– корпоративные карты, позволяющие компании оптимизировать представительские траты сотрудников;

– закупочные карты, представляющие собой дебетовые карты, используемые для разовых платежей на небольшие суммы; если держатель карты представляет предприятие при закупке товаров, то при расчетах используется счет этого предприятия; при обработке транзакций по таким картам создается весь необходимый пакет документов финансовой отчетности.

Правила проведения операций с банковскими картами предполагают присутствие дополнительных участников при проведении сделки между покупателем и продавцом (англ. merchant), а именно: банков каждой из сторон и системы банковских карт, например Visa или MasterCard. Банк поставщика товаров или услуг называется банком-эквайером, или банком-получателем платежа (англ. acquirer), банк покупателя – банком-эмитентом, он выпускает карты для своих клиентов (англ. issuer). Платежные системы предусматривают использование серверов авторизации, подключенных к операторским центрам (call center), чья функция заключается в фильтрации незаконных транзакций. Процесс фильтрации использует некий заранее установленный критерий, к примеру, лимит суммы на транзакцию или количество транзакций в единицу времени. На завершающей стадии производятся окончательные расчеты (клиринг) между

банками, для которых используется национальная или международная система платежей (рис. 1.1).

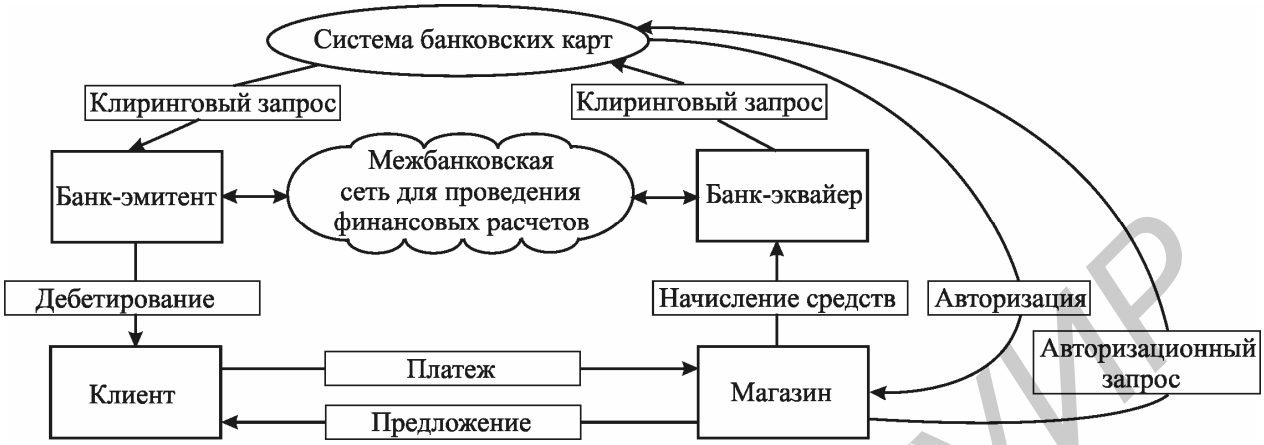


Рис. 1.1. Проведение транзакции с использованием банковских карт

По аналогичной схеме должны осуществляться платежи по банковским картам с использованием открытой сети Интернет. Новое поколение банковских карт (микропроцессорных или смарт-карт) характеризуется большей скоростью вычислений и большей емкостью запоминающего устройства. Такие карты предоставляют возможность защищать транзакции электронной коммерции на качественно новом уровне, в дополнение к повышенному уровню безопасности других небанковских приложений.

1.3. Клиринг и взаиморасчет

Понятия «клиринг» (clearance) и «взаиморасчет» (settlement) между финансовыми институтами помогают выделить основные принципы функционирования системы скриптуальных платежей [1]. Исторически взаиморасчет происходил между представителями банков, которые ежедневно встречались в специальной палате для сравнения взаимных счетов по различным финансовым инструментам и затем производили расчет наличными. Сейчас для передачи данных используют компьютерные сети. Однако уникальный ход эволюции финансовых потоков в каждой стране привел к различным требованиям к безопасности и разнообразию форматов используемых клиринговых систем.

Так, в Европе существует несколько различных моделей клиринга, а модель США совершенно отличается от европейских.

С технической точки зрения различаются и европейские клиринговые структуры. Во Франции, Италии и Испании существуют как региональные, так и национальные системы. Параллельно в Германии, Бельгии, Португалии существуют несовместимые с ними двусторонние и многосторонние системы, а Великобритания имеет централизованную клиринговую систему.

Классификация клиринговых сетей может базироваться на некоторых из нижеследующих критериев:

– характер процессинга:

– системы для крупных платежей;

– системы массовых платежей на относительно небольшие суммы;

– принадлежность и менеджмент сети:

– публичная сеть в собственности центрального банка;

– частная сеть, принадлежащая группе банков;

– частная сеть, арендуемая банками;

– способ взаиморасчетов:

– в режиме реального времени;

– с использованием неттинга (netting), иначе говоря, взаимной компенсации требований и обязательств;

– с использованием группировки при расчетах между подразделениями одних и тех же компаний для исключения многократной уплаты налогов.

В США существует две основные клиринговые системы – Fedwire и CHIPS (Clearing House Interbank Payment System – клиринговая межбанковская платежная система). Fedwire – это сеть Федеральной резервной системы (ФРС), предназначена для операций в реальном масштабе времени. Она используется для проведения небольшого количества транзакций с большими суммами. Напротив, CHIPS – частная система, управляемая New York Clearing House Association (Нью-Йоркской ассоциацией клиринговых палат). При проведении

взаиморасчетов в системе производится консолидация операций организаций – членов ассоциации.

Наряду с федеральной системой существует частная система, находящаяся под надзором ФРС, которая предназначена для проведения крупных платежей. Она включает в себя 32 региональные клиринговые палаты, подчиняющиеся NACHA (National Automated Clearinghouse Association – Национальная система клиринговых палат США), расположенной в Вашингтоне. Система называется ACH (Automated Clearinghouse – автоматизированная клиринговая система). Она была разработана NACHA как частная организация, вовлеченная в систему электронного перевода платежей EFT (Electronic Fund Transfer).

Для обмена информацией используются следующие форматы:

– CCD (cash concentration and disbursement) – концентрация наличности и денежные расходы;

– CTP (corporate trade payments) – корпоративные торговые платежи;

– CTX (corporate trade exchange) – корпоративный торговый обмен.

Среди перечисленных форматов CCD является обязательным для всех организаций – членов NACHA, в то время как поддержка CTP и CTX необязательна. CCD используется для переводов и прямого дебетования и не требует интероперабельности (возможности взаимодействия) информационных систем различных организаций. В данном формате чек выглядит как набор полей по 94 символа в каждом, для заметок и приложений зарезервировано поле на 34 символа. Эти дополнения не стандартизованы, что затрудняет создание систем автоматической обработки сообщений.

В соответствии с форматами CTP и CTX сообщения формируются блоками по 99 байт каждый, в одно сообщение можно объединить до 4999 блоков. Формат CTX создавался под влиянием ANSI ASC (American National Standards Institute, Accredited Standards Committee – Национальный институт стандартизации США, Комитет общепринятых стандартов) и позволяет использовать по-

ля переменной длины. Этот стандарт хорошо поддается автоматизации и используется для EFT.

Клиринговые операций в Великобритании производятся тремя основными операторами. Их можно классифицировать по виду используемых инструментов:

– BACS (Banker's Automated Clearing Service – Банковский автоматизированный клиринговый сервис), основанный в 1968 г. В настоящий момент является крупнейшей и старейшей в мире автоматизированной клиринговой системой.

– Cheque & Credit Clearing Company Ltd (Чековая и кредитная клиринговая компания) – ориентирована на операции с чеками и «бумажными» инструментами.

– CHAPS (Clearinghouse Automated Payment System – Клиринговая автоматизированная платежная система) – специализируется на крупных переводах.

Данные для BACS передаются магнитной ленте, дискетах или по телефону с использованием системы BACSTEL. Аутентификация в BACSTEL осуществляется посредством одноразового пароля, формируемого для каждой транзакции специальным терминалом.

Французская клиринговая система представлена несколькими подсистемами, ранжированными по объему проводимых транзакций. Так, для небольших сумм используется система клиринговых домов (chambres de compensation), Creic (Centre Regionaux d'Eehanges d'Images-Cheques – Региональные центры обмена изображениями чеков) и SIT (Systeme Interbancaire de Telecompensation – Межбанковская система удаленного клиринга), введенная в эксплуатацию в 1995 г. SIT работает непрерывно и предназначена для постепенной замены предыдущих двух систем. Для работы с большими суммами используется клиринговый дом Парижа; сеть SAGITTAIRE предназначена для обеспечения международных транзакций; переводы осуществляются через Центральный банк Франции (Banque de France).

Для связи SIT использует сеть X 25, Transpac; используются также протоколы защиты информации для соединений типа «точка-точка» («point-to-point»), регламентированные CFONB в 1988 г.:

– ETEBAC5 (Echange Telematique entre les Banques et Leurs Clients – телематический обмен данными между банком и клиентом);

– PESIT (Protocole de Transfert de Fichier pour le Systeme Interbancaire de Telecompensation – протокол файлового обмена для межбанковских систем удаленного клиринга).

По стандарту сообщения ETEBAC5 содержат поля фиксированной длины. Протокол предоставляет различные функции обеспечения безопасности в части целостности сообщений, конфиденциальности информации, двусторонней аутентификации участников информационного обмена, а также невозможности отказа от полученного сообщения.

1.4. Типы дематериализованных денег

В 1980-х гг. появилось несколько видов нематериальных валют. Это было вызвано растущей популярностью предоплаченных карт, например телефонных карт, успехом Minitel во Франции. Рассмотрим три вида дематериализованных денег: электронные, виртуальные и цифровые [1].

Электронные деньги (electronic money)

Согласно определению Банка международных расчетов (BIS – Bank for International Settlements), электронные деньги могут быть определены как «денежная стоимость, измеренная в фидуциарных единицах и хранящаяся в электронном устройстве, принадлежащем потребителю или доступном для него». Таким образом, это не что иное, как мобильное скриптуальное средство платежа, хранящее суммы в единицах платежа в неком электронном хранилище. Это определение главным образом соотносится с двоичной формой скриптуальных денег, хранящихся в неком портативном устройстве, например

смарт-карте. ***Скриптуальный характер*** электронных денег связан со статусом эмитента (так как они выпускаются не центральным банком), а также с возможностью оперативного контроля транзакций и движения денег.

Единицы платежа, содержащиеся в картах или в программном обеспечении, покупаются либо за наличные, либо путем пополнения банковского счета. Покупательная способность таких условных единиц ограничена кругом организаций, принимающих платежи.

Виртуальные деньги (virtual money)

Виртуальные деньги отличаются от электронных тем, что их поддержка, представление и способ использования нематериальны. Они могут содержаться в программном обеспечении, поддерживающем платежи по открытым сетям, таким, как Интернет. Можно рассматривать виртуальные деньги как ссылку на некоторый счет (например банковский). Скриптуальный характер виртуальных денег также привязан к статусу эмитента (они не выпускаются центральным банком) и к возможности отслеживания транзакции.

В особых случаях виртуальные деньги могут принимать вид виртуальных токенов (или жетонов), выпускаемых ответственным эмитентом для ограниченного использования. Жетоны отличаются от электронных версий официальных платежных средств тем, что имеют уникальное назначение и ограниченное хождение. В этом состоит их отличие от электронных денег, которые представляют собой многофункциональное, повсеместно признаваемое платежное средство. Например, Millicent представляет собой систему, предлагающую для расчетов виртуальный жетон – скрип (scrip). Поставщик услуг эмитирует скрип, который не связан напрямую с банковской системой, но является предоплаченной услугой – обещанием выполнить услугу в будущем. Поставщик услуги может эмитировать жетоны и даже привязывать их к собственным банковским счетам, оставаясь в рамках закона до тех пор, пока хождение выпущенных жетонов ограничено и строго регламентировано. Телефонные карты являются

особым типом виртуальных кошельков, выпускаемых телефонными компаниями. Это предоплаченные карты, предназначенные для оплаты услуг телефонной связи определенного оператора. Покупательная способность карты выражается в условных единицах – «телефонных жетонах».

Межбанковские отношения строго регулируются законодательством и находятся под наблюдением руководящих денежно-кредитных учреждений в каждой стране. Предполагается, что правом печатать деньги обладает только центральный банк. Причина, по которой телефонные карты вообще разрешены, кроется в том, что телефонные токены предоставляют услуги, которые будут оказаны в будущем, оплаченные законными деньгами. К тому же банкам в подобных ситуациях очень трудно предложить другой вариант процедур оплаты и сбора сумм.

Пример использования телефонных карт, как одноразовых, так и перезаряжаемых, может стимулировать телефонные компании выступать посредниками в электронной коммерции, особенно в случае микроплатежей. Однако это требует перехода от режима «виртуального кошелька» к режиму «электронного кошелька». Другими словами, значение, хранимое в телефонной карте (например «условные единицы»), должно восприниматься как новые скриптуальные универсальные деньги, представленные в двоичной форме. Это порождает новую проблему регулирования денежных потоков для представителей власти.

Цифровые деньги (digital money)

Как и обычные деньги, каждая цифровая купюра имеет свой серийный номер, однако поддержка таких денег виртуальна, значение номинала хранится в виде алгоритма в памяти компьютера пользователя, на жестком диске или в памяти смарт-карты.

Как будет показано далее, одной из поразительных особенностей цифровых денег DigiCash является то, что «печатает» эти деньги клиент, а их подлинность подтверждается банком. Кредитор, получающий цифровые деньги в об-

мен на продукт или услугу, проверяет их подлинность при помощи открытого ключа банка-эмитента. Таким образом гарантируется анонимность, но возникает проблема передачи стоимости между участниками сделки без вмешательства банка-эмитента. К тому же вследствие того что каждый шаг алгоритма ассоциирован с фиксированной суммой, сложности возникают со сдачей.

На новом этапе дематериализации цифровая денежная единица превращается в денежный знак, наделенный реальной покупательной способностью, который может использоваться для платежей в максимально широком экономическом пространстве. Обмен стоимостью происходит в реальном времени в сети, использующей зашифрованные цифровые монеты, однако расчет может происходить как в реальном, так и не в реальном времени. Цифровые деньги могут быть обменены на реальные в банковских организациях после проверки их подлинности по специальной базе данных, которая может быть централизованной или распределенной.

Одной из характеристик, отличающих цифровые деньги от других электронных средств платежа, является возможность совершения полностью анонимных транзакций, т. е. транзакций, в которых отсутствует связь между собственно средством платежа и личностью его держателя, как это происходит в случае фидуциарных денег. Дестабилизирующим аспектом цифровых денег является возможность появления универсальных денег, не зависящих от действующей денежной системы. По этой причине попытки создания цифровых денег связаны со всевозможными проблемами технического и законодательного характера. Действительно, международная цифровая валюта будет конфликтовать с различными региональными и национальными валютами и в результате создавать проблемы экономике отдельных стран. Иначе говоря, создание таких денег является не только технологической проблемой, но затрагивает национальный суверенитет.

1.5. Кошельки

По определению BIS ***электронный кошелек*** – «перезаряжаемая, многофункциональная предоплаченная карта, используемая в розничной торговле и других платежах коммерции face-to-face» [1]. Такое средство платежа может по желанию его владельца служить заменителем других форм денег. Таким образом, электронный кошелек – это устройство с памятью, в которой учитываются средства, которыми физически обладает владелец кошелька. В памяти содержится предварительно записанное значение – сумма денег, которая может служить инструментом обмена в открытом денежном обращении.

Защита содержимого кошелька основана на невозможности создания фальшивой карты или осуществления операций с ячейками памяти. В данном случае идея «открытого использования» подразумевает беспрепятственное использование средств платежа независимо от эмитента. Такая идея «открытости» отличается от случая телекоммуникационных сетей, где сеть может быть открытой или закрытой в зависимости от используемых протоколов (стандартизированных или проприетарных).

Применение электронных кошельков зависит от эмитента (торговое предприятие, банк, торговая ассоциация и т. п.) и его прав по закону. Банковские сети по определению открыты всюду, где электронные деньги соответствуют официальной валюте. Напротив, кошелек, эмитированный не банком, имеет ограниченное использование, так как он содержит только жетоны, которые имеют ограниченное хождение и используются для предопределенных транзакций с привлечением эмитента.

Кошельки электронных жетонов аналогичны частным средствам платежа, таким, как ресторанные купоны. Наиболее часто используемые кошельки такого типа – телефонные карты, дающие право на предоплаченное телефонное соединение.

Электронные кошельки привлекательны для банков, потому что они позволяют снизить стоимость транзакции и заменить собой монеты, билеты или

чеки на небольшие суммы. Они могут рассматриваться как кибернетическая форма дорожных чеков, впервые представленных American Express в 1980 г.

Электронные кошельки и кошельки электронных жетонов уже доказали свою экономическую эффективность в коммерции face-to-face и автоматизированных платежах. Они имеют преимущество перед традиционными платежными картами, которые не подходят для микроплатежей и даже для face-to-face-коммерции, так как стоимость транзакции вполне может превысить размер платежа. Тем не менее возможно объединение электронного кошелька и кошелька электронных токенов на одной карте, поддерживающей несколько приложений. Торговец может быть связан с банком и выпускать дисконтные карты (fidelity card), одновременно предлагая кредиты (под управлением банка). В табл. 1.1 отражены финансовые и законодательные отличия между электронными кошельками и кошельками электронных жетонов.

Таблица 1.1

Сравнение электронных кошельков и кошельков электронных жетонов

Характеристика	Электронный кошелек	Кошелек электронных жетонов
Выражение покупательской способности	Официальное платежное средство	Потребительские единицы
Единицы платежа	Универсальные: любой платеж на указанной территории	Зависит от элемента
Гарант покупательской способности	Банк	Поставщик услуг
Начисление суммы производится	Банком или его агентом	Не регулируется
Тип финансовых операций	Открытие	Закрытие

Виртуальные кошельки и кошельки виртуальных жетонов

Виртуальный кошелек представляет собой счет, на который предначислены единицы официальных денег, учитываемых не банком (например виртуальным магазином). Микроплатежи осуществляются при онлайн-доступе к такому

виртуальному кошельку при помощи ПО, установленного на персональный компьютер клиента.

Платежная система функционирует следующим образом. Оператор открывает в своем банке несколько субсчетов к своему основному счету. Субсчета затем привязываются к абонентам системы – покупателям или продавцам. Субсчета клиентов-покупателей называют виртуальными кошельками, субсчета продавцов – виртуальными кассовыми аппаратами. Кошелек называется «виртуальным», потому что хранимая в нем сумма физически не ощутима, до нее нельзя дотронуться; тем не менее хранимая сумма относится к официальному средству платежа.

Покупательная способность клиента отражается в виртуальном кошельке – субсчете к основному счету оператора; на жестком диске своего компьютера клиенты имеют копию баланса субсчета. Там же содержатся файлы, необходимые для криптографических операций. Такая организация хранения информации выигрышна с той точки зрения, что информация не теряется при сбое в компьютере клиента.

При каждом заказе дебетуется виртуальный кошелек покупателя и кредитуется виртуальный кошелек продавца на сумму транзакции за вычетом комиссии оператора. Через некоторые установленные интервалы времени оператор совершает платеж в пользу каждого продавца на общую сумму, аккумулированную в виртуальном кассовом аппарате. Группировка сумм до совершения такого компенсационного платежа позволяет системе быть экономически обоснованной для проведения микроплатежей.

В принципе кошельки виртуальных жетонов могут использоваться для микроплатежей через Интернет, например, при покупке/продаже информации или других виртуальных продуктов. Покупательная способность будет выражаться в единицах «обещаний» предоставления или потребления услуги определенного поставщика. Это значение, выраженное в жетонах, хранится в памяти и может использоваться ограниченным количеством приложений – только в

транзакциях, где поставщики зарегистрированы оператором платежной системы. Однако у оператора может возникнуть проблема с кредитной организацией. Дело в том, что оператор стремится привлечь как можно большее число клиентов своей системы, в то время как кредитная организация может работать только в сфере легальных денежных отношений.

Вопросы для самоконтроля

1. Какие функции выполняют деньги?
2. Приведите примеры фидуциарных и скриптуальных денег.
3. Каково назначение платежных средств?
4. Приведите примеры платежных средств.
5. Что называется клирингом?
6. По каким критериям можно классифицировать клиринговые сети?
7. Какие форматы сообщений используются для обмена информацией в рамках технологии электронного перевода платежей?
8. Приведите примеры крупных клиринговых сетей.
9. Чем различаются электронные, виртуальные и цифровые деньги?
10. Какие функции выполняют электронные кошельки?

2. ПОЛИТИКА БЕЗОПАСНОСТИ

2.1. Понятие и модели политики безопасности

Политика безопасности – набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе [2]. Она должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

Политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер, программно-технических средств и определяющих архитектуру системы защиты. Ее реализация для конкретной АБС (автоматизированной банковской сети) осуществляется при помощи средств управления механизмами защиты.

Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации, используемых программных и технических средств, расположения организации и т. д.

Под «системой» будем понимать некоторую совокупность субъектов и объектов и отношений между ними.

Субъект – активный компонент системы, который может явиться причиной появления потока информации от объекта к объекту или изменения состояния системы.

Объект – пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации.

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к ее объектам. Название этого способа, как правило, определяет название политики безопасности.

Для изучения свойств способа управления доступом создается его формальное описание – математическая модель. При этом модель должна отражать состояния всей системы, ее переходы из одного состояния в другое, а также учитывать, какие состояния и переходы можно считать безопасными в смысле данного управления. Без этого говорить о каких-либо свойствах системы, и тем более гарантировать их, по меньшей мере некорректно. Отметим лишь, что для разработки моделей применяются различные математические методы (моделирование, теории информации, графов, автоматов и другие).

В настоящее время широко применяются два вида политики безопасности: избирательный и полномочный, основанные соответственно на избирательном и полномочном способах управления доступом. Особенности каждой из них, а также их отличия друг от друга будут описаны ниже.

Кроме того, существует набор требований, усиливающий действие этих видов политики и предназначенный для управления информационными потоками в системе.

Следует отметить, что средства защиты, предназначенные для реализации какого-либо из названных выше способов управления доступом, только предоставляют возможности надежного управления доступом или информационными потоками. Определение прав доступа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т. д.) входит в компетенцию администрации системы.

Избирательная политика безопасности

Основой избирательной политики безопасности является избирательное управление доступом (ИУД; Discretionary Access Control, DAC), которое подразумевает следующее:

– все субъекты и объекты системы должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной.

Матрица доступа (рис. 2.1) представляет собой прямоугольную матрицу, в которой объекту системы ($O_1 \ldots O_n$) соответствует строка, а субъекту ($C_1 \ldots C_n$) – столбец. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение» (Read Only), «доступ на запись» (Write Only), «доступ на чтение-запись» (Read-Write) и др.

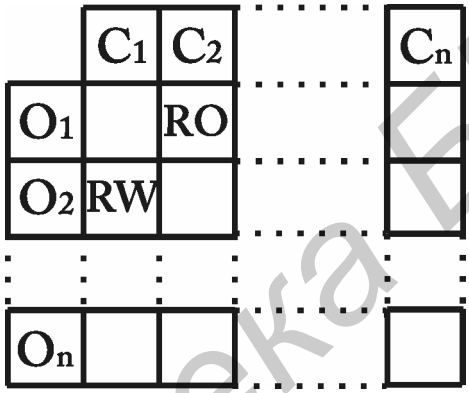


Рис. 2.1. Матрица доступа

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей ИУД. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (датозависимое условие), часы (времязависимое условие) в зависимости от других характеристик субъекта (контекстно-зависимое условие) или характера предыдущей работы. Такие условия доступа к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение о доступе субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно

избирательное управление доступом реализует принцип «что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту.

Матрица доступа – наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных АБС.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД. Каждый из этих способов представления МД имеет свои достоинства и недостатки, обуславливающие область их применения. Поэтому в каждом конкретном случае надо знать, во-первых, какое именно представление использует средство защиты и, во-вторых, какие особенности и свойства имеет это представление.

Избирательное управление доступом является основой требований к классам С2 и С1 стандарта США «Критерий оценки безопасности компьютерных систем» (Trusted Computer Systems Evaluation Criteria, известен как «Оранжевая книга»).

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности (accountability), а также имеет приемлемую стоимость и небольшие накладные расходы.

Полномочная политика безопасности

Основу полномочной политики безопасности составляет полномочное управление доступом (Mandatory Access Control, MAC), которое подразумевает следующее:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

В случае если совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру, поэтому в системе можно реализовать иерархически не исходящий (по ценности) поток информации (например от рядовых исполнителей к руководству). Чем важнее объект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападула (Bell-LaPadulla model), включающая в себя понятия безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: простым условием защиты (simple security condition) и *-свойством (*-property). В упрощенном виде они

определяют, что информация может передаваться только «наверх», т. е. субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него – если не выше (*-свойство).

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Полномочное управление доступом составляет основу требований к классу B1 («Оранжевая книга»), где оно используется совместно с избирательным управлением.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая требованиям последней иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах МО США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами:

– отсутствием в коммерческих организациях четкой классификации хранимой и обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);

– высокой стоимостью реализации и большими накладными расходами.

Управление информационными потоками

Помимо управления доступом субъектов к объектам системы проблема защиты информации имеет еще один аспект.

Для того чтобы получить информацию о каком-либо объекте системы, вовсе не обязательно искать пути несанкционированного доступа к нему. Можно получать информацию, наблюдая за работой системы и, в частности, за обработкой требуемого объекта. Иными словами, при помощи каналов утечки информации. По этим каналам можно получать информацию не только о содержимом объекта, но и о его состоянии, атрибутах и т. д. в зависимости от особенностей системы и установленной защиты объектов. Эта особенность связана с тем, что при взаимодействии субъекта и объекта возникает некоторый поток информации от субъекта к объекту (информационный поток, information flow).

Информационные потоки существуют в системе всегда. Поэтому возникает необходимость определить, какие информационные потоки в системе являются «легальными», т. е. не ведут к утечке информации, а какие – ведут. Таким образом, возникает необходимость разработки правил, регулирующих управление информационными потоками в системе.

Для этого необходимо построить модель системы, которая может описывать такие потоки. Такая модель разработана Гогеном и Мисгаером (Goguen-Meseguer model) и называется потоковой. Модель описывает условия и свойства взаимного влияния (интерференции) субъектов, а также количество информации, полученной субъектом в результате интерференции.

Управление информационными потоками в системе не есть самостоятельная политика, так как оно не определяет правил обработки информации. Управление информационными потоками применяется обычно в рамках избирательной или полномочной политики, дополняя их и повышая надежность системы защиты. В рамках полномочной политики оно является основой требований к классу B2 стандарта «Оранжевая книга».

Управление доступом (избирательное или полномочное) сравнительно легко реализуемо (аппаратно или программно), однако оно неадекватно реальным АБС из-за существования в них скрытых каналов. Тем не менее управление доступом обеспечивает достаточно надежную защиту в простых системах,

не обрабатывающих особо важную информацию. В противном случае средства защиты должны дополнительно реализовывать управление информационными потоками. Организация такого управления в полном объеме достаточно сложна, поэтому его обычно используют для усиления надежности полномочной политики: восходящие (относительно уровней безопасности) информационные потоки считаются разрешенными, все остальные – запрещенными.

Отметим, что кроме способа управления доступом политика безопасности включает еще и другие требования, такие как подотчетность, гарантии и т. д.

Избирательное и полномочное управление доступом, а также управление информационными потоками – вот на чем строится вся защита.

2.2. Механизмы защиты

Основой ДВБ (достоверной вычислительной базы) является ***ядро безопасности*** (security kernel) – элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам [3].

Ядро безопасности является реализацией концепции монитора ссылок (reference monitor) – абстрактной концепции механизма защиты.

Помимо ядра безопасности ДВБ содержит также механизмы, отвечающие за жизнедеятельность системы. К ним относятся планировщики процессов, диспетчеры памяти, программы обработки прерываний, примитивы ввода-вывода и другие программно-аппаратные средства, а также системные наборы данных.

Под монитором ссылок понимают концепцию контроля доступа субъектов к объектам в абстрактной машине. Схематически монитор ссылок изображен на рис. 2.2.

Под базой данных защиты (security database) понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам. Основу

базы данных защиты составляет матрица доступа (МД), которая служит основой избирательной политики безопасности, или ее представления.

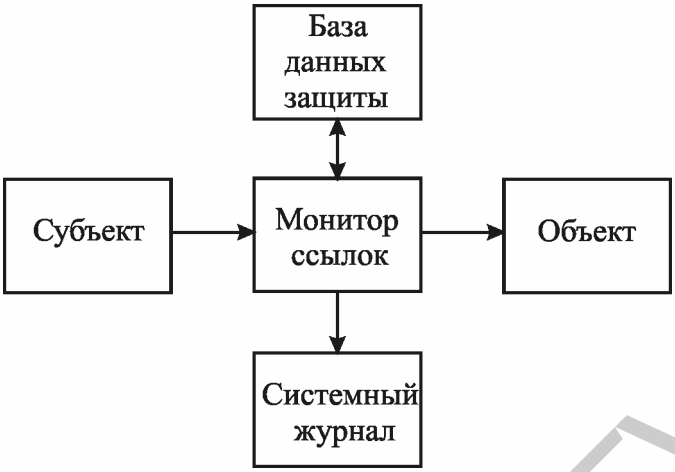


Рис. 2.2. Концепция монитора ссылок

Любая операционная система, поддерживающая ИУД, использует МД и операции над ней, поскольку МД – удобный инструмент контроля использования и передачи привилегий. Однако вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих системах используют более экономные представления МД: по строкам, по столбцам, поэлементно.

1. *Профиль (profile)*

Профилем называется список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым субъектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа. Таким образом, МД представляется своими строками.

В системах с большим количеством объектов профили могут иметь большие размеры и вследствие этого ими трудно управлять; изменение профилей нескольких субъектов может потребовать большого количества операций и привести к трудностям в работе системы. Поэтому профили обычно используются лишь администраторами безопасности для контроля работы субъектов, однако такое их применение весьма ограничено.

2. *Список контроля доступа (access control list)*

Это представление МД по столбцам – каждому объекту соответствует список субъектов вместе с их правами. В современных условиях списки контроля доступа (СКД) – лучшее направление реализации ИУД, поскольку это очень гибкая структура, предоставляющая пользователям много возможностей.

3. *Мандат, или билет (capability, или ticket)*

Это элемент МД, определяющий тип доступа определенного субъекта к определенному объекту (т. е. субъект имеет «билет» на доступ к объекту). Каждый раз билет выдается субъекту динамически – при запросе доступа, и также динамически билет может быть изъят у субъекта. Поскольку распространение билетов происходит очень динамично и они могут размещаться непосредственно внутри объектов, то вследствие этого контроль за ним очень затруднен. В чистом виде билетный механизм хранения и передачи привилегий используется редко. Однако реализация других механизмов присвоения привилегий (например с использованием СКД) часто осуществляется с помощью билетов.

При реализации полномочной политики безопасности база данных защиты также содержит метки критичности всех объектов и уровни прозрачности субъектов системы.

Монитор ссылок должен выполнять следующие функции:

1. Проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты и положений политики безопасности (избирательной или полномочной).

2. При необходимости регистрировать факт доступа и его параметры в системном журнале.

Реализующее монитор ссылок ядро безопасности должно обладать следующими свойствами:

– контролировать все попытки доступа субъектов к объектам;

– иметь защиту от модификации, подделки, навязывания;

– быть протестированным и верифицированным для получения гарантий надежности;

– иметь небольшой размер и компактную структуру.

В терминах модели Белла-Лападула (избирательном и полномочном видах политики безопасности) монитор ссылок должен контролировать состояния системы и переходы из одного состояния в другое. Основными функциями, которые должно выполнять ядро безопасности совместно с другими службами ОС, являются:

1. ***Идентификация, аутентификация и авторизация субъектов и объектов системы***

Эти функции необходимы для подтверждения подлинности субъекта, законности его прав на данный объект или на определенные действия, а также для обеспечения работы субъекта в системе.

Идентификация – процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

Аутентификация – проверка идентификатора (подлинности) пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

Авторизация – предоставление субъекту прав на доступ к объекту.

Эти функции необходимы для поддержания разрешительного порядка доступа к системе и соблюдения политики безопасности: авторизованный (разрешенный) доступ имеет только тот субъект, чей идентификатор удовлетворяет результатам аутентификации. Они выполняются как в процессе работы (при обращении к наборам данных, устройствам, ресурсам), так и при входе в систему. Во втором случае имеются отличия (см. далее п. 2).

2. ***Контроль входа пользователя в систему и управление паролями***

Эти функции являются частным случаем перечисленных выше: при входе в систему и вводе имени пользователя осуществляется идентификация, при вводе пароля – аутентификация, и если пользователь с данными именем и паролем зарегистрирован в системе, ему разрешается доступ к определенным объектам и ресурсам (авторизация). Однако при входе в систему существуют отличия при выполнении этих функций. Они обусловлены тем, что в процессе работы система уже имеет информацию о том, кто работает, какие у него полномочия (на основе информации в базе данных защиты) и т. д., и поэтому может адекватно реагировать на запросы субъекта. При входе в систему это все только предстоит определить. В данном случае возникает необходимость организации «достоверного маршрута» (trusted path) – пути передачи идентифицирующей информации от пользователя к ядру безопасности для подтверждения подлинности. Как показывает практика, вход пользователя в систему – одно из наиболее уязвимых мест защиты; известно множество случаев взлома пароля, входа без пароля, перехвата пароля и т. д. Поэтому при выполнении входа и пользователь, и система должны быть уверены, что они работают непосредственно друг с другом, между ними нет других программ и вводимая информация истинна.

Достоверный маршрут реализуется привилегированными процедурами ядра безопасности, чья работа обеспечивается механизмами ДВБ, а также некоторыми другими механизмами, выполняющими вспомогательные функции. Они проверяют, например, что терминал, с которого осуществляется вход в систему, не занят никаким другим пользователем, который имитировал окончание работы.

3. ***Регистрация и протоколирование. Аудит***

Эти функции обеспечивают получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных администрацией потенциально опасными для безопасности системы. Такими средствами могут быть различные системные

утилиты или прикладные программы, выводящие информацию непосредственно на системную консоль или другое определенное для этой цели устройство, а также системный журнал. Кроме того, почти все эти средства контроля могут не только обнаружить какое-либо событие, но и фиксировать его. Например, большинство систем имеет средства протоколирования сеансов работы отдельных пользователей (всего сеанса или его отдельных параметров).

Большинство систем защиты имеют в своем распоряжении средства управления системным журналом (audit trail). Как было показано выше, системный журнал является составной частью монитора ссылок и служит для контроля соблюдения политики безопасности. Он является одним из основных средств контроля, помогающим администратору предотвращать возможные нарушения. Свойства системного журнала:

– способен оперативно фиксировать происходящие в системе события;

– может помочь выявить средства и априорную информацию, использованные злоумышленником для нарушения;

– может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Содержимое системного журнала и других наборов данных, хранящих информацию о результатах контроля, должны подвергаться периодическому просмотру и анализу (аудиту) с целью проверки соблюдения политики безопасности.

4. ***Противодействие «сборке мусора»***

После окончания работы программы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Она хранится на диске до перезаписи или уничтожения. После выполнения этих действий на освободившемся пространстве диска находятся «остатки» информации.

При изменении заголовка файла эти «остатки» прочитать трудно, однако с помощью специальных программ и оборудования такая возможность все-таки

реализуется. Этот процесс называется «сборкой мусора» (disk scavenging). Он может привести к утечке важной информации.

Для защиты от «сборки мусора» используются специальные средства, которые могут входить в ядро безопасности ОС или устанавливаться дополнительно.

5. *Контроль целостности субъектов*

Согласно модели Белла-Лападула множество субъектов системы есть подмножество множества объектов, т. е. каждый субъект одновременно является объектом. При этом под содержимым субъекта обычно понимают содержимое контекста процесса, куда входит содержимое общих и специальных регистров (контекст процесса постоянно изменяется). Кроме содержимого, или значения, субъект имеет ряд специфических атрибутов: приоритет, список привилегий, набор идентификаторов и другие. В этом смысле поддержание целостности субъекта, т. е. предотвращение его несанкционированной модификации, можно рассматривать как частный случай этой задачи для объектов вообще.

В то же время субъект отличается от объекта тем, что является, согласно определению, активным компонентом системы. В связи с этим для защиты целостности субъекта, в качестве представителя которого выступает процесс, вводится такое понятие, как рабочая среда, или область исполнения процесса. Эта область является логически защищенной подсистемой, которой доступны все ресурсы системы, относящиеся к соответствующему процессу. Другими словами, область исполнения процесса является виртуальной машиной. В рамках этой области процесс может выполнять любые санкционированные действия без опасения нарушения целостности. Таким образом, реализуется концепция защищенной области для отдельного процесса.

Контроль целостности обеспечивается процедурами ядра безопасности, контролируемыми механизмами поддержки ДВБ. Основную роль играют такие механизмы, как поддержка виртуальной памяти (для создания области данного

процесса) и режим исполнения процесса (определяет его возможности в рамках данной области и вне ее).

Область исполнения процесса может содержать другие подобласти, которые составляют единую иерархическую структуру системы, или вкладываться в них. Процесс может менять области: это действие называется переключением области процесса (process switching). Оно всегда связано с переходом центрального процессора в привилегированный режим работы.

Механизмы поддержки областей исполнения процесса обеспечивают контроль их целостности достаточно надежно. Однако даже разделенные процессы должны иметь возможность обмениваться информацией. Для этого разработаны несколько специальных механизмов, чтобы можно было осуществлять обмен информацией между процессами без ущерба безопасности или целостности каждого из них. К таким механизмам относятся, например, кластеры флагов событий, почтовые ящики и другие системные структуры данных. Следует, однако, учитывать, что с их помощью может осуществляться утечка информации, поэтому если использование таких механизмов разрешено, их обязательно следует контролировать.

6. Контроль доступа

Под контролем доступа будем понимать ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности. Под доступом понимается выполнение субъектом некоторой операции над объектом из множества разрешенных для данного типа. Примерами таких операций являются чтение, открытие, запись набора данных, обращение к устройству и т. д.

Контроль должен осуществляться при доступе к следующим объектам:

– оперативной памяти;

– разделяемым устройствам прямого доступа и последовательного доступа;

– разделяемым программам и подпрограммам;

– разделяемым наборам данных.

Основным объектом внимания средств контроля доступа являются совместно используемые наборы данных и ресурсы системы. Совместное использование объектов порождает ситуацию «взаимного недоверия», при которой разные пользователи одного объекта не могут до конца доверять друг другу. Поэтому если с этим объектом что-нибудь случится, все они попадают в круг подозреваемых.

Существует четыре основных способа разделения субъектов по отношению к совместно используемым объектам:

1. Физическое – субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т. д.).

2. Временное – субъекты с различными правами доступа к объекту получают его в различные промежутки времени.

3. Логическое – субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа, которые моделируют виртуальную операционную среду «один субъект – все объекты»; в этом случае разделение может быть реализовано различными способами: разделение оригинала объекта, разделение с копированием объекта и т.д.

4. Криптографическое – все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифровки объекта.

Существует множество различных вариантов одних и тех же способов разделения субъектов, они могут иметь разную реализацию в различных средствах защиты.

Контроль доступа субъектов системы к объектам (не только к совместно используемым, но и к индивидуальным) реализуется с помощью тех же механизмов, которые реализуют ДВБ, и осуществляется процедурами ядра безопасности.

2.3. Принципы реализации политики безопасности

Как уже отмечалось, настройка механизмов защиты – дело сугубо индивидуальное для каждой системы и даже для каждой задачи. Поэтому дать ее подробное описание довольно трудно. Однако существуют общие принципы, которых следует придерживаться, так как они проверены практикой [2].

1. Группирование

Это объединение множества субъектов под одним групповым именем; всем субъектам, принадлежащим одной группе, предоставляются равные права (рис. 2.3). Принципы объединения пользователей в группы могут быть самые разные: ссылки на одни и те же объекты, одинаковый характер вычислений, работа над совместным проектом и т. д. При этом один и тот же субъект может входить в несколько различных групп и соответственно иметь различные права по отношению к одному и тому же объекту.

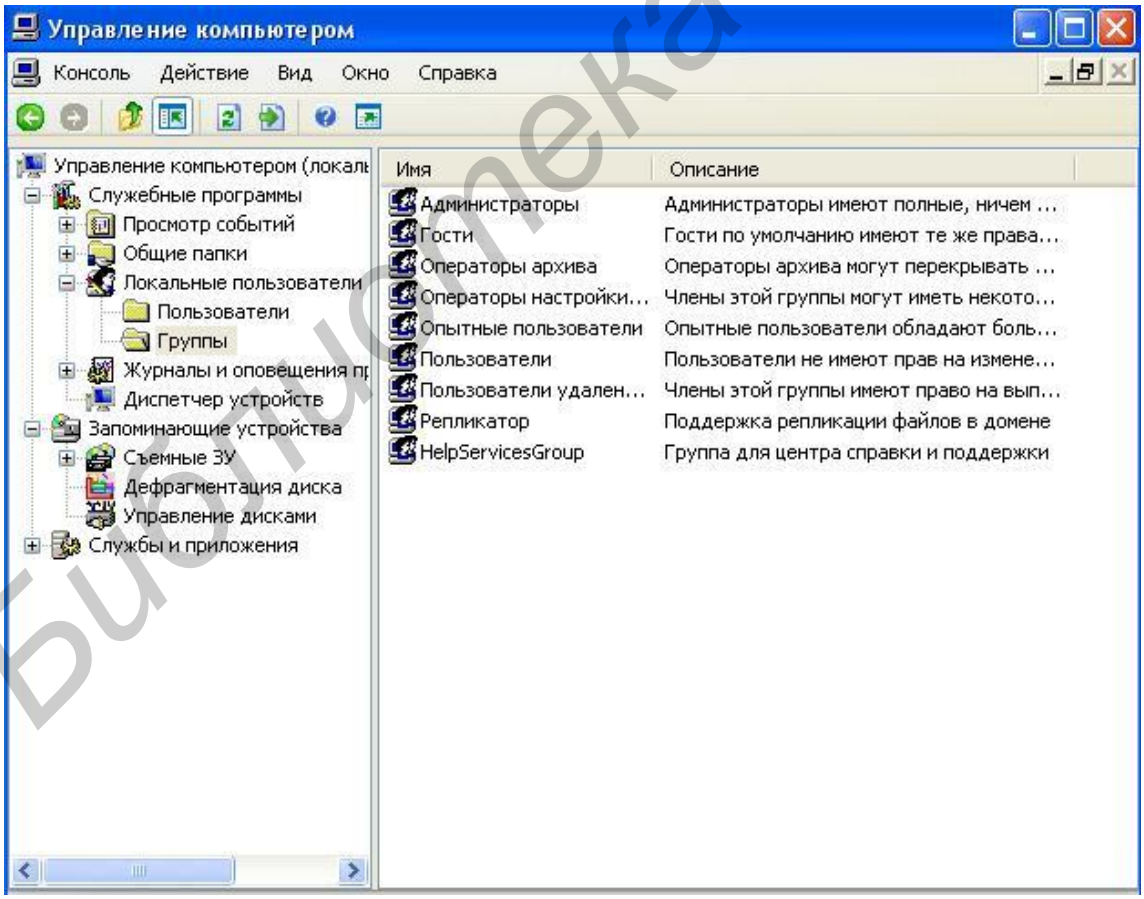


Рис. 2.3. Реализация принципа группирования в Windows XP

Механизм группирования может быть иерархическим. Это означает, что каждый субъект является членом нескольких групп, упорядоченных по отношению «быть подмножеством». Контроль за состоянием групп очень важен, поскольку члены одной группы имеют доступ к большому числу объектов, что не способствует их безопасности. Создание групп и присвоение групповых привилегий – функция администратора безопасности, руководителя группы или какого-либо другого лица, несущего ответственность за сохранность групповых объектов.

2. Правила умолчания

Большое внимание при назначении привилегий следует уделять правилам умолчания, принятым в данных средствах защиты; это необходимо для соблюдения политики безопасности (рис. 2.4.). Например, во многих системах субъект, создавший объект и являющийся его владельцем, по умолчанию получает все права на него. Кроме того, он может эти права передавать кому-либо.

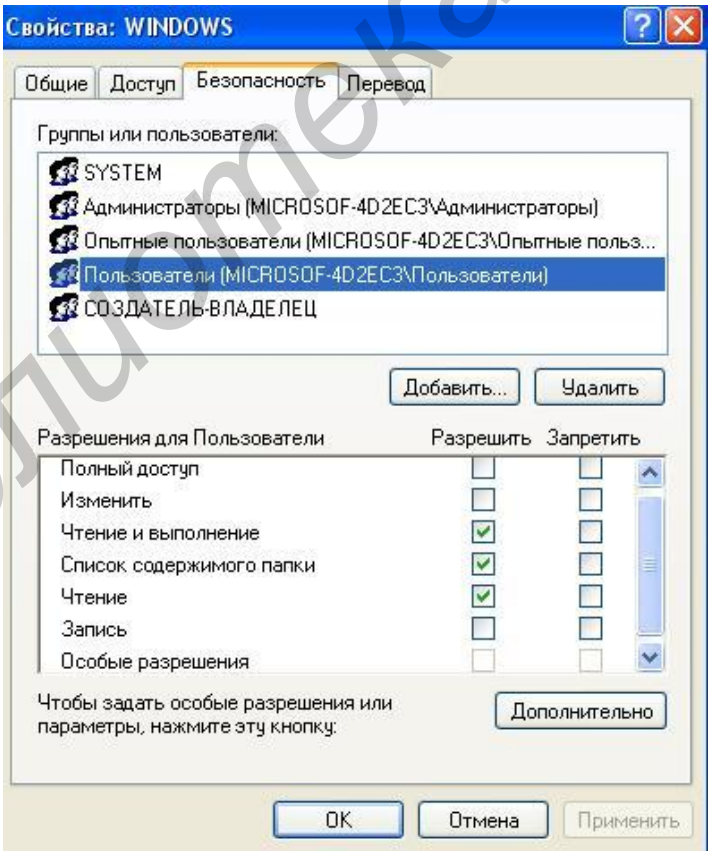


Рис. 2.4. Права доступа (по умолчанию) пользователей группы «Пользователи» к папке Windows

В различных средствах защиты используются свои правила умолчания, однако принципы назначения привилегий по умолчанию в большинстве систем одни и те же. Если в системе используется древовидная файловая структура, то необходимо принимать во внимание правила умолчания для каталогов. Корректное использование правил умолчания способствует поддержанию целостности политики безопасности.

3. Минимум привилегий

Это один из основополагающих принципов реализации любой политики безопасности, используемый повсеместно. Каждый пользователь и процесс должен иметь минимальное число привилегий, необходимое для работы. Определение числа привилегий для всех пользователей, позволяющих, с одной стороны, осуществлять быстрый доступ ко всем необходимым для работы объектам, а с другой, – запрещающих доступ к чужим объектам, – проблема достаточно сложная. От ее решения во многом зависит корректность реализации политики безопасности.

4. «Надо знать»

Этот принцип во многом схож с предыдущим. Согласно ему, полномочия пользователей в свою очередь назначаются согласно их обязанностям. Доступ разрешен только к той информации, которая необходима пользователям для работы.

5. Объединение критичной информации

Во многих системах сбор, хранение и обработка информации одного уровня производятся в одном месте (узле сети, устройстве, каталоге). Это связано с тем, что проще защитить одним и тем же способом большой массив информации, чем организовывать индивидуальную защиту для каждого набора.

Для реализации этого принципа могут быть разработаны специальные программы, управляющие обработкой таких наборов данных. Это будет простейший способ построения защищенных областей.

6. Иерархия привилегий

Контроль объектов системы может иметь иерархическую организацию. Такая организация принята в большинстве коммерческих систем.

При этом схема контроля имеет вид дерева, в котором листья – субъекты системы, ветви – право контроля привилегий согласно иерархии, корень – администратор системы, имеющий право изменять привилегии любого пользователя (рис. 2.5).

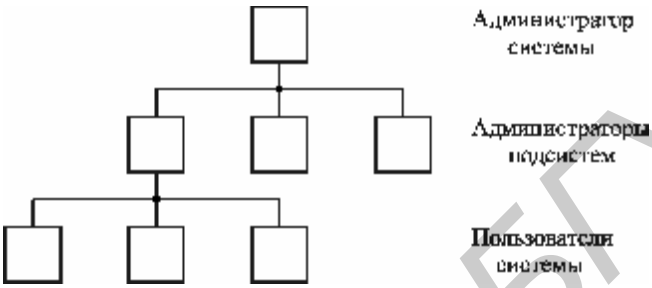


Рис. 2.5. Пример иерархической организации привилегий в АБС

Узлами нижележащих уровней являются администраторы подсистем, имеющие права изменять привилегии пользователей этих подсистем (в их роли могут выступать руководители организаций, отделов). Листьями дерева являются все пользователи системы. Вообще говоря, субъект, стоящий в корне любого поддерева, имеет право изменять защиту любого субъекта, принадлежащего этому поддереву.

Достоинство такой структуры – точное копирование схемы организации, которую обслуживает АБС. Поэтому легко определить множество субъектов, имеющих право контролировать данный объект. Недостаток иерархии привилегий – сложность управления доступом при большом количестве субъектов и объектов, а также возможность получения доступа администратора системы (как высшего по иерархии) к любому набору данных.

7. Привилегии владельца

При таком контроле каждому объекту соответствует единственный субъект с исключительным правом контроля объекта - владелец (owner). Как прави-

ло, это его создатель. Владелец обладает всеми разрешенными для этого типа данных правами на объект, может разрешать доступ любому другому субъекту, но не имеет права никому передать привилегию на корректировку защиты. Однако такое ограничение не касается администраторов системы – они имеют право изменять защиту любых объектов.

Главным недостатком принципа привилегий владельца является то, что при обращении к объекту пользователь должен предварительно получить разрешение у владельца (или администратора). Это может приводить к сложностям в работе (например, при отсутствии владельца или просто нежелании его разрешить доступ). Поэтому такой принцип обычно используется при защите личных объектов пользователей.

8. Свободная передача привилегий

При такой схеме субъект, создавший объект, может передать любые права на него любому другому субъекту вместе с правом корректировки СКД этого объекта. Тот в свою очередь может передать все эти права другому субъекту.

Естественно, при этом возникают большие трудности в определении круга субъектов, имеющих в данный момент доступ к объекту (права на объект могут распространяться очень быстро и так же быстро исчезать), и поэтому такой объект легко подвергнуть несанкционированной обработке. В силу этих обстоятельств подобная схема применяется достаточно редко – в основном в исследовательских группах, работающих над одним проектом (когда все имеющие доступ к объекту заинтересованы в его содержимом).

В чистом виде рассмотренные принципы реализации политики безопасности применяются редко. Обычно используются их различные комбинации. Ограничение доступа к объектам в ОС включает в себя ограничение доступа к некоторым системным возможностям, например, ряду команд, программам и т. д., если при использовании их нарушается политика безопасности. Набор полномочий каждого пользователя должен быть тщательно продуман, чтобы исключить возможные противоречия и дублирования, поскольку большое количество

нарушений происходит именно из-за этого. Может произойти утечка информации и без нарушения защиты, если плохо была спроектирована или реализована политика безопасности.

Политика безопасности и механизмы поддержки ее реализации образуют единую защищенную среду обработки информации. Эта среда имеет иерархическую структуру, где верхние уровни представлены требованиями политики безопасности, далее следует интерфейс пользователя, затем идут несколько программных уровней защиты (включая уровни ОС) и, наконец, нижний уровень этой структуры представлен аппаратными средствами защиты. На всех уровнях, кроме верхнего, должны реализовываться требования политики безопасности, за что, собственно, и отвечают механизмы защиты.

В различных системах механизмы защиты могут быть реализованы поразному; их конструкция определяется общей концепцией системы. Однако одно требование должно выполняться неукоснительно: эти механизмы должны адекватно реализовывать требования политики безопасности.

2.4. Оценка безопасности банковских систем

Основные критерии оценки безопасности систем

Для оценки надежности средств защиты применяются различные критерии. Анализ некоторых критериев показал общность идеи, лежащей в основе подхода к оценке безопасности (степени защищенности) компьютерных систем. Ее сущность состоит в следующем. Для предоставления пользователям возможности обоснованного выбора средств защиты вводится некая система классификации их свойств. Задается иерархия функциональных классов безопасности. Каждому классу соответствует определенная совокупность обязательных функций. Конкретное средство разграничения доступа относится к такому классу безопасности, в котором реализованы все соответствующие ему функции безопасности, если оно не может быть отнесено к более высокому классу [3].

В разных странах за разработку этих документов и проверку средств разграничения доступа на соответствие им отвечают различные организации. Например, в США – это Национальный Центр компьютерной безопасности, в России – Государственная техническая комиссия при Президенте Российской Федерации (в дальнейшем просто ГТК РФ).

Система документов США

В период с 1983 по 1988 гг. в США Министерством обороны и Национальным Центром компьютерной безопасности была разработана система документов в области компьютерной безопасности. В нее вошли:

1. «Критерий оценки безопасности компьютерных систем» (больше известен как «Оранжевая книга»);

2. «Программа оценки безопасности продуктов»;

3. «Руководство по применению критерия оценки безопасности компьютерных систем в специфических средах» (известно под названием «Желтая книга»);

4. «Разъяснение критерия оценки безопасности компьютерных систем для безопасных сетей», «Разъяснение критерия оценки безопасности компьютерных сетей для безопасных СУБД», «Разъяснение критерия оценки безопасности компьютерных систем для отдельных подсистем безопасности» (комплект документов под общим названием «Радужная серия»).

Областью действия «Оранжевой книги» являются операционные системы и программно-аппаратные средства, изменяющие функции операционных систем. Оценка безопасности СУБД и сетей ПК производится по другим документам.

«Оранжевая книга» необходима:

– пользователям – для того чтобы они могли оценить степень доверия к системе, выбираемой для обработки конфиденциальной информации;

– производителям – чтобы они знали требования, предъявляемые к системам защиты информации, и учитывали это в своих коммерческих продуктах;

– разработчикам стандартов – для обеспечения основы разработки других документов в области безопасности.

В документе изложены единые для МО США требования к обеспечению безопасности компьютерных систем и порядок определения классов защищенности компьютерных систем МО США.

В документе выделены общие требования по обеспечению безопасности обрабатываемой информации, определен перечень показателей (показатели защищенности), характеризующих реализацию этих требований. Совокупность показателей определяет уровень безопасности рассматриваемой системы.

Выделено также шесть основных требований безопасности; четыре из них относятся к управлению доступом к информации (политика безопасности, маркировка, идентификация и учет), а два – к предоставляемым гарантиям (уверенность в системе и непрерывность защиты). Эти основные требования конкретизируются в показателях защищенности (табл. 2.1).

Таблица 2.1

Требования защищенности

Наименование показателя	Класс защищенности					
	C1	C2	B1	B2	B3	A1
1	2	3	4	5	6	7
SECURITY POLICY						
1. Discretionary Access Control	+	+	+	=	=	=
2. Mandatory Access Control	–	–	+	+	=	=
3. Labels	–	–	+	+	=	=
4. Labels Integrity	–	–	+	=	=	=
5. Working labels	–	–	–	+	=	=
6. Labels Frequency	–	–	+	=	=	=
7. Object Reuse	–	+	=	+	=	=
8. Resource Encapsulation	–	+	=	–	–	–
9. Exported Machine Readable Output	–	–	+	=	=	=
10. Exported Human-Readable Labels	–	–	+	=	=	=
ACCOUNTABILITY						
11. Identification & Authentication	+	+	=	=	=	=
12. Audit	–	+	+	+	+	=
13. Trusted Path	–	–	–	+	=	=

Окончание табл. 2.1

1	2	3	4	5	6	7
ASSURANCE						
14. Design Specification & Verification	–	–	+	+	+	+
15. System Architecture	+	=	=	+	+	=
16. System Integrity	+	=	=	=	=	=
17. Security Testing	+	+	+	+	+	=
18. Trusted Recovery	–	–	–	–	+	=
19. Configuration Management	–	–	–	+	+	+
20. Trusted Facility Management	–	–	–	+	+	=
21. Trusted Distribution	–	–	–	–	+	=
22. Covert Channel Analysis	–	–	–	+	=	+
DOCUMENTATION						
23. Security Features User's Guide	+	=	=	=	=	=
24. Trusted Facility Manual	+	+	+	+	+	=
25. Test Documentation	+	=	=	+	=	+
26. Design Documentation	+	=	+	+	=	+

Примечание. «–» – нет требований к данному классу; «+» – новые или дополнительные требования; «=» – требования совпадают с требованиями к предыдущему классу.

В документе перечислены подробные требования к реализации каждого показателя защищенности для соответствующего класса. Класс защищенности присваивается системе при прохождении ею сертификации. При сертификации специалисты NCSC на основании представленных исходных текстов программ и документации на систему оценивают уровень реализации той или иной возможности системы по защите информации.

Следует отметить, что сертификации подвергается вся система в целом, а класс защищенности присваивается только в том случае, когда самый «слабый» показатель удовлетворяет его требованиям.

Классы безопасности компьютерных систем в порядке возрастания требований к обеспечению безопасности приведены ниже.

Класс* D: *подсистемы безопасности

Класс D присваивается тем системам, которые не прошли испытаний на более высокий уровень защищенности, а также системам, использующим для защиты лишь отдельные функции (подсистемы) безопасности.

Класс* C1: *избирательная защита

Средства защиты систем класса C1 удовлетворяют требованиям избирательного управления доступом, обеспечивая разделение пользователей и данных. Для каждого объекта и субъекта в системе явно и недвусмысленно задается перечень допустимых типов доступа (чтение, запись и др.) субъекта к объекту.

В системах этого класса обязательна идентификация и аутентификация субъекта доступа, а также поддержка его со стороны оборудования.

Класс* C2*: управляемый доступ

К требованиям класса C1 добавляются требования уникальной идентификации субъекта доступа, защиты по умолчанию и регистрации событий. Уникальная идентификация означает, что любой пользователь системы должен иметь уникальное имя.

Защита по умолчанию предполагает назначение полномочий доступа пользователям по принципу «все что не разрешено, то запрещено». Т. е. все те ресурсы, которые явно не разрешены пользователю, полагаются недоступными.

В системах этого класса обязательно ведение системного журнала, в котором должны отмечаться события, связанные с безопасностью системы. Данные журнала должны быть защищены от доступа любых пользователей, за исключением администратора системы.

***Системы класса* B**

Системы класса B характеризуются реализацией в них полномочного управления доступом, при котором каждый субъект и объект системы снабжается метками (или уровнями) конфиденциальности и решение на доступ субъекта к объекту принимается по определенному правилу на основе сопоставления информации, содержащейся в обеих метках. При этом оборудование должно обеспечить целостность меток безопасности и использование их при разграничении доступа. Системы этого класса предполагают реализацию концепции монитора ссылок. Реализация полномочной политики безопасности имеет в виду использование модели Белла-Лападула, хотя явно это не отражено.

Класс* B1: *меточная защита

Метки безопасности должны быть присвоены всем субъектам и объектам системы, которые могут содержать конфиденциальную информацию. Доступ к объектам внутри системы разрешается только тем субъектам, чья метка (или уровень) удовлетворяет определенному критерию относительно метки объекта. Примером такого критерия являются простое условие безопасности и свойство в модели Белла-Лападула.

При этом необходимо контролировать соответствие меток на данных, экспортируемых из системы, и устройствах, на которые осуществляется их вывод. Метка безопасности на вводимые данные запрашивается у пользователя.

Класс* B2: *структурированная защита

Дополнительно к требованиям класса B1 добавляется требование наличия хорошо определенной и документированной формальной модели политики безопасности, требующей действия избирательного и полномочного управления доступом ко всем объектам системы. Вводится требование управления информационными потоками в соответствии с полномочной политикой безопасности.

Система должна быть четко разделена на чувствительные и нечувствительные к защите элементы. Также предъявляются дополнительные тре-

бования по защите механизмов аутентификации. Интерфейс с ДВБ должен быть хорошо документирован.

Класс* B3: *области безопасности

В оборудовании систем этого класса должна быть реализована концепция монитора ссылок (reference monitor). Все взаимодействия субъектов с объектами должны контролироваться этим монитором. Действия должны выполнятся в рамках областей безопасности, которые имеют иерархическую структуру и защищены друг от друга с помощью специальных механизмов.

Из системы защиты должен быть исключен код, который не требуется для обеспечения поддержки политики безопасности. Механизмы регистрации событий безопасности должны также оповещать администратора и пользователя о нарушении безопасности.

Класс* A1: *верифицированная разработка

Системы этого класса отличаются от класса B3 тем, что для проверки спецификаций применяются методы формальной верификации – анализа спецификаций системы на предмет неполноты или противоречивости, что могло бы привести к появлению уязвимостей в безопасности.

Анализ классов защищенности показывает, что чем он выше, тем более жесткие требования предъявляются к системе. Это выражается не только в расширенном тестировании возможностей системы и представлении расширенной документации, но и в использовании формальных методов проверки правильности спецификаций программ и верификации их текстов.

Система документов России

Руководящие документы (в некоторой степени аналогичные разработанным NSCS) в области защиты информации разработаны ГТК РФ. Требования всех приведенных ниже документов обязательны для исполнения только в государственном секторе либо коммерческими организациями, которые обрабатывают информацию, содержащую государственную тайну. Для остальных коммерческих структур документы носят рекомендательно-консультативный характер.

Руководящие документы ГТК РФ включают:

1) концепцию защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа (НСД) к информации. Этот документ содержит определение НСД, основные способы осуществления НСД, модель нарушителя, основные направления и принципы организации работ по защите информации от НСД;

2) термины и определения в области защиты от НСД к информации. Этот документ вводит в действие основные термины и определения, используемые в других документах;

3) показатели защищенности СВТ от НСД к информации. Этот документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности предъявляемых к ним требований;

4) классификацию автоматизированных систем и требования по защите информации. Документ устанавливает классификацию автоматизированных систем (АС), подлежащих защите от НСД к информации, и требования по защите информации в АС различных классов.

5) временное положение о государственном лицензировании деятельности в области защиты информации. Документ устанавливает основные принципы, организационную структуру системы лицензирования деятельности предприятий в сфере оказания услуг в области защиты информации, а также правила осуществления лицензирования и надзора за деятельностью предприятий, получивших лицензию.

Система документов Республики Беларусь

В сфере информационной безопасности Республики Беларусь на практике нашла широкое применение система документов России, а также используется ряд документов, разработанных в США.

Вопросы для самоконтроля

1. Что называется политикой безопасности?

2. Что составляет основу политики безопасности?

3. Что составляет основу избирательного управления доступом?

4. В чем отличие полномочной политики безопасности от избирательной политики безопасности?

5. В чем смысл управления информационными потоками?

6. Что называется ядром безопасности?

7. В чем сущность концепции монитора ссылок?

8. Какие способы представления матрицы доступа существуют, и в чем их сущность?

9. Какие функции выполняет ядро безопасности совместно с операционной системой?

10. Какие существуют способы разделения совместно используемых объектов различными субъектами?

11. Какие принципы реализации политики безопасности широко используются на практике?

12. В чем заключается сущность оценки безопасности банковских систем?

3. УПРАВЛЕНИЕ ЗАЩИТОЙ АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СЕТИ

3.1. Административная группа управления защитой

Организация группы управления защитой информации, включающей специалистов в этой области, – одна из наиболее важных задач управления защитой автоматизированной банковской сети (АБС). Иногда эту группу называют также группой информационной безопасности [3].

В обязанности входящих в эту группу сотрудников должно быть включено не только исполнение директив вышестоящего руководства, но и участие в выработке решений по всем вопросам, связанным с процессом обработки информации с точки зрения обеспечения его защиты. Более того, все их распоряжения, касающиеся этой области, обязательны к исполнению сотрудниками всех уровней и организационных звеньев. Кроме того, организационно эта группа должна быть обособлена от всех отделов или групп, занимающихся управлением самой системой, программированием и другими относящимися к системе задачами во избежание возможного столкновения интересов.

Несмотря на то, что обязанности и ответственность сотрудников группы информационной безопасности варьируются от организации к организации, можно составить перечень основных функциональных обязанностей сотрудников группы информационной безопасности во всех учреждениях:

1. Управление доступом пользователей системы к данным, включая установку, периодическую смену паролей, управление средствами защиты коммуникаций и криптозащиту предаваемых, хранимых и обрабатываемых данных.

2. Разработка планов защиты. Контроль за их соблюдением, а также контроль за хранением резервных копий.

3. Доведение до пользователей изменений в области защиты, которые имеют к ним отношение, обучение персонала и пользователей АБС.

4. Взаимодействие со службой менеджмента АБС по вопросам защиты информации в АБС.

5. Совместная работа с представителями других организаций по вопросам безопасности - непосредственный контакт или консультации с партнерами или клиентами.

6. Тесное сотрудничество и поддержание хороших отношений со службой менеджмента и администрацией АБС.

7. Расследование происшедших нарушений защиты.

8. Координация действий с аудиторской службой, совместное проведение аудиторских проверок.

9. Постоянная проверка соответствия принятых в организации правил безопасности обработки информации существующим правовым нормам, контроль за соблюдением этого соответствия.

10. Поддержание хороших отношений с теми отделами, чьи задачи могут (по каким-то особым причинам) выполняться в обход существующих правил.

Естественно, все эти задачи не под силу одному человеку, особенно если организация (банк) довольно велика. Более того, в группу управления защитой могут входить сотрудники с разными функциональными обязанностями. Обычно выделяют четыре группы сотрудников (по возрастанию служебной иерархии):

1. Сотрудник группы безопасности

В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема АБС имеет своего сотрудника группы безопасности.

2. Администратор безопасности системы

В его обязанности входит ежемесячная публикация нововведений в области защиты, новых стандартов, а также контроль за выполнением планов не-

прерывной работы и восстановления (если в этом возникает необходимость), а также за хранением резервных копий.

3. Администратор безопасности данных

В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

4. Руководитель (начальник) группы по управлению обработкой информации и защитой

В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах АБС (при децентрализованном управлении).

Существует несколько вариантов детально разработанного штатного расписания такой группы, которые включают перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы.

3.2. Опасные события и их предупреждение

Для того чтобы предотвратить проявление угрозы безопасности или устранить ее последствия, прежде всего надо хорошо представлять, какие вообще возможны угрозы Вашей АБС. Для большинства АБС перечень угроз, которые могут повлечь за собой частичную или полную потерю информации или работоспособности системы и которые мы будем называть опасными, один и тот же. К таким угрозам можно отнести:

1. Перехват информации из линии связи.

2. Перехват паролей.

3. Попытка проникновения в систему.

4. Создание или изменение записей базы данных защиты.

5. Несанкционированное получение и использование привилегий.

6. Несанкционированный доступ к наборам данных.

7. Установка непроверенных выполняемых модулей и командных процедур, которые могут содержать вредоносное программное обеспечение (вирусы).

8. «Сборка мусора» на диске или в оперативной памяти.

9. Использование узлов сети как портов для проникновения в другие узлы сети ЭВМ.

В каждом из этих случаев должны предприниматься срочные меры для предотвращения нарушения работоспособности АБС и сохранения данных.

При этом необходимо особо остановиться на таком опасном нарушении, как несанкционированный доступ. Дело в том, что понятие «несанкционированный» достаточно трудно определить. Чаще всего под НСД понимают проникновение пользователя к информации, которая ему не должна быть доступна. Это возможно в двух случаях:

1. В программно-аппаратных средствах поддержки политики безопасности есть ошибки, приводящие к возможности действий, позволяющих их обход. В этом случае единственный выход – смена средств защиты (внести исправления в рабочем порядке обычно не представляется возможным).

2. Некорректно сформулирована или реализована политика безопасности для данной конфигурации технических и программных средств системы. Следует пересмотреть политику безопасности или способы ее реализации, проверить полноту и однозначность сформулированных требований (этот вопрос лежит больше в плоскости проектирования и реализации средств защиты или политики безопасности, но никак не управления защитой).

НСД может быть обнаружен с помощью средств контроля или явиться побочным эффектом другого нарушения (например вирусной атаки).

Когда систему пытаются «атаковать», умышленно или неумышленно, информацию об этом можно получить из следующих источников:

– от пользователей – о состоянии защиты личных наборов данных отдельных пользователей;

– при мониторинге функционирования АБС – о состоянии общих характеристик системы;

– из системного журнала – о состоянии защиты различных наборов данных.

Пользователи

Пользователи в своей работе постоянно сталкиваются с работой средств защиты. В некоторых ситуациях, когда функционирование таких средств может показаться некорректным, необходимо обращаться к администратору или оператору защиты. Это могут быть следующие ситуации:

– потеря набора данных или ошибки при обращении к нему;

– неудовлетворительное содержание сообщения о последнем входе (зафиксирован более поздний вход в систему, чем был на самом деле);

– неудача при входе в систему (возможно, изменен пароль);

– зафиксирована попытка проникновения и как следствие невозможность входа в систему;

– наличие наборов данных, которые никогда не создавались;

– неожиданные изменения защиты личных объектов пользователя;

– появление листингов, сообщений и др. под именем пользователя, который их не генерировал;

– истощение ресурсов пользователя (например памяти на диске).

Каждая возникающая нестандартная ситуация нуждается в тщательном анализе, его результаты должны быть известны соответствующим пользователям.

Мониторинг функционирования автоматизированной банковской системы

Под мониторингом системы мы понимаем получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля. Такими средствами могут быть различные системные утилиты или прикладные программы, выводящие информацию непосредственно на системную консоль или другое определенное для этой цели устройство. Отличительная особенность мониторинга – получение и анализ информации, осуществляемые в реальном времени.

Ниже перечислены некоторые ситуации возможного нарушения защиты, информацию о которых можно получить с помощью мониторинга:

– в списке пользователей находятся такие, которые не должны в настоящее время работать в системе;

– неожиданные события при загрузке системы;

– нарушения физической защиты – не работают или утеряны носители информации;

– изменения в списке пользователей, допущенных к защищенным файлам;

– появление в системных библиотеках выполняемых модулей, которые не были проверены;

– обнаружение выполнения неизвестных программ при контроле системы;

– добавление неизвестных имен к списку привилегированных пользователей;

– во время сеанса работы пользователей зафиксировано чрезмерно большое время использования процессора – возможно, вследствие НСД;

– в очереди пакетных заданий находятся неизвестные или подозрительные;

– в АБС обнаружены неизвестные устройства;

– наблюдается повышенный уровень загруженности системы;

– неожиданное изменение характеристик системы (средств) защиты;

– изменение характера работы пользователей.

Этот список может быть дополнен еще множеством других ситуаций. Для каждой АБС такой список индивидуален. Здесь приведены лишь наиболее часто встречающиеся ситуации, которые могут сигнализировать о наличии угрозы. Появление каждой из них должно тщательно и своевременно анализироваться, чтобы избежать потенциальной опасности.

Кроме того, средства контроля, как правило, фиксируют сведения о прошедшем событии. Например, большинство систем имеет средства протоколирования сеансов работы отдельных пользователей. Отчеты о сеансах работы помогут обнаружить следующие факты:

– неизвестные имена пользователей;

– настораживающие характеристики сеансов – неурочные часы или дни работы, например, чрезмерное использование ресурсов системы; источники некорректных входов в систему – узлы сети, удаленные терминалы и др.

Системный журнал

Для того чтобы своевременно обнаруживать и предотвращать опасные события, ведется системный журнал (audit trail). Работа с системным журналом является частным случаем мониторинга функционирования АБС, однако его обычно считают самостоятельным средством контроля, забывая о принципиальном различии их целей: в процессе мониторинга осуществляется слежение за общими характеристиками системы, и он осуществляется оператором, а системный журнал регистрирует состояние средств защиты и управляется администратором безопасности.

По ряду причин системный журнал является одним из основных средств контроля, помогающим предотвращать возможные нарушения:

1. В журнале оперативно фиксируются происходящие в системе события, например:

– вводимые команды и имена выполняемых программ;

– доступ к определенным наборам данных или устройствам и его параметры;

– вход и выход пользователей из системы;

– имя терминала или другого устройства, с которого был осуществлен ввод команды или запуск программы;

– случались ли похожие события ранее, и кто (или что) были их причиной;

– другие события.

2. Анализ содержимого системного журнала может помочь выявить средства и априорную информацию, использованные злоумышленником для осуществления нарушения, поскольку очевидно, что без предварительной информации любая сознательная попытка нарушения практически обречена на провал. К такой информации можно отнести:

– сведения об АБС;

– сведения о структуре организации;

– знание параметров входа в систему (имена и пароли);

– сведения об используемом оборудовании и программном обеспечении;

– характеристики сеансов работы и т. д.

Кроме того, анализ содержимого системного журнала может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Естественно, с помощью одного системного журнала не всегда удается определить источник нарушения, однако он несомненно позволяет значительно сузить круг подозреваемых.

В дополнение к перечисленным выше мерам рекомендуется обязательно осуществлять контроль следующих событий с помощью системного журнала:

1. События типа «ошибка входа», или «попытка проникновения» (если «ошибка входа» фиксируется слишком часто, обычно более трех раз подряд). Это лучший способ распознавания попыток проникновения в систему.

2. События типа «вход в систему». Помогает контролировать работу, особенно при доступе к узлу из сети. Такой доступ является источником повышенной опасности.

3. События типа «ошибка при доступе к набору данных». Дает возможность обнаружить попытки преодоления защиты наиболее ценных объектов АБС.

4. Запись (доступ типа WRITE) в наборы данных. Помогает предотвратить их несанкционированную модификацию. При этом необходимо учитывать особенности модификации некоторых системных наборов.

5. Осуществление действий, на которые необходимы различного рода привилегии. Дает возможность выявить злоупотребления ими.

Мониторинг функционирования системы и системный журнал дают умелому администратору мощное средство слежения за функционированием системы. Однако изобилие информации, поступающее в результате мониторинга и анализа системного журнала (рис. 3.1), может быть эффективно обработано лишь при наличии у администратора специальных средств работы с этой информацией.

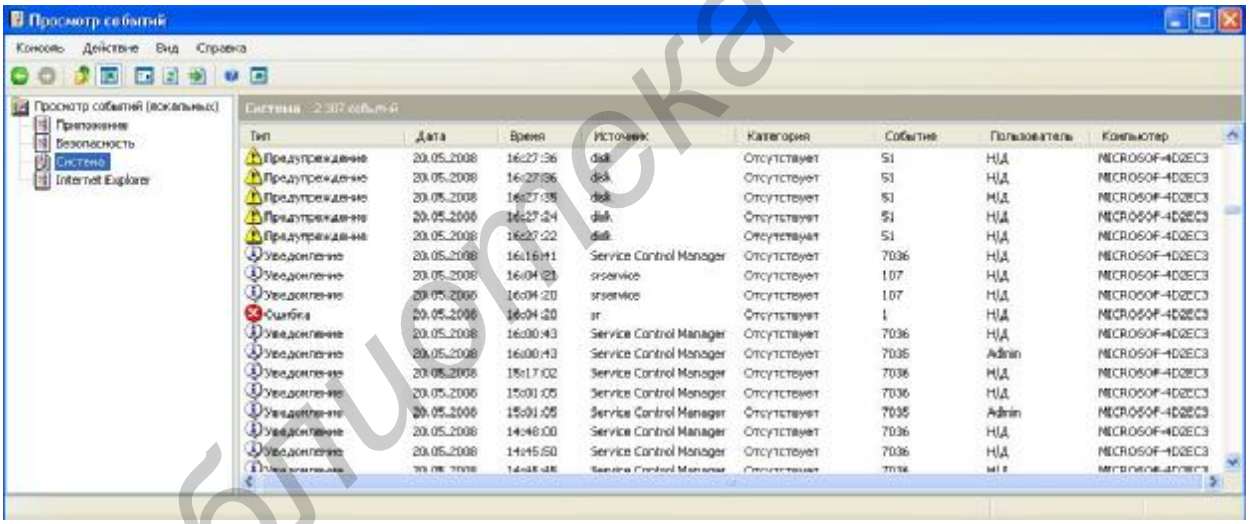


Рис. 3.1. Системный журнал

3.3. Устранение нарушений

Используя информацию, поступающую от пользователей, на основе мониторинга и записей системного журнала, оператор системы должен своевременно обнаруживать нарушения и предпринимать меры по их локализации и устранению. Если его знаний или полномочий недостаточно, то такую работу выполняет администратор безопасности [3].

В случае установления попытки или факта проникновения в систему администратор безопасности или оператор обязан предпринять следующие действия:

1. Локализовать нарушение.

2. Установить личность нарушителя.

3. Предотвратить дальнейшие нарушения.

4. Попытаться устранить последствия нарушения.

Прежде всего необходимо локализовать нарушение, т. е. определить, кто нарушитель, что он делает и что будет делать дальше. Для этого прежде всего необходимо определить круг подозреваемых: кто мог вообще это сделать? Кто обладал необходимыми полномочиями? Кто знал, как это сделать? После этого, используя имеющуюся информацию, сужать этот круг. Например, определив, с какого терминала осуществлено нарушение, в какое время и каким образом, вы значительно сузите круг подозреваемых.

Конкретные действия оператора и/или администратора безопасности в каждом случае определяются особенностями АСОИ и системы защиты.

Каждая попытка нарушения может оказаться удачной или неудачной. В зависимости от этого должны предприниматься соответствующие действия. Рассмотрим этот вопрос более подробно.

Неудачные попытки проникновения

Под неудачными попытками проникновения будем понимать безуспешные попытки угадать или перехватить пароль, а также попытки НСД.

Как правило, они обнаруживаются в следующих случаях:

– пользователи сообщают о неожиданных ошибках входа;

– установлены необычные действия в системе или использование недействительных коммутируемых линий;

– система вывела тревожные сообщения об ошибках входа, попытках проникновения, нарушениях защиты наборов данных;

– обнаружены записи об опасных событиях в системном журнале.

Установить личность нарушителя очень просто с помощью соответствующего вида контроля, если он является пользователем данного узла сети. В этом случае имя нарушителя просто фиксируется в системном журнале вместе с характеристиками нарушения. Далее следуют оргвыводы.

Если нарушитель является пользователем другого узла сети, то свои действия необходимо согласовывать с администратором защиты этого узла. Дело в том, что системный журнал данного узла может зафиксировать только точку входа в систему и характеристики входа. Например, если осуществлено проникновение с удаленного узла, то системный журнал зафиксирует только его имя. С помощью дополнительной информации можно проследить вход в лучшем случае до соседнего узла, т. е. установить имя пользователя, осуществившего вход на данный узел.

Установление нарушителя, осуществившего проникновение издалека с помощью сети, – задача очень сложная и порой неразрешимая. Даже если удастся определить имя нарушителя, то, во-первых, сложно установить, кто скрывается за ним, а во-вторых, наказать его. Последняя задача иногда вообще нереальна. Он может находиться в другой организации, другом городе или за границей. Такие методы применяются лишь в самых крайних случаях, так как они требуют большого количества времени (до месяца и более), труда, привлечения дополнительных специалистов и, следовательно, денежных средств.

Всегда предпочтительнее использовать превентивные меры, чем потом тратить время и деньги на поиск нарушителя (а поиск может и не увенчаться успехом). Единственный надежный способ избежать этих сложностей – установить контроль за проникновением в АСОИ и постараться не допускать его вовсе. Предотвращение попыток проникновения подразумевает действия относительно потенциальных нарушителей и прогнозирует возможное усложнение таких попыток.

Чтобы свести до минимума вероятность успешного перехвата паролей, необходимо выполнить следующие действия:

1. Разрешить определенным пользователям выбор подходящего пароля. Предупреждать их о возможности перехвата пароля. Использовать генератор паролей.

2. Использовать для входа пароль администратора. Это лучший способ защиты от проникновений, доставляющий лишь небольшие дополнительные неудобства пользователям. Если системный пароль уже разрешен, то изменить его.

3. Провести анализ успешных входов в систему для определения возможных проникновений.

Для уменьшения вероятности успешного НСД необходимо выполнить следующие действия:

1. Если возможно, установить нарушителя, немедленно предпринять соответствующие действия, предусмотренные планом защиты для данной АСОИ.

2. Предупредить пользователей о необходимости адекватной защиты наборов данных; регулярно проверять защиту наиболее ценных из них.

3. Если сетевой НСД становится периодическим – резко ограничить возможный доступ из сети, возможно, вообще запретить его.

В случае установления факта попытки проникновения, не увенчавшегося успехом, никаких действий по ликвидации последствий предпринимать не требуется, за исключением блокировки повторных нарушений подобного рода.

Удачные попытки проникновения

Удачные попытки проникновения включают успешный захват пароля, ознакомление с информацией или ее искажение, истощение системных ресурсов, разрушение программного обеспечения. Они требуют большого количества времени для ликвидации последствий в зависимости от квалификации и возможностей нарушителя.

Определение личности нарушителя – наиболее трудный этап при ликвидации последствий проникновения. Прежде всего необходимо установить, является ли нарушитель зарегистрированным пользователем системы или нет. Это определяет порядок дальнейших действий.

Информация, полученная в результате контроля, зачастую бывает неполной. В таких ситуациях можно разрешить дальнейшее проникновение, если необходимо получить о нарушителе более полную информацию. При этом в каких-либо системных процедурах, находящихся под полным контролем администратора, организуются «люки» (traps) для получения дополнительной информации. Необходимо позаботиться о восстановлении наборов по резервным копиям в случае их уничтожения или модификации. Именно в этих редких, но чрезвычайно опасных ситуациях разрабатывается план организации непрерывной работы и восстановления системы.

Наиболее сложно определить нарушителя при проникновении через сеть, особенно при использовании коммутируемых (или выделенных) линий связи.

Меры, которые необходимо предпринять после установления факта проникновения, зависят от его сущности. Основные из них перечислены ниже в порядке возрастания предполагаемого ущерба:

1. Обезопасить базу данных защиты, хранящую информацию о пользователях и их полномочиях, а также о защите объектов системы.

2. Изменить пароли, если есть подозрения в их компрометации. Изменить хотя бы пароли привилегированных пользователей, строго следя за тем, чтобы они не повторялись.

3. Полностью или частично обновить системные модули из резервных копий.

4. Ужесточить защиту. Применить дополнительные меры по защите наборов данных; использовать системные пароли, генераторы паролей; усилить меры контроля.

В качестве первоочередной меры по ликвидации последствий проникновения в систему необходимо перезагрузить модифицированные или уничтоженные файлы. Также следует определить, обязательна ли полная перезагрузка данных; пересмотреть защиту файлов; выяснить, имелась ли возможность при данном нарушении внести в системные или прикладные модули «червей», «троянских коней» и т. д. В случае положительного решения вопроса произвести уничтожение и перезагрузку соответствующих компонентов системы.

3.4. Дополнительные меры контроля

В некоторых случаях обычных мер контроля, предлагаемых системой, может оказаться недостаточно. Тогда применяют специально разработанные дополнительные меры.

К ним можно отнести, во-первых, статистические меры контроля. Особые программы постоянно следят за состоянием некоторых параметров системы, постоянно отслеживая их изменение. Специальная экспертная система периодически (например, в определенные моменты времени или при изменении определенных параметров) анализирует состояние контролируемых параметров, при этом сравнивая их с предыдущими значениями (на основе методов многомерного статистического анализа). При появлении каких-либо отклонений сразу выдается тревожное сообщение. Это своего рода автоматизация мониторинга системы. Такие методы достаточно хорошо разработаны, некоторые из них уже реализованы.

Во-вторых, к дополнительным мерам можно отнести некоторые интеллектуальные средства. Если АБС имеет большие размеры, то следить за состоянием ее защиты трудно. Поэтому можно установить специальные программные

средства, которые будут настроены на анализ определенных состояний системы, например на опасные события или изменение конфигурации. Они могут вовремя сообщить о появлении возможности НСД или каналов утечки информации, которые обычным способом обнаружить непросто.

Примером средства контроля, совмещающего в себе некоторые черты как статистических, так и интеллектуальных средств, может быть контроль банковских операций. С помощью такого контроля можно автоматически следить за пересылаемыми суммами, номерами счетов, местом назначения, временем платежа. Если какой-то отдельный параметр или их комбинация перейдут в разряд запрещенных (например размер платежа превышает установленный), подается сигнал тревоги. Эта же система может накапливать и анализировать определенные сведения в течение длительного периода времени. Она может контролировать, например, все переводы на определенный счет, и если за определенный промежуток времени сумма превысит допустимую, также выдается сигнал тревоги.

3.5. Методы и механизмы защиты автоматизированных сетей

Решаемые протоколами задачи аналогичны задачам, решаемым при защите локальных систем: обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети. Реализация этих функций осуществляется с помощью специальных механизмов. К их числу следует отнести:

Механизмы шифрования. Обеспечивают конфиденциальность передаваемых данных и/или информации о потоках данных.

Используемый в данном механизме алгоритм шифрования может использовать секретный или открытый ключ. В первом случае предполагается наличие механизмов управления и распределения ключей. Различают два способа шифрования: канальное (link encryption), реализуемое с помощью протокола канального уровня, и оконечное (абонентское, end-to-end encryption), реализуемое с помощью протокола прикладного или в некоторых случаях представительного уровня.

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

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

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

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

– пользователь не принимает участия в выполняемых операциях;

– для каждой пары узлов требуется свой ключ;

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

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

Оконечное (абонентское) шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. Другими словами, отправитель зашифровывает данные, получатель – расшифровывает. Такой способ имеет следующие особенности (сравните с канальным шифрованием):

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

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

– маршрут передачи несущественен – в любом канале информация останется защищенной;

– для каждой пары пользователей требуется уникальный ключ;

– пользователь должен знать процедуры шифрования и распределения ключей.

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

Механизмы цифровой подписи. Включают процедуры закрытия блоков данных и проверки закрытого блока данных.

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

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

Механизмы обеспечения целостности передаваемых данных. Обеспечивают как целостность отдельного блока или поля данных, так и потока данных. Целостность блока данных обеспечивается передающим и принимающим объектами. Передающий объект добавляет к блоку данных признак, значение которого является функцией от самих данных. Принимающий объект также

вычисляет эту функцию и сравнивает ее с полученной. В случае несовпадения выносится решение о нарушении целостности. Обнаружение изменений может повлечь за собой действия по восстановлению данных.

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

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

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

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

Механизмы управления маршрутом. Маршруты могут выбираться динамически или быть заранее заданы с тем, чтобы использовать физически безопасные подсети, ретрансляторы, каналы. Оконечные системы при установлении

попыток навязывания могут в свою очередь потребовать установления соединения по другому маршруту. Кроме того, может использоваться выборочная маршрутизация (т. е. часть маршрута задается отправителем явно – в обход опасных участков).

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

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

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

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

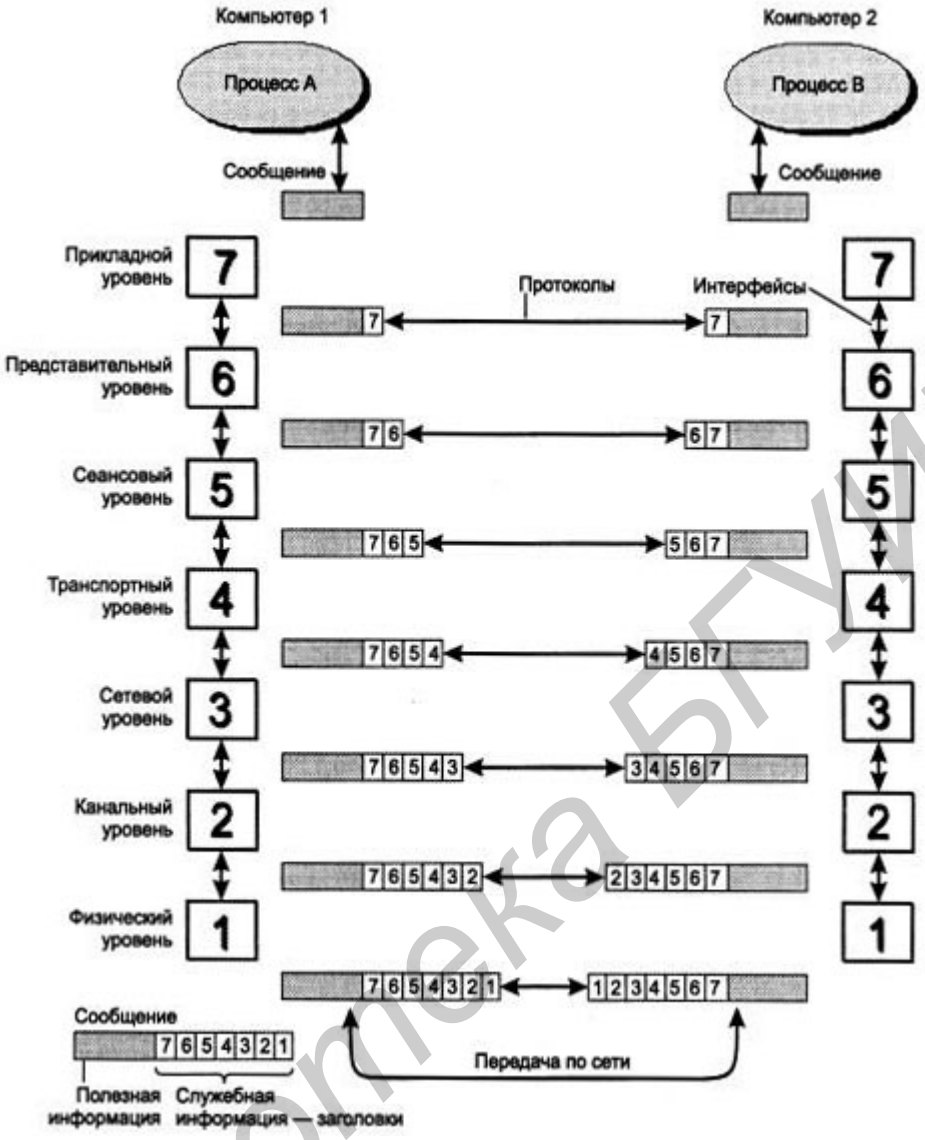


Рис. 3.2. Модель OSI (BOC)

Функции защиты протоколов каждого уровня модели OSI (Open System Interconnection) – Взаимодействия открытых систем (рис. 3.2) определяются их назначением:

1. Физический уровень – контроль электромагнитных излучений линий связи и устройств, поддержка коммуникационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень – увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информацию.

3. Сетевой уровень – наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизируемая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и других промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.).

Защита от всех подобных угроз осуществляется протоколами сетевого и транспортного уровней и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень – контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и другие функции. Все активные угрозы становятся видимыми на данном уровне.

Гарантом целостности передаваемых данных является криптозащита данных и служебной информации. Никто, кроме имеющих секретный ключ получателя и/или отправителя, не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Анализ трафика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как настоящие. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации, можно постоянно добиваться равномерного трафика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней – контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы сеансового и представительного уровня функций защиты не выполняют. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

Соответствие механизмов защиты уровням эталонной модели OSI, на которых они реализованы, представлено в табл. 3.1.

Таблица 3.1

Соответствие механизмов защиты уровням модели OSI

Механизм защиты	Уровень						
	1	2	3	4	5	6	7
Аутентификация одноуровневых объектов	–	–	+	+	–	–	+
Аутентификация источника данных	–	–	+	+	–	–	+
Цифровая подпись	–	–			–	–	+
Контроль доступа	–	–	+	+	–	–	+
Конфиденциальность сообщения	–	–	+	+	–	–	+
Конфиденциальность потока данных	+	+	+	–	–	–	–
Конфиденциальность отдельных полей	–	–	–	–	–	–	+
Целостность с восстановлением	–	–	–	+	–	–	+
Целостность без восстановления	–	–	+	+	–	–	+
Целостность отдельных полей	–	–	–	–	–	–	+
Защита от отказов	–	–	–	–	–	–	+

Примечание. «+» – означает, что данный механизм может быть реализован в протоколе данного уровня.

Вопросы для самоконтроля

1. Что входит в обязанности сотрудников административной группы управления защиты?

2. Какие группы сотрудников в составе административной группы управления защиты выделяют, и каковы их функции?

3. Какие угрозы информационной безопасности относят к опасным событиям?

4. От каких источников возможно получение информации об опасных событиях?

5. В чем заключается специфика получения информации об опасных событиях от пользователей?

6. В чем заключается специфика получения информации об опасных событиях от средств мониторинга функционирования системы?

7. В чем заключается специфика получения информации об опасных событиях из системного журнала?

8. Какие попытки проникновения в автоматизированную банковскую систему можно классифицировать как неудачные?

9. В чем заключается специфика реагирования на удачные попытки проникновения в автоматизированную банковскую систему?

10. Какие дополнительные меры контроля автоматизированных банковских систем используют на практике?

11. Какие механизмы защиты используют в автоматизированных банковских системах, в чем их особенности?

12. Какие механизмы защиты используются для обеспечения безопасности на каждом из уровней модели OSI?

4. АВТОМАТИЗАЦИЯ БАНКОВСКИХ ОПЕРАЦИЙ И ИХ ЗАЩИТА

4.1. Угрозы безопасности автоматизированных банковских систем

«Атака» на АБС – автоматизированную банковскую систему может осуществляться с двух уровней (возможна их комбинация) [3]:

1. Верхнего – злоумышленник использует свойства сети для проникновения на другой узел и выполнения определенных несанкционированных действий. Предпринимаемые меры защиты определяются потенциальными возможностями злоумышленника и надежностью средств защиты отдельных узлов.

2. Нижнего – злоумышленник использует свойства сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом. Нарушение потока сообщений может привести к утечке информации и даже потере контроля за сетью. Используемые протоколы должны обеспечивать защиту сообщений и их потока в целом.

Ниже приводится классификация угроз, специфических для сетей (угрозы нижнего уровня):

1. Пассивные угрозы (нарушение конфиденциальности данных, циркулирующих в сети) – просмотр и/или запись данных, передаваемых по линиям связи:

– просмотр сообщения – злоумышленник может просматривать содержание сообщения, передаваемого по сети;

– анализ трафика – злоумышленник может просматривать заголовки пакетов, циркулирующих в сети, и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности и т. д.); кроме того, он может выяснить длину сообщения и объем трафика.

2. Активные угрозы (нарушение целостности или доступности ресурсов (компонентов) сети) – несанкционированное использование устройств, имеющих доступ к сети, для изменения отдельных сообщений или потока сообщений:

– отказ служб передачи сообщений – злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;

– «маскарад» – злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;

– внедрение сетевых вирусов – передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;

– модификация потока сообщений – злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Совершенно очевидно, что любые описанные выше манипуляции с отдельными сообщениями и потоком в целом могут привести к нарушениям работы сети или утечке конфиденциальной информации. Особенно это касается служебных сообщений, несущих информацию о состоянии сети или отдельных узлов, о происходящих на отдельных узлах событиях (удаленном запуске программ, например). Активные «атаки» на такие сообщения могут привести к потере контроля за сетью. Поэтому протоколы, формирующие сообщения и ставящие их в поток, должны предпринимать меры для их защиты и неискаженной доставки получателю.

4.2. Особенности защиты информации в автоматизированных банковских системах

Специфика защиты автоматизированных банковских систем (АБС; Electronic banking system) обусловлена особенностями решаемых ими задач.

Как правило, АБС обрабатывают большой поток постоянно поступающих запросов в реальном масштабе времени, каждый из которых не требует для обработки многочисленных ресурсов, но все вместе они могут быть обработаны только высокопроизводительной системой.

В АБС хранится и обрабатывается конфиденциальная информация, не предназначенная для широкой публики. Подделка ее или даже утечка могут

привести к серьезным (для банка или его клиентов) последствиям. Поэтому АБС обречены оставаться относительно закрытыми, работать под управлением специфического программного обеспечения и уделять большое внимание обеспечению своей безопасности.

Другой особенностью АБС являются повышенные требования к надежности аппаратного и программного обеспечения. В силу этого многие современные АБС тяготеют к так называемой отказоустойчивой архитектуре («fault-tolerant») компьютеров, позволяющей осуществлять непрерывную обработку информации даже в условиях различных сбоев и отказов.

Можно выделить два типа задач, решаемых АБС:

1. Аналитические

К этому типу относятся задачи планирования, анализа счетов и т. д. Они не являются оперативными и могут требовать для решения длительного времени, а их результаты могут оказать влияние на политику банка в отношении конкретного клиента или проекта. Поэтому подсистема, с помощью которой решаются аналитические задачи, должна быть надежно изолирована от основной системы обработки информации.

Для решения такого рода задач обычно не требуется мощных вычислительных ресурсов; как правило, обычно достаточно 10 – 20 % мощности всей системы. Однако ввиду возможной ценности результатов их защита должна быть постоянной.

2. Повседневные

К этому типу относятся задачи, решаемые в повседневной деятельности, в первую очередь, выполнение платежей и корректировка счетов. Именно они и определяют размер и мощность основной системы банка; для их решения обычно требуется гораздо больше ресурсов, чем для аналитических задач.

В то же время ценность информации, обрабатываемой при решении таких задач, имеет временный характер. Постепенно ценность информации, например, о выполнении какого-либо платежа, становиться не актуальной. Естест-

венно, это зависит от многих факторов, как-то: суммы и времени платежа, номера счета, дополнительных характеристик и т. д. Поэтому обычно бывает достаточным обеспечить защиту платежа именно в момент его осуществления. При этом защита самого процесса обработки и конечных результатов должна быть постоянной.

Главное в защите коммерческих организаций – оперативное и по возможности полное восстановление информации после аварий и катастроф. В основном защита информации от разрушения достигается созданием резервных копий и их «внешним хранением», использованием средств бесперебойного электропитания и организацией горячего резерва аппаратных средств.

Следующая по важности для финансовых организаций проблема – это управление доступом пользователей к хранимой и обрабатываемой информации. Здесь широко используются различные программные системы управления доступом, которые иногда могут заменять и антивирусные программные средства. В основном используются приобретенные программные средства управления доступом. Причем в финансовых организациях особое внимание уделяют такому управлению пользователей именно в сети.

В государственных организациях гораздо шире применяются сертифицированные NCSC программные средства. Это объясняется существующими требованиями к обработке информации. Для защиты от компьютерных вирусов широко применяются специализированные антивирусные пакеты. Средства разграничения доступа используются намного реже.

К отличиям организации защиты сетей ПЭВМ в финансовых организациях можно отнести широкое использование коммерческого программного обеспечения для управления доступом к сети, защиты точек подключения к системе через коммутируемые линии связи. Другие способы защиты, такие, как применение антивирусных средств, оконечное и канальное шифрование передаваемых данных, аутентификация сообщений, в основном применяются примерно одинаково (за исключением антивирусных средств).

Большое внимание как в коммерческих, так и в государственных организациях уделяется физической защите помещений, в которых расположены компьютеры. Это означает, что защита ПК от доступа посторонних лиц решается не только с помощью программных средств, но и организационно-технических (охрана, кодовые замки и т. д.).

Шифрование локальной информации применяют чуть более 20 % коммерческих организаций. Причинами этого являются сложность распространения ключей, жесткие требования к быстродействию системы, а также необходимость оперативного восстановления информации при сбоях и отказах оборудования.

Значительно меньшее внимание в финансовых организациях уделяется защите телефонных линий связи (4 %) и использованию ПК, разработанных с учетом требования стандарта Tempest (защита от утечки информации по каналам электромагнитных излучений и наводок). В государственных организациях решению проблемы противодействия получению информации с использованием электромагнитных излучений и наводок уделяют гораздо большее внимание.

Защита финансовых организаций (в том числе и банков) строится несколько иначе, чем государственных (в том числе и военных). Следовательно, для защиты АБС нельзя применять те же самые технические и организационные решения, которые были разработаны для государственного сектора.

Защита АБС должна разрабатываться для каждой системы индивидуально в соответствии с общими правилами:

– анализ риска, заканчивающийся разработкой проекта системы и планов защиты, непрерывной работы и восстановления;

– реализация системы защиты на основе результатов анализа риска;

– постоянный контроль за работой системы защиты и АБС в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

Каждую систему защиты информации АБС следует разрабатывать индивидуально, учитывая следующие особенности:

– организационную структуру банка;

– объем и характер информационных потоков (внутри банка в целом, внутри отделов, между отделами, внешних);

– количество и характер выполняемых операций: аналитических и повседневных (один из ключевых показателей активности банка – число банковских операций в день – является основой для определения параметров системы);

– количество и функциональные обязанности персонала;

– количество и характер клиентов;

– график суточной нагрузки;

– другие.

Нельзя бездумно копировать чужие системы – они разрабатывались для иных условий. Одним из способов построения системы обработки информации является использование так называемого внешнего ресурса.

4.3. Внешний ресурс

Известно, что банковский бизнес относится к числу наиболее рискованных. Конкуренция между отдельными банками, риск при финансировании проектов, непредсказуемая политическая и экономическая ситуация заставляют многие банки прибегать к любым мерам, способствующим экономии средств. Одной из таких мер, относящихся к проектированию информационной системы, является использование внешнего ресурса.

Внешний ресурс (outsourcing) – использование банком для решения своих задач ресурсов другой организации (поставщика). Различают два вида внешнего ресурса:

1. Сервис-бюро (service bureau)

Банк заключает контракт с поставщиком (возможно, другим банком) на предоставление вычислительных ресурсов (машинного времени, магнитных накопителей) для обработки информации в центре поставщика. При этом используются техническое и программное обеспечение последнего.

2. Услуги по управлению (facilities management)

Поставщик управляет работой центра обработки информации банка, используя при этом оборудование самого банка. В этом случае служащие информационного отдела банка являются работниками поставщика ресурса.

Очень часто многие средние и крупные банки идут на использование внешнего ресурса, получая в результате существенную, но краткосрочную (на время контракта с поставщиком) экономию средств, которые могли бы быть затрачены на организацию собственной системы взамен частичной потери контроля за процессом обработки информации. Тем не менее в условиях непредсказуемого будущего такая мера часто оказывается оправданной по следующим соображениям.

С одной стороны, банки неохотно вкладывают деньги в новые информационные технологии, расширение или модернизацию существующих систем. С другой стороны, чтобы остаться конкурентоспособными, они должны предоставлять своим клиентам самый современный сервис со всеми возможными гарантиями надежности. Внешний ресурс является компромиссом в этой ситуации не потому, что банки не могут позволить себе выполнение определенных операций в собственных системах, – просто использование чужих систем может быть выгоднее.

Традиционно клиентами поставщика ресурса являлись мелкие предприятия, в том числе мелкие банки и их объединения. Они считали, что лучше платить за использование чужих систем, чем организовывать свои. Со средними и крупными предприятиями ситуация несколько иная. Поскольку они не желают терять контроль за выполнением операций, то многие поставщики предлагают

компромиссное решение. В этом случае банки выбирают набор прикладных задач, наименее сложных или второстепенных, которые и будут решаться поставщиком ресурса. К числу таких задач могут быть отнесены, например, обработка изображений и др.

В случае использования внешнего ресурса банки получают следующие преимущества:

– уменьшается нагрузка на АБС банка;

– уменьшается номенклатура задач, решаемых с помощью единого интегрированного программного обеспечения;

– обеспечивается доступ к новым технологиям и прикладным задачам;

– привлекается новый персонал с новыми знаниями и опытом.

Банк также получает новые продукты и услуги, повышающие его конкурентоспособность.

Правильно выбранная политика использования внешнего ресурса помогает сэкономить значительные суммы денег. При этом необходимо очень тщательно подходить к выбору поставщика ресурса с обязательным опытом соответствующей работы, прочной репутацией, гарантирующей конфиденциальность услуг, и использовать современную технологию.

По оценкам западных специалистов оптимальный срок контракта банка с поставщиком на предоставление внешнего ресурса находится в пределах 5 – 10 лет. Кроме того, поставщик ресурса может сыграть определенную положительную роль при взаимодействии банков, поскольку, как отмечают специалисты, банковское дело сегодня в гораздо большей степени зависит от партнерства, чем ранее.

Внешний ресурс может сэкономить банкам от 10 % до 50 % средств по сравнению с обработкой в собственной системе. Реальное значение экономии изменяется от случая к случаю.

Вопросы для самоконтроля

1. Какие из угроз информационной безопасности в автоматизированных банковских системах являются наиболее опасными?

2. Какие из угроз информационной безопасности в автоматизированных банковских системах сложнее всего обнаружить?

3. В чем заключается особенность реализации повседневных задач в автоматизированных банковских системах?

4. Какая из задач обеспечения безопасности является первоочередной при защите финансовых организаций?

5. Какие существуют общие правила защиты электронных банковских систем?

6. Какие особенности автоматизированных банковских систем необходимо учитывать при разработке мероприятий по защите информации?

7. В каких случаях задействуется внешний ресурс?

8. Какие виды внешнего ресурса широко используют на практике?

9. Какие преимущества получает банк при использовании внешнего ресурса?

5. ЭЛЕКТРОННЫЕ ПЛАТЕЖИ

5.1. Обмен электронными данными

Обмен электронными данными (ОЭД, Electronic Data Interchange; EDI) – это межкомпьютерный обмен деловыми, коммерческими, финансовыми электронными документами. Например, заказами, платежными инструкциями, контрактными предложениями, накладными, квитанциями и т. п.

Существует две ключевые стратегии развития ОЭД [3]:

1. ОЭД используется как преимущество в конкурентной борьбе, позволяющее осуществлять более тесное взаимодействие с партнерами. Такая стратегия принята в крупных организациях и получила название «Подхода Расширенного Предприятия» (Extended Enterprise).

2. ОЭД используется в некоторых специфических индустриальных проектах или в инициативах объединений коммерческих и других организаций для повышения эффективности их взаимодействия.

Основным препятствием широкому распространению ОЭД является многообразие представлений документов при обмене ими по каналам связи. Для преодоления этого препятствия различными организациями были разработаны стандарты представления документов в системах ОЭД для различных отраслей деятельности:

GDTI – General Trade Interchange (Европа, международная торговля);

NACHA – National Automated Clearing House Association (США, Национальная ассоциация автоматизированных расчетных палат);

TDCC – Transportation Data Coordinating Committee (Координационный комитет по данным перевозок);

VICS – Voluntary Interindustry Communication Standart (США, Добровольный межотраслевой коммуникационный стандарт);

WINS – Warehouse Information Netwoark Standarts (Стандарты информационной сети товарных складов).

В октябре 1988 г. международная группа UN/ECE опубликовала первую версию стандарта EDIFACT. Разработанный набор синтаксических правил и коммерческих элементов данных был оформлен в виде двух стандартов ISO:

ISO 7372 – Trade Data Element Directory (Справочник коммерческих элементов данных);

ISO 9735 – (EDIFACT) – Application Level Syntax Rules (Синтаксические правила прикладного уровня).

Частным случаем ОЭД являются электронные платежи (EFT – Electronic Funds Transfer) – обмен финансовыми документами между клиентами и банками, между банками и другими финансовыми и коммерческими организациями.

Суть концепции электронных платежей заключается в том, что пересылаемые по линиям связи сообщения, должным образом оформленные и переданные, являются основанием для выполнения одной или нескольких банковских операций. Никаких бумажных документов для их выполнения в принципе не требуется (хотя они могут быть выданы). Другими словами, пересылаемое по линиям связи сообщение представляет «живые деньги». На его основании можно переслать или получить деньги, открыть кредит, оплатить покупку или услугу и выполнить любую другую банковскую операцию. Такие сообщения называются электронными деньгами, а выполнение банковских операций на основании посылки или получения таких сообщений – электронными платежами. Естественно, весь процесс осуществления электронных платежей нуждается в надежной защите, иначе банк и его клиентов ожидают серьезные неприятности.

Электронные платежи применяются при межбанковских, торговых и наличных (персональных) расчетах (рис. 5.1).

Межбанковские и торговые расчеты производятся между организациями (юридическими лицами), поэтому их иногда называют корпоративными.

Наличные расчеты, как правило, производятся с участием физических лиц – клиентов. Поэтому они получили название ***персональных.***

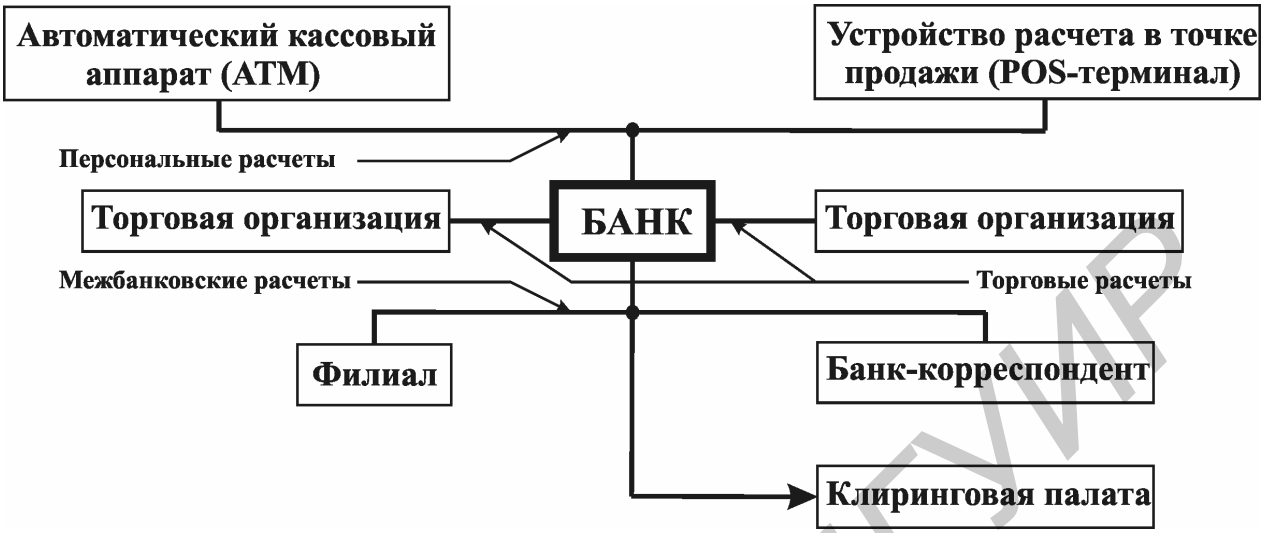


Рис. 5.1. Применение электронных платежей

Как только банк решает ввести систему электронных платежей, сложности его работы сразу возрастают на несколько порядков. Большинство крупных хищений в банковских системах прямо или косвенно связано именно с системами электронных платежей.

На пути создания систем электронных платежей, особенно глобальных, охватывающих большое число финансовых институтов и их клиентов в различных странах, встречается множество препятствий. Основными из них являются:

1. Отсутствие единых стандартов на операции и услуги, что существенно затрудняет создание объединенных банковских систем. Каждый крупный банк стремится создать свою сеть ОЭД, что увеличивает расходы на ее эксплуатацию и содержание. Дублирующие друг друга системы затрудняют пользование ими, создавая взаимные помехи и ограничивая возможности клиентов.

2. Возрастание мобильности денежных масс, что ведет к увеличению возможности финансовых спекуляций, расширяет потоки «блуждающих капиталов». Эти деньги способны за короткое время менять ситуацию на рынке, дестабилизировать ее.

3. Сбои и отказы технических и программных средств при осуществлении финансовых расчетов, что может привести к серьезным осложнениям для дальнейших расчетов и потере доверия к банку со стороны клиентов, особенно в силу тесного переплетения банковских связей (своего рода «размножение ошибки»). При этом существенно возрастает роль и ответственность операторов и администрации системы, которые непосредственно управляют обработкой информации.

Любая организация, которая хочет стать клиентом какой-либо системы электронных платежей либо организовать собственную систему, должна отдавать себе в этом отчет. Для надежной работы система электронных платежей должна быть надежно защищена.

5.2. Торговые расчеты

Торговые расчеты производятся между различными торговыми организациями. Банки в этих расчетах участвуют как посредники при перечислении денег со счета организации-плательщика на счет организации-получателя [3].

Торговые расчеты чрезвычайно важны для общего успеха программы электронных платежей. Объем финансовых операций различных компаний обычно составляет значительную часть общего объема операций банка.

Виды торговых расчетов сильно различаются для разных организаций, но всегда при их осуществлении обрабатывается два типа информации: платежных сообщений и вспомогательная (статистика, сводки, уведомления). Для финансовых организаций наибольший интерес представляет, конечно, информация платежных сообщений – номера счетов, суммы, баланс и т. д. Для торговых организаций оба вида сведений одинаково важны – первый дает ключ к финансовому состоянию, второй помогает при принятии решений и выработке политики.

Широко распространены торговые расчеты следующих двух видов:

Прямой депозит (direct deposit)

Смысл этого вида расчетов заключается в том, что организация поручает банку осуществлять некоторые виды платежей своих служащих или клиентов автоматически, с помощью заранее подготовленных магнитных носителей или специальных сообщений. Условия осуществления таких расчетов оговариваются заранее (источник финансирования, сумма и т. д.). Они используются в основном для регулярных платежей (выплаты различного рода страховок, погашение кредитов, зарплата и т. д.). В организационном плане прямой депозит более удобен, чем, например, платежи с помощью чеков.

Банкам прямой депозит сулит следующие выгоды:

– уменьшение объема задач, связанных с обработкой бумажных документов и, как следствие, экономия значительных сумм (до 1/3);

– увеличение числа депозитов, так как 100 % объема платежей должны быть внесены на депозит.

Кроме банков в выигрыше остаются и хозяева, и работники организации; повышаются удобства и уменьшаются затраты.

Расчеты при помощи ОЭД

В качестве данных здесь выступают накладные, фактуры, комплектующие ведомости и т. д.

Для осуществления ОЭД необходима реализация следующего набора основных услуг:

– электронная почта по протоколу X.400;

– передача файлов;

– связь «точка-точка»;

– доступ к базам данных в режиме on-line;

– почтовый ящик;

– преобразование стандартов представления информации.

Примерами систем торговых расчетов с использованием ОЭД являются:

– National Bank и Royal Bank (Канада) связаны со своими клиентами и партнерами с помощью IBM Information Network;

– Transcontinental Automated Payment Service (TAPS) – служба, основанная в 1986 г., связывает Bank of Scotland с клиентами и партнерами в 15 странах с помощью корреспондентских банков и автоматизированных клиринговых палат.

5.3. Межбанковские расчеты

Система электронных межбанковских (interbank) расчетов включает в себя:

– клиринговые расчеты с использованием мощной вычислительной системы банка-посредника (клирингового банка) и корреспондентских счетов банков-участников для расчетов в этом банке. Система основана на зачете взаимных денежных требований и обязательств юридических лиц с последующим переводом сальдо. Клиринг также широко используется на фондовых и товарных биржах, где зачет взаимных требований участников сделок проводится через клиринговую палату или особую электронную клиринговую систему.

Межбанковские клиринговые расчеты осуществляются через специальные клиринговые палаты, коммерческие банки, а между отделениями и филиалами одного банка – через головную контору. В ряде стран функции клиринговых палат выполняют центральные банки.

Автоматизированные клиринговые палаты (АКП; Automating Clearing House (ACH)) предоставляют услуги по обмену средствами между финансовыми учреждениями. Платежные операции в основном сводятся либо к дебетованию, либо к кредитованию. Членами системы АКП являются финансовые учреждения, которые состоят в ассоциации АКП. Ассоциация образуется для того, чтобы разрабатывать правила, процедуры и стандарты выполнения электронных платежей в пределах географического региона. Необходимо отметить, что АКП - не что иное, как механизм для перемещения денежных средств и сопроводительной информации. Сами по себе палаты не выполняют платежных услуг.

Объем и характер операций постоянно расширяются. АКП начинают выполнять деловые расчеты и операции обмена электронными данными. После трехлетних усилий различных банков и компаний была создана система CTP (Corporate Trade Payment), предназначенная для автоматизированной обработки кредитов и дебетов. По мнению специалистов, в ближайшее время тенденция расширения функций АКП будет сохраняться;

– ***прямые расчеты,*** при которых два банка осуществляют связь непосредственно между собой, возможно, при участии третьего лица, играющего организационную или вспомогательную роль. Естественно, объем взаимных операций должен быть достаточно велик для оправдания затрат на организацию такой системы расчетов. Обычно такая система объединяет несколько банков, при этом каждая пара может связываться непосредственно между собой, минуя посредников. Однако в этом случае возникает необходимость управляющего центра, занимающегося защитой взаимодействующих банков (рассылкой ключей, управлением, контролем функционирования и регистрацией событий).

В мире существует достаточно много таких систем – от небольших, связывающих несколько банков или филиалов, до гигантских международных, связывающих тысячи участников. Наиболее известной системой этого класса является SWIFT.

В последнее время появился третий вид электронных платежей – ***обработка электронных чеков*** (electronic check truncation), суть которого состоит в прекращении пути пересылки бумажного чека в финансовой организации, в которую он был предъявлен. В случае необходимости дальше «путешествует» его электронный аналог в виде специального сообщения. Пересылка и погашение электронного чека осуществляются с помощью АКП.

Функционирующие системы такого рода в настоящий момент широкого применения не нашли. В 1990 г. NACHA анонсировала первый этап тестирования национальной экспериментальной программы «Electronic Check

Truncation». Ее целью является сокращение расходов на обработку огромного количества бумажных чеков.

Пересылка денег с помощью системы электронных платежей включает следующие этапы (в зависимости от конкретных условий и самой системы порядок может меняться):

1. Определенный счет в системе первого банка уменьшается на требуемую сумму.

2. От первого банка второму посылается сообщение, содержащее информацию о выполняемых действиях (идентификаторы счетов, сумма, дата, условия и т. д.); при этом пересылаемое сообщение должно быть соответствующим образом защищено от подделки: зашифровано, снабжено цифровой подписью и контрольными полями и т. д.

3. Определенный счет во втором банке увеличивается на требуемую сумму.

4. Второй банк посылает первому уведомление о произведенных корректировках счета; это сообщение также должно быть защищено от подделки способом, аналогичным защите платежного сообщения.

5. Протокол обмена фиксируется у обоих абонентов и, возможно, у третьего лица (в центре управления сетью) для предотвращения конфликтов.

Это примерная схема действий. На пути передачи сообщений могут быть и посредники – клиринговые центры, банки-посредники в передаче информации и т. п. Основная сложность таких расчетов – уверенность в своем партнере, т. е. каждый из абонентов должен быть уверен, что его корреспондент выполнит все необходимые действия.

Для расширения применения электронных платежей проводится стандартизация электронного представления финансовых документов. Она была начата в 70-х гг. XX века в рамках двух организаций:

1) ANSI (American National Standart Institute) опубликовал документ ANSI X9.2–1980, Interchange Message Specification for Debit and Credit Card Message Exchange Among Financial Institute (Спецификация обменных сообще-

ний для дебетных и кредитных карточек обмена между финансовыми организациями). В 1988 г. аналогичный стандарт был принят ISO и получил название ISO 8583 (Bank Card Originated Messages Interchange Message Specifications – Content for Financial Transactions);

2) SWIFT (Society for Worldwide Interbank Financial Telecommunications) разработало серию стандартов межбанковских сообщений.

В соответствии со стандартом ISO 8583 финансовый документ содержит ряд элементов данных (реквизитов), расположенных в определенных полях сообщения или электронного документа (электронной кредитной карточки, сообщения в формате X.400 или документа в синтаксисе EDIFACT). Каждому элементу данных (ЭД) назначается свой уникальный номер. Элемент данных может быть как обязательным (т. е. входить в каждое сообщение данного вида), так и необязательным (в некоторых сообщениях может отсутствовать). Общая структура сообщения приведена на рис. 5.2.

Рис. 5.2. Общая структура сообщения

Битовая шкала определяет состав сообщения (ЭД, которые в нем присутствуют). Если некоторый разряд битовой шкалы принимает значение логической единицы, это означает, что соответствующий ЭД присутствует в сообщении. Благодаря такому методу кодирования сообщений уменьшается общая длина сообщения, достигается гибкость в представлении сообщений со многими ЭД, обеспечивается возможность включения новых ЭД и типов сообщений в электронный документ стандартной структуры.

Элементы данных, которые могут присутствовать в сообщении, определяются стандартом ISO 7982–1 1987 г.

5.4. Основные способы межбанковских платежей

Существует несколько способов электронных межбанковских платежей. Рассмотрим два из них: оплата чеком (оплата после услуги) и оплата аккредитивом (оплата ожидаемой услуги). Другие способы, как, например, оплата с помощью платежных требований или платежных поручений, имеют сходную организацию.

Оплата чеком основана на бумажном или другом документе, содержащем идентификацию предъявителя (подателя). Этот документ является основанием для перевода определенной в чеке суммы со счета владельца на счет предъявителя. Платеж чеком включают следующие этапы (рис. 5.3):

– получение чека;

– представление чека в банк;

– запрос о переводе со счета владельца чека на счет предъявителя;

– перевод денег;

– уведомление о платеже.

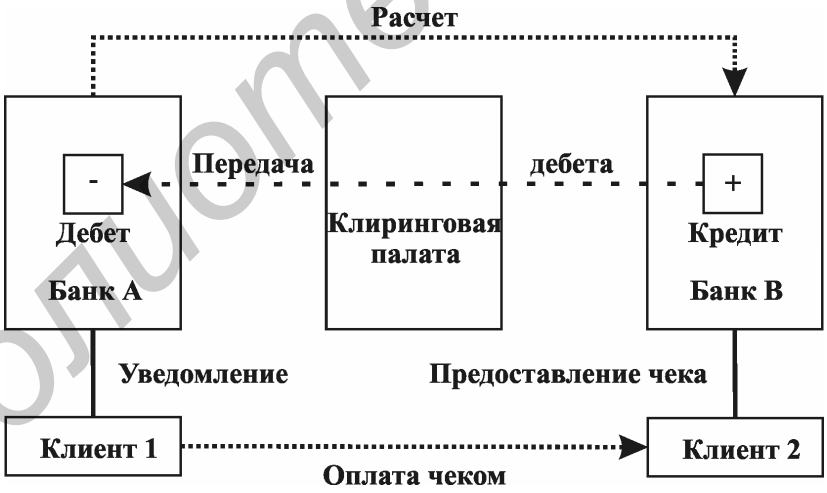


Рис. 5.3. Платеж чеком

Основными недостатками таких платежей являются необходимость существования вспомогательного документа (чека), который легко подделать, а также значительные затраты времени на выполнения платежа (до нескольких дней).

Поэтому в последнее время более распространен такой вид платежей, как оплата аккредитивом. Он включает следующие этапы (рис. 5.4):

– уведомление банка клиентом о предоставлении кредита;

– уведомление банка получателя о предоставлении кредита и перевод денег;

– уведомление получателя о получении кредита.

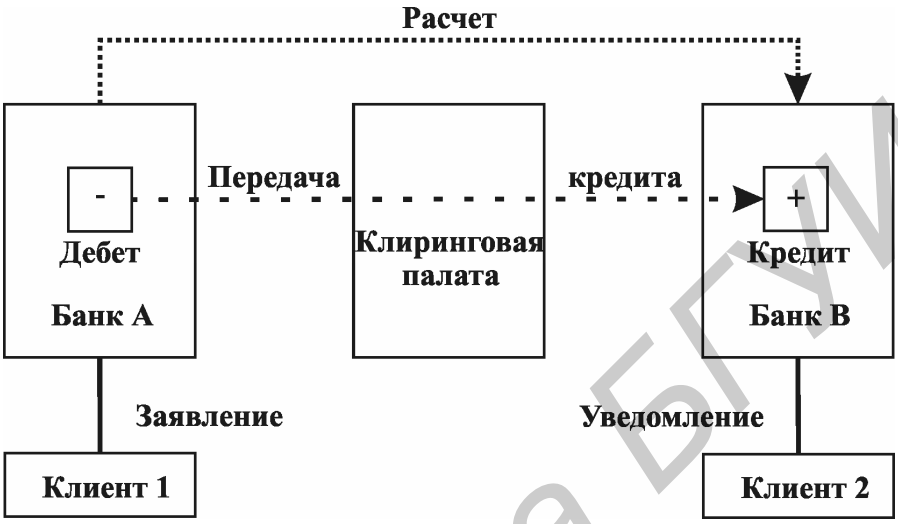


Рис. 5.4. Платеж аккредитивом

Такая система позволяет осуществлять платежи в очень короткие сроки. Уведомление о предоставлении кредита можно направлять по почте на дискетах, магнитных лентах или по электронной почте.

Каждый из рассмотренных выше видов платежей имеет свои преимущества и свои недостатки. Чеки наиболее удобны при оплате незначительных сумм, а также при нерегулярных платежах. В этих случаях задержка платежа не очень существенна, а использование кредита нецелесообразно. Расчеты с помощью аккредитива обычно используются при регулярной оплате и для значительных сумм. В этих случаях отсутствие клиринговой задержки позволяет сэкономить много времени и средств за счет уменьшения периода оборота денег. Общим недостатком этих двух способов является необходимость затрат на организацию надежной системы электронных платежей.

5.5. Проблемы безопасности электронного обмена данных

Для определения общих проблем защиты систем ОЭД рассмотрим прохождение документа при ОЭД. Можно выделить три основных этапа:

– подготовка документа к отправке;

– передача документа по каналу связи;

– прием документа и его обратное преобразование.

С точки зрения защиты в системах ОЭД существуют следующие уязвимые места:

1. Пересылка платежных и других сообщений между банками или между банком и клиентом.

2. Обработка информации внутри организаций отправителя и получателя.

3. Доступ клиента к средствам, аккумулированным на счете.

При пересылке платежных и других сообщений возникают следующие проблемы:

Внутренние системы организаций получателя и отправителя должны быть приспособлены к получению/отправке электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

Взаимодействие Получателя и Отправителя документа осуществляется опосредованно – через канал связи. Это порождает три типа проблем:

– взаимного опознавания абонентов (проблема установления аутентификации при установлении соединения);

– защиты документов, передаваемых по каналам связи (обеспечение целостности и конфиденциальности документов);

– защиты самого процесса обмена документами (проблема доказательства отправления/доставки документа).

В общем случае отправитель и получатель документа принадлежат к различным организациям и друг от друга независимы. Этот факт порождает

проблему недоверия – будут ли предприняты необходимые меры по данному документу (обеспечение исполнения документа).

С технической точки зрения эти проблемы решаются с помощью нескольких механизмов, отвечающих за обеспечение адекватной безопасности электронных банковских систем. Работа большинства этих механизмов обеспечивается службами сети с расширенным набором услуг (Value-Added Network, VAN). Службы, реализующие ОЭД, должны выполнять следующие функции:

– обеспечивать защиту от случайных и умышленных ошибок;

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

– поддерживать различные типы аппаратного и программного обеспечения, поставляемого различными производителями;

– осуществлять управление и поддержку сети для обеспечения непрерывности работы и быстрой диагностики нарушений;

– реализовывать полный спектр прикладных задач ОЭД, включая электронную почту;

– реализовывать максимально возможное число требований партнеров;

- включать службы резервного копирования и восстановления после аварий.

Тем не менее службы сети представляют собой только один элемент, обеспечивающий работу и безопасность ОЭД. Помимо перечисленных выше в системах ОЭД должны быть реализованы следующие механизмы, обеспечивающие реализацию функций защиты на отдельных узлах системы ОЭД и на уровне протоколов высокого уровня:

– равноправная аутентификаця абонентов;

– невозможность отказа от авторства сообщения/приема сообщения;

– контроль целостности сообщения;

– обеспечение конфиденциальности сообщения;

– управление доступом на оконечных системах;

– гарантии доставки сообщения;

– невозможность отказа от принятия мер по сообщению;

– регистрация последовательности сообщений;

– контроль целостности последовательности сообщений;

– обеспечение конфиденциальности потока сообщений.

Полнота решения рассмотренных выше проблем напрямую зависит от правильного выбора системы шифрования. Система шифрования (или криптосистема) представляет собой совокупность алгоритмов шифрования и методов распространения ключей. Правильный выбор системы шифрования помогает:

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

– обеспечить совместное использование документа группой пользователей системы ОЭД путем криптографического разделения информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, документ недоступен;

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

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

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

Надежность всей криптосистемы в целом во многом зависит от механизмов рассылки (распределения) ключей между участниками взаимодействия. Проблема рассылки ключей в настоящее время не имеет общих решений. В ка-

ждом конкретном случае она должна решаться с учетом особенностей функционирования всей защищаемой АСОИ. Существует много различных подходов к решению этой проблемы. Кратко опишем основные из них.

Метод базовых/сеансовых ключей (master/session keys)

Подробно изложен в стандарте ISO 8532 (Banking-Key Management). Суть метода состоит в том, что вводится иерархия ключей (главный ключ (ГК)/ключ шифрования ключей (КК)/ключ шифрования данных (КД)).

Иерархия может быть двухуровневой (КК/КД) или трехуровневой (ГК/КК/КД). При этом старший ключ в иерархии распространяется между участниками взаимодействия неэлектронным образом, исключающем его перехват и/или компрометацию. Стандарт определяет три способа распространения ключей: непосредственная передача (peer-to-peer), передача с использованием центра распространения (key distribution center) и передача с использованием центра трансляции ключей (key translation center). Стандарт не применяется для распространения ключей между специализированными банковскими устройствами, такими как банкоматы и устройства расчета в точке продажи.

Метод открытых ключей (public keys)

Основан на односторонних преобразованиях, при которых часть ключа остается открытой и может быть передана по линиям связи в открытом виде. Это избавляет от дорогостоящей процедуры распространения ключей шифрования неэлектронным способом.

Метод выведенного ключа (derived key)

Применяется для защиты информации, передаваемой между терминалом системы расчета в точке продажи и компьютером банка.

При этом методе ключ для шифрования каждой следующей транзакции вычисляется путем одностороннего преобразования предыдущего ключа и параметров транзакции.

Метод ключа транзакции (transaction key)

Также применяется для защиты информации, передаваемой между терминалом системы расчета в точке продажи и компьютером банка. Он отличается от метода выведенного ключа тем, что при вычислении ключа для следующей транзакции не используются ее параметры.

Уже существующие стандарты ОЭД жестко ограничивают реализацию мер по защите информации. Поскольку абсолютно неуязвимых систем не бывает, каждая организация должна самостоятельно решать вопрос об уровне защищенности собственной системы ОЭД: что лучше – затратить дополнительные средства на организацию и поддержание защиты или сэкономить и работать в условиях постоянного риска.

Вопросы для самоконтроля

1. Для чего используют обмен электронными данными?
2. Какое назначение имеет технология EFT?
3. Какая особенность торговых расчетов с использованием технологии электронного обмена данными?
4. Какие цели преследуются при выполнении межбанковских расчетов?
5. Какая роль в банковской сфере отводится автоматизированным клиринговым палатам?
6. Способы межбанковских платежей.
7. Какие угрозы электронного обмена данными существуют на современном этапе, и в чем их сущность?

6. ПЕРСОНАЛЬНЫЕ ПЛАТЕЖИ

6.1. Формы организации персональных платежей

Домашнее (телефонное) обслуживание

Домашнее банковское обслуживание позволяет клиентам получить доступ к банковским и информационным услугам не выходя из дома.

Достоинства этого вида обслуживания [3]:

– для клиента – большая доступность данных и управление своими финансовыми делами;

– для банка – уменьшение стоимости обслуживания (operational costs). При этом виде обслуживания клиент связывается с банком по телефону и дает непосредственные распоряжения по своему счету. Распоряжения могут быть отданы как голосом специальному служащему банка или электронной системе, так и в электронной форме непосредственно банковскому компьютеру.

Ввод данных для платежа при голосовой связи (идентификатор, номер счета, размер платежа) производится клиентом с клавиатуры телефона.

Системы домашнего (телефонного) обслуживания начали внедряться банками в начале 80-гг. XX века, однако до настоящего времени широкого распространения не получили. Основными причинами, по мнению специалистов, являются необходимость дополнительных устройств при электронной связи (компьютера и модема) и неуверенность в безопасности системы голосовой связи. Этот вид обслуживания пользуется популярностью среди мелких предпринимателей и частных клиентов. Многие банки настойчиво предлагают ее внедрить путем установки специальных терминалов.

Этот вид обслуживания в разных странах находится на различном уровне развития. Например, в США домашнее обслуживание не распространилось в

больших масштабах, в то время как во Франции около 3,5 млн терминалов подключено к сети MiniTel.

Некоторое распространение получило телефонное обслуживание и в Великобритании. Основным банком страны, обеспечивающим эти услуги, является Trustee Savings Banks. Его система SpeedLink в настоящее время обслуживает более 250 000 клиентов, не имеющих специального оборудования, за исключением современного телефона.

Для получения доступа к услугам SpeedLink клиенту необходимо соединиться с ним и назвать свой номер счета и личный идентификатор (PIN SpeedLine) для подтверждения личности. После установления связи клиенты SpeedLink могут получить уведомление на факс-аппарат или по почте (если факс отсутствует). Система предоставляет также такие услуги, как оплата счетов, передача денег, ознакомление с последними шестью транзакциями, перевод денег. Соотношение персональных и корпоративных клиентов этой системы 2:1.

First Direct – полная система телефонного обслуживания клиентов на дому. Она введена в действие Midland Bank Group в 1989 г. Основное ее отличие: система не использует синтезируемый голос или персональный компьютер для проведения расчетов. Клиент по телефону взаимодействует с человеком, который может быть (по необходимости) квалифицированным банковским работником.

Проведенные после установки First Direct исследования показали, что 30 % населения посещают банки для того, чтобы использовать банкоматы, а 30 % – пользуются телефоном.

В системе First Direct особое внимание уделяется начальной идентификации и проверке абонента. Для идентификации используется десятисимвольный пароль, устанавливаемый клиентом и известный только ему. Проверка абонента осуществляется при взаимодействии с оператором. В начале работы оператор запрашивает наугад одну или несколько букв из пароля пользователя. Дополни-

тельно клиенту присваивают кодовое слово, которое используется при идентификации. Детали процедуры идентификации и аутентификации системы First Direct держатся в секрете.

Будущее этого вида услуг сильно зависит от прогресса в области распознавания речи и создания надежных и сравнительно недорогих устройств с приемлемыми характеристиками такого распознавания.

Автоматические кассовые аппараты

Банковский автомат-кассир (Automatic Teller Machine, ATM; или же Автоматический кассовый аппарат, АКА, банкомат) – специализированное устройство, предназначенное для обслуживания клиента в отсутствие банковского персонала (рис. 6.1). Это наиболее существенная часть банковской системы, предназначенная в основном для выдачи наличных денег. Помимо этой функции АКА может выполнять ряд дополнительных, в числе которых:

– проверка состояния счета клиента;

– изменение параметров счета клиента;

– осуществление различных платежей;

– предоставление информации о:

1) страховом полисе клиента;

2) котировках ценных бумаг на фондовом рынке;

3) покупке и продаже акций;

4) обменных курсах валют и т. д.

Автоматический кассовый аппарат состоит из трех устройств ввода (считыватель с пластиковых карточек, цифровая и функциональная клавиатуры), двух выходных устройств (микродисплей и принтер) и устройства обработки информации. Взаимодействие клиента с АКА осуществляется при помощи пластиковой карточки, на которой записана необходимая информация, выносной клавиатуры и дисплея.

Рис. 6.1. Внешний вид автоматического кассового аппарата Opteva 720-3 Diebold

В настоящее время устройства обработки информации АКА разрабатываются на основе микропроцессоров. Выполнение операций осуществляется с помощью прикладного программного обеспечения. Шифрование конфиденциальной информации при передаче по каналам связи или при записи на диск осуществляется на основе стандарта DES. Кроме криптозащиты предусмотрены и другие меры безопасности.

Расчет в точке продажи

Системы, обеспечивающие расчеты продавца и покупателя в точке продажи (point-of-sale, POS), получили распространение в США более 20 лет назад (рис. 6.2). В основном все терминалы, подключенные к этим системам, размещены на предприятиях торговли. Большинство таких терминалов установлены в супермаркетах, так как там совершается большое количество покупок в течение дня, а также в других магазинах и на автозаправочных станциях.

Системы POS обеспечивают выполнение следующих услуг:

– проверку и подтверждение чеков;

– проверку и обслуживание дебетовых и кредитных карточек;

– использование системы электронных расчетов.

Банки, финансирующие систему расчетов в точке продажи, таким образом, расширяют список своих клиентов путем предоставления им больших удобств для покупок в магазинах с использованием удаленных устройств. Торговля в свою очередь увеличивает количество клиентов, расширяет управление имуществом (inventory control), сохраняет время клиентов и уменьшает риск потери наличных денег.

Рис. 6.2. Внешний вид POS терминала Beetle-20 Wincor Nixdorf

Существует два типа систем POS. Основной из них предполагает, что продавец и покупатель имеют счета в одном и том же банке. Данные, необходимые для платежа, передаются через терминалы системы POS банковскому компьютеру, производится платеж, и деньги переводятся со счета покупателя на счет продавца. В более сложной системе участвуют два или более банков. При платеже сначала вызывается банк покупателя, производится платеж и записывается на магнитную ленту для передачи в расчетную палату. Расчетная палата в свою очередь пересылает данные о платеже в банк продавца, который кредитует платеж.

6.2. Персональный идентификатор

Персональный номер (идентификатор) (Personal Identification Number, PIN) – это последовательность цифр (обычно 4 – 6, но может быть до 12), используемая для идентификации клиента. Для ввода PIN как в АКА, так и в тер-

миналах систем POS предусмотрена цифровая клавиатура, аналогичная телефонной. По способу назначения можно выделить следующие типы PIN [3]:

– назначаемые выведенные (derived) PIN;

– назначаемые случайные (random) PIN;

– PIN, выбираемые пользователем.

Клиент различает только два типа PIN: PIN, который назначен ему банком, выдавшим карту, и PIN, который пользователь может выбирать себе самостоятельно.

В связи с тем что PIN предназначен для идентификации и аутентификации клиента, его значение должно быть известно только клиенту. Однако на практике многоцифровой PIN трудно удержать в памяти и поэтому клиент банка куда-нибудь его записывает. Главное – это не записать PIN непосредственно на карту или в ежедневник на первой странице. Иначе задача злоумышленника будет сильно облегчена.

Использование PIN, назначенных банком, неудобно даже при небольшом количестве цифр. Для большего удобства клиента используются PIN, выбираемые им самим. Такой способ определения PIN, во-первых, позволяет клиенту использовать один и тот же PIN для различных целей, и, во-вторых, позволяет задавать PIN как совокупность цифр.

Как уже отмечалось выше, PIN обычно состоит из 4 – 6 цифр. Следовательно, для его перебора в наихудшем (для защиты, естественно) случае необходимо осуществить 10 000 комбинаций (четырехсимвольный PIN). Такой перебор возможен за короткое время. Поэтому в системах, использующих такой PIN, должны быть предусмотрены меры защиты от подбора.

Алгоритм идентификации клиента

Существуют два основных способа проверки PIN: алгоритмический и неалгоритмический.

Алгоритмический способ проверки заключается в том, что у пользователя запрашивается PIN, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением PIN, хранившемся на карте. Достоинством этого метода проверки является:

– отсутствие копии PIN на главном компьютере, что исключает его раскрытие персоналом банка;

– отсутствие передачи PIN между АКА и главным компьютером банка, что исключает перехват его злоумышленником или навязывание результатов сравнения;

– облегчение работы по созданию программного обеспечения системы, так как необходимость действий в реальном масштабе времени отсутствует.

Неалгоритмический способ проверки PIN, как это следует из его названия, не требует применения специальных алгоритмов. Проверка PIN осуществляется путем прямого сравнения полученного PIN со значениями, хранимыми в базе данных. Часто сама база данных со значениями PIN шифруется прозрачным образом, чтобы не затруднять процесс сравнения, но повысить ее защищенность.

Генерация PIN

Процесс получения (выведения) назначаемого PIN из номера счета показан на рис. 6.3.

Рис. 6.3. Процесс получения PIN

Вначале номер счета клиента дополняется нулями или другой константой до 8 байт. Затем получившиеся 8 байт шифруются с использованием секретного

ключа по алгоритму DES. Из получившегося шифротекста, начиная с «младших» байт, выделяются по 4 бита. Если значение числа, образуемого этими битами, менее 10, то полученная цифра включается в PIN; иначе значение отбрасывается. Таким образом обрабатываются все 8 байт (64 бита). Если в результате обработки не удалось получить требуемое количество десятичных цифр, то из неиспользуемых комбинаций вычитается 10.

В том случае, когда необходимо получить выбираемый пользователем PIN, каждая его цифра складывается по модулю 10 с соответствующей цифрой выведенного PIN (без учета переноса). Получаемое десятичное число называется «смещением» и запоминается на карте. Так как выводимый PIN имеет случайное значение, то невозможно получить выбранный пользователем PIN по его «смещению».

Альтернативы PIN

В настоящее время ведется широкая дискуссия по поводу применения PIN для идентификации клиентов. Сторонники применения утверждают, что вскрытие PIN в Великобритании, например, составило несколько случаев в месяц против несколько сотен миллионов проведенных транзакций в год. Противники же доказывают, что идентификация клиента с использованием PIN работает только в следующих случаях:

– отсутствует перехват карты и/или PIN при передаче от банка клиенту;

– банковские карты не воруют, не теряют и их невозможно подделать;

– PIN невозможно узнать при доступе к системе другого пользователя;

– PIN иным образом не может быть скомпрометирован;

– в электронной системе банка отсутствуют сбои и ошибки;

– в самом банке нет мошенников.

В качестве альтернативы PIN предлагается применять устройства идентификации, основанные на биометрическом принципе, однако их широкое применение сдерживается высокой стоимостью.

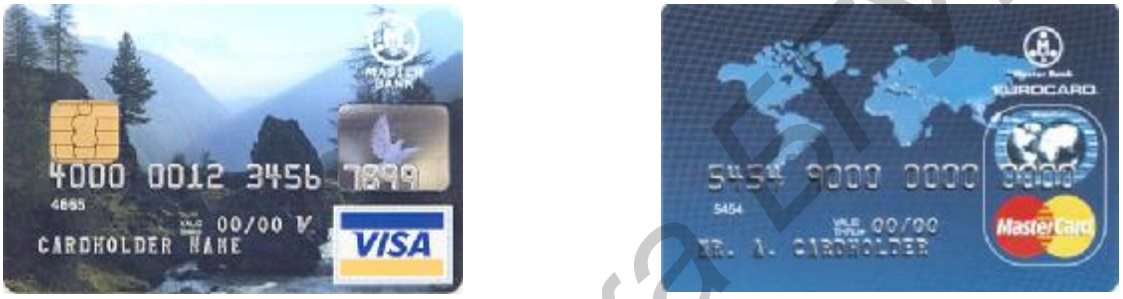
6.3. Обзор технологий электронных пластиковых карт

Использование систем POS и АКА потребовало появления некоторого носителя информации, который мог бы идентифицировать пользователя и хранить некоторые учетные данные. В качестве такого носителя стали выступать различные виды пластиковых карт [4]. Наиболее известные из них:

– кредитные карты Visa и MasterCard (рис. 6.4);

– международные чековые гарантии Eurocheque и Postcheque;

– карты для оплаты путешествий и развлечений American Express и Diners Club.



а б

Рис. 6.4. Электронные пластиковые карты международных платежных систем Visa (а) и MasterCard (б)

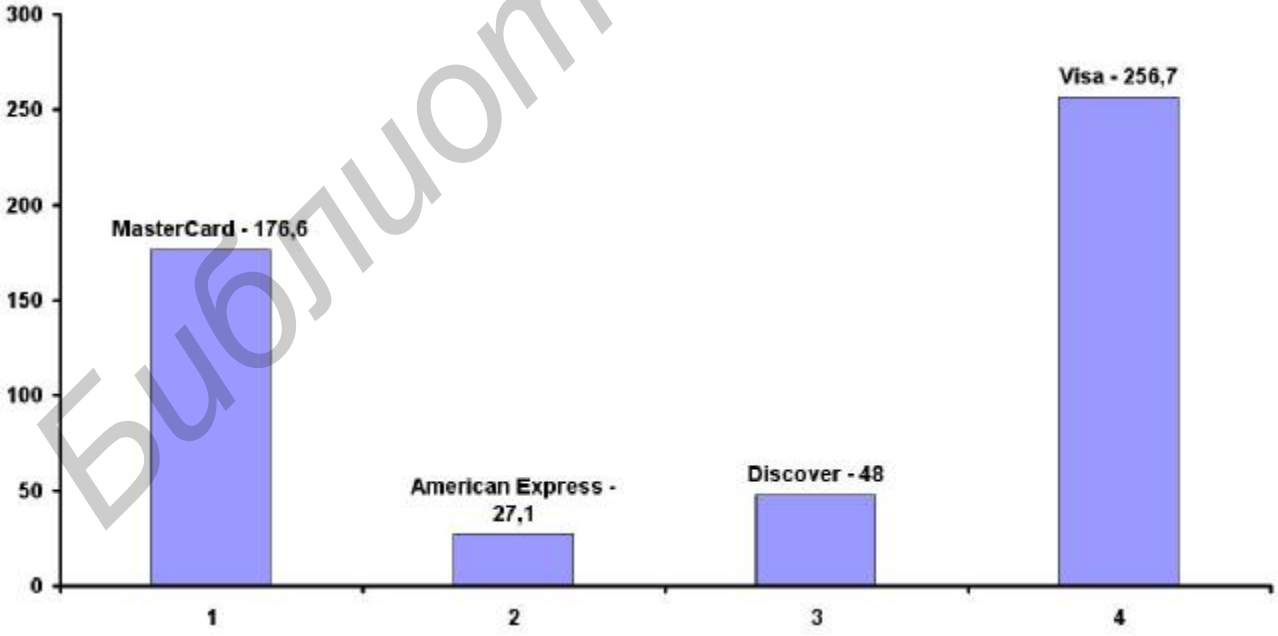


Рис. 6.5. Число карт в обращении (млн шт.)

В настоящее время выпущено большое количество карт (рис. 6.5) в различных странах мира.

Существует много признаков, по которым можно классифицировать карты (рис. 6.6):

1. По материалу, из которого карты изготовлены:

– *бумажные (картонные);*

– *пластиковые;*

– *металлические.*

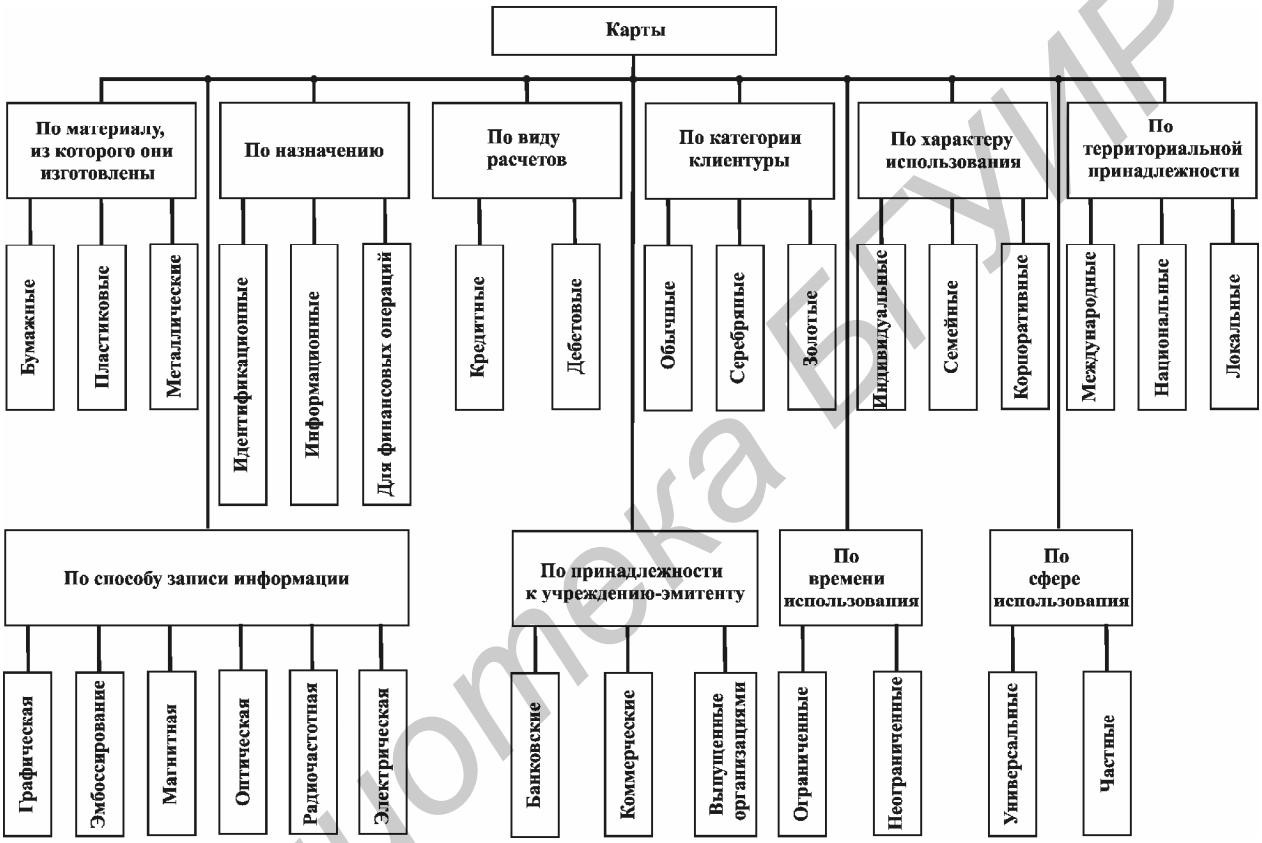


Рис. 6.6. Классификация карт

В настоящее время повсеместное распространение получили пластиковые карты. Однако для идентификации держателя карты часто используются бумажные (картонные) карты, запаянные в прозрачную пленку. Это ламинированные карты. Ламинирование является довольно дешевой и легкодоступной процедурой, и поэтому, если карта используется для расчетов, с целью повышения защищенности от подделок применяют более совершенную и сложную технологию изготовления карт из пластика. В то же время в отличие от металла

пластик легко поддается термической обработке и давлению (эмбоссированию), что весьма важно для персонализации карты перед выдачей ее клиенту.

2. По общему назначению:

– *идентификационные;*

– *информационные;*

– *для финансовых операций.*

Это разделение не является взаимоисключающим. Например, крупная компания может выдать каждому своему сотруднику карту, которая:

– является пропуском, разрешающим проход в определенные зоны предприятия (идентификационная функция);

– содержит в кодированном виде какую-либо важную информацию о держателе карты (информационная функция);

– используется также для расчетов в столовых и магазинах данной компании (расчетная функция).

Система с использованием многофункциональных карт существует за рубежом, и очевидно, что объединение многих функций в одной пластиковой карточке является перспективным, поскольку такая многофункциональная карта удобна и для эмитента, и держателя.

3. По виду проводимых расчетов (рис. 6.7):

– *кредитные;*

– *дебетные.*

Иногда выделяют в особую категорию *платежные карты* как разновидность кредитных карт. Отличие состоит в том, что общая сумма долга при использовании платежной карты должна погашаться полностью в течение определенного времени после получения выписки без права продления кредита.

Кредитная карта представляет собой такое средство расчетов, при котором эмитент берет на себя не только обязанность перечисления средств клиента на счета его контрагентов, но и риск немедленной оплаты товаров, работ и услуг ее владельца в пределах установленного им лимита кредитования. Таким

образом, кредитная карта позволяет ее владельцу при совершении любой покупки отсрочить ее оплату путем получения у банка кредита.

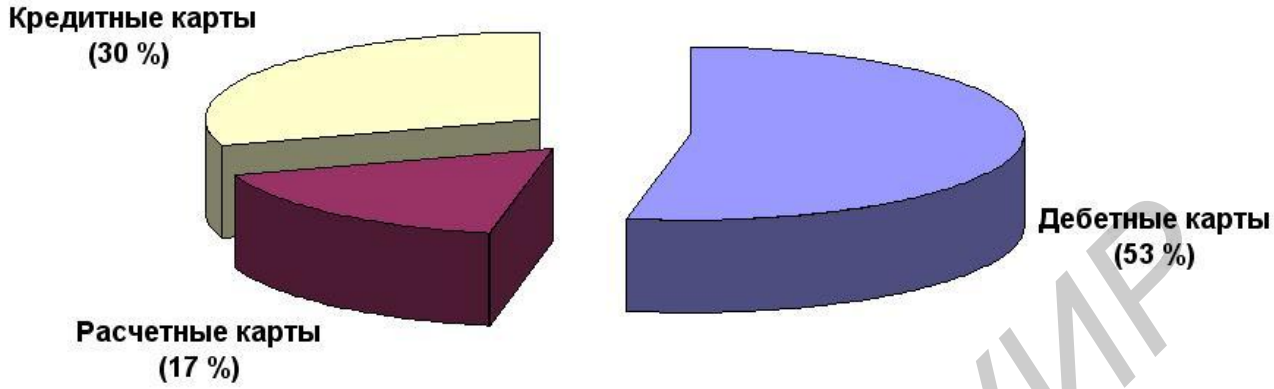


Рис. 6.7. Европейский рынок пластиковых карт

Лимит кредитования определяется банком-эмитентом каждому владельцу карты на его ссудном счете. Этот счет абсолютно независим от обычного (текущего, расчетного и пр.) счета клиента в банке.

Как правило, перед открытием ссудного счета банк или соответствующая компания по выпуску карт проверяют финансовое положение будущего владельца кредитной карты, а также детали предыдущих кредитных операций клиента – его «кредитную историю». На основании этих данных эмитент определяет сальдо денежных средств клиента на ссудном счете, а также суммы возможных поступлений и списаний.

Следует заметить, что эмитентами, как правило, устанавливаются конкретные сроки, в пределах которых клиент обязан вернуть банковский кредит. В случае задержки возврата денежных средств банк вправе взимать заранее оговоренные с клиентом проценты за каждый день просрочки. Для этой цели банками довольно часто устанавливается специальный страховой депозит, средства которого могут использоваться как для списания задолженности банку, так и для обращения взыскания в пользу возможных кредиторов клиента. Только некоторые банки работают без страховых депозитов.

Многими банками допускается ***овердрафт*** – перерасход кредитуемых средств. Пользование кредитными ресурсами осуществляется также под про-

центы, причем в данном случае повышенные. С точки зрения западных экономистов, кредитные карты имеют определенные недостатки, к числу которых относятся: ежемесячные платежи банку в размере 2,5 – 3 % общего товарооборота, уплата вступительного взноса для пользования компьютерной системой банка, дополнительное время для проверки платежеспособности карты и наличия лимита кредитования по ней, заинтересованность продавца в наличном расчете с покупателем.

Дебетные карты предназначены для немедленной оплаты товаров, работ и услуг путем прямого списания средств с текущего счета владельца карточки на счет его кредитора в пределах имеющейся там суммы. В этом случае при недостаточности средств расчеты банком производиться не будут, так как лимит, вносимый при открытии счета, снижаться не может, а обязательств по кредитованию клиента банк на себя не принимал.

Таким образом, расчеты по дебетной карте производятся путем прямого перечисления списанных со счета ее владельца денежных средств, а не за счет получения у банка кредита.

В отдельных банках при наступлении определенных условий дебетная карта может превратиться в кредитную (такие случаи банк определяет для каждого клиента индивидуально). Это значит, что банком при расчетах с использованием карты может быть предоставлен кредит, размер которого банк также определяет индивидуально. Величина кредита, к примеру, может зависеть от сумм постоянных остатков на карточном счете и регулярности пополняемости лимита.

Все очевидные преимущества кредитных и дебетовых карт проявились в так называемых исполнительных, или ***экзекьютивных***, картах, выдаваемых, как правило, высокооплачиваемым клиентам, крупным бизнесменам и т. п. Такой тип платежных карт считается наиболее престижным и отличается более крупным размером минимального депозита, дороговизной их открытия и обслуживания, а также более высоким лимитом кредитования в сочетании с про-

стотой получения наличных денег. Представителями исполнительных карт сегодня являются «золотые», «платиновые», «премиальные» и др.

В качестве гарантии чека была выпущена специальная **чековая гарантийная карточка** (Check Guarantee Card). Она выдается банком, где открыт счет клиента, и применяется для того, чтобы избежать получения от недобросовестного клиента необеспеченного чека или чека с поддельной подписью.

Появление таких карт связано с широким распространением одной из форм чекового кредита, которая основана на наличии у того или иного лица обычного текущего счета. Чековая гарантийная карта предусматривает автоматическое предоставление кредита в момент исчерпания остатка на чековом счете. При такой системе чеки принимаются к оплате до определенного оговоренного лимита, который может составлять от 100 до 500 у.е. или долл., а иногда и больше. Подобная система иногда называется ***овердрафтными счетами***. В большинстве случаев кредит выдается автоматически, как только сумма чека превысила остаток на счете. Такие ссуды могут погашаться либо в процессе поступления на счет обычных вкладов, либо чаще всего специальными взносами.

Карточки гарантии чеков используются для идентификации клиента. Указанная система весьма привлекательна своими возможностями расширения сферы применения чековых платежей. На гарантийных картах обычно имеется идентификационый номер, срок их действия и подпись клиента. Для идентификации привилегированных клиентов некоторые банки выпускают гарантийные карты без условий овердрафта. Такие карты используются владельцами евро- и других чеков, имеющих хождение в нескольких странах. В то же время в системе расчетов такими распространенными чеками, как American Express Travel Checks, никакие дополнительные банковские карты не применяются. Использование чековой гарантийной карты имеет свои недостатки, к числу которых относится наличие ежедневного лимита – предельной суммы платежа, гарантированной картой.

4. По категории клиентуры, на которую ориентируется эмитент:

– обычные;

– серебряные;

– золотые.

Обычные карты предназначены для рядового клиента. Это Visa Classic, EuroCard/MasterCard Mass (Standard).

Серебряная карта (Silver, Business) называется бизнес-картой и предназначена для частных лиц, для сотрудников компаний, уполномоченных расходовать в тех или иных пределах средства своей компании.

Золотая карта (Gold) предназначена для наиболее состоятельных клиентов.

В системах Visa и MasterCard есть карты, которые могут быть использованы только в АТМ-терминалах и в POS-терминалах для получения наличных денег: Visa Electron, Cirrus/Maestro. Они действуют в пределах остатка на счете, по ним, как правило, держателю карточки кредит не предоставляется, и поэтому они могут быть выданы любому клиенту независимо от уровня его обеспеченности или «кредитной истории».

5. По характеру использования:

– **индивидуальные карты**, выдаваемые отдельным клиентам банка, могут быть «стандартными» или «золотыми»;

– **семейные карты**, выдаваемые членам семьи лица, заключившего контракт и несущего ответственность по счету;

– **корпоративные карты** – выдаются юридическому лицу.

На основе корпоративной карты могут выдаваться индивидуальные карты избранным лицам (руководителям, главному бухгалтеру или ценным сотрудникам). Для них открываются персональные счета, привязанные к корпоративному карточному счету. Ответственность перед банком по корпоративному счету имеет организация, а не индивидуальные владельцы корпоративных карт.

6. По принадлежности к учреждению-эмитенту:

– **банковские**, эмитент которых – банк или консорциум банков;

– **коммерческие**, выпускаемые нефинансовыми учреждениями: коммерческими фирмами или группой коммерческих фирм;

– **карты, выпущенные организациями**, чьей деятельностью непосредственно является эмиссия пластиковых карт и создание инфраструктуры по их обслуживанию.

7. По сфере использования:

– **универсальные**. Служат для оплаты любых товаров и услуг;

– **частные коммерческие**. Служат для оплаты какой-либо определенной услуги (например карты гостиничных сетей, автозаправочных станций, супермаркетов).

8. По территориальной принадлежности:

– **международные**, действующие в большинстве стран;

– **национальные**, действующие в пределах какого-либо государства;

– **локальные**, используемые на части территории государства или действующие в одном конкретном учреждении.

9. По времени использования:

– **ограниченные** каким-либо временным промежутком (иногда с правом пролонгации);

– **неограниченные** (бессрочные).

10. По способу записи информации на карту:

– графическая;

– эмбоссирование;

– штрих-кодирование;

– магнитная;

– электрическая;

– лазерная;

– радиочастотная.

Самой ранней и простой формой записи информации на карту была и остается ***графическая***. Она до сих пор используется во всех картах, включая самые технологически сложные. Вначале на карту наносились только фамилия, имя держателя карты и информация об ее эмитенте. Позднее на универсальных банковских картах был предусмотрен образец подписи, а фамилия и имя стали эмбоссироваться (механически выдавливаться).

Эмбоссирование – нанесение данных на карточку в виде рельефных знаков. Это позволило значительно быстрее оформлять операцию оплаты картой, делая на ней оттиск слипа. Информация, эмбоссированная на карте, моментально переносится на слип. Способ переноса эмбоссированной на карте информации – механическое давление. Эмбоссирование не вытеснило полностью графическое изображение.

Штрих-кодирование – запись информации таким образом применялась до изобретения магнитной полосы и в платежных системах распространения не получила. Карточки со штрих-кодами, подобными тем, которые наносятся на товары, довольно популярны в специальных карточных программах, где не требуются расчеты. Это связано с относительно низкой стоимостью таких карточек и считывающего оборудования. При этом для лучшей защиты штрих-коды покрываются непрозрачным для невооруженного глаза слоем и считываются в инфракрасном свете.

Магнитные карты – на обратной стороне карты имеется магнитная полоса, иногда фотография держателя и образец его подписи. Способы записи и чтения аналогичны способам, используемым в бытовом магнитофоне. Магнитная полоса может хранить около 100 байт информации, которая считывается специальным считывающим устройством – карт-ридером. Информация, нанесенная на магнитной полосе, имеет идентификационный характер, а стоимостные показатели отсутствуют. На лицевой стороне карточки указываются:

– имя держателя;

– номер его банковской карты;

– шифр отделения банка;

– наименование банка;

– символы электронной системы платежей, в которой используются карточки данного вида;

– голограмма – фирменный знак платежной системы.

Цель нанесения голограммы – сделать внешний вид карты более привлекательным и защитить от подделки; впервые голограмму применили в системе MasterCard 1985 г.; срок пользования картой от полугода до трех лет.

Существует много национальных и международных стандартов на магнитные карты. Наибольшее распространение получил стандарт с трехдорожечной магнитной полосой ISO 7813.

В соответствии со стандартом ISO 7813 на первой дорожке записываются следующие данные: номер карты, имя держателя, срок истечения действия карты, сервис-код (максимальная длина записи – 89 символов); на второй дорожке – номер карты, срок истечения действия, сервис-код (до 40 символов).

Сервис-код – код из двух цифр, определяющий допустимые для данной карты типы операций, например: 03 – только операции, выполняемые банкоматом; 20 – операции, которые требуют авторизации у эмитента.

На третьей дорожке чаще всего записывается PIN-код. Помимо определенных в стандарте величин на магнитной полосе могут записываться некоторые другие коды, например, PVV (PIN Verification Value) или CVC (Card Verification Code) – коды, позволяющие проверить PIN устройством, выполняющим операцию.

Магнитные карты нельзя считать идеальным платежным средством, так как они имеют ряд недостатков:

– плохие эксплуатационные характеристики (информацию на магнитном носителе легко можно разрушить);

– отсутствует возможность надежного обновления информации, что не позволяет хранить на карточке информацию о состоянии счета клиента;

– необходимость обслуживания карты в режиме on-line, что повышает издержки эксплуатации подобной системы;

– слабая защита от мошенничества (эти карточки легко украсть, подделать либо путем производства фальшивок, либо скопировав информацию с них).

Поэтому специалисты предложили более надежный способ записи информации – электрический с применением чипов (от англ. chip – кристалл с интегральной схемой), или микросхемы. Карты с чипом очень часто называются также ***смарт-картами***. Название «смарт-карта» (от англ. smart – интеллектуальная, или разумная) связано с возможностью последней выполнять весьма сложные операции по обработке информации. Основными преимуществами этого вида карт являются повышенная надежность, безопасность и многофункциональность. Существенным недостатком является ее высокая себестоимость. Стоимость таких карт определяется стоимостью микросхемы, которая прямо зависит от размера имеющейся памяти и колеблется для тиража в миллион карточек от 0,6 до 9,5 долл.

Смарт-карты имеют различную емкость. Объем памяти обычной карты составляет приблизительно 256 байт, но существуют карты с объемом памяти от 32 байт до 8 Кбайт. Микросхемы позволяют хранить в памяти такой карты, кроме идентификационной информации, и стоимостные показатели.

Рассмотрим типологию смарт-карт. В зависимости от внутреннего устройства и выполняемых функций специалисты подразделяют смарт-карты на два вида:

– карты с памятью;

– микропроцессорные карты.

Карты с памятью. Это название весьма условно, так как все смарт–карты имеют память. Обычно карты подобного типа используются для хранения информации. Существуют два подтипа подобных карт: с незащищенной и с защищенной памятью.

В ***картах с незащищенной памятью*** нет ограничений по чтению или записи данных. Иногда их называют картами с полнодоступной памятью. Можно произвольно структурировать карту на логическом уровне, рассматривая ее память как набор байтов, который можно скопировать в оперативную память или обновить специальными командами.

Карты с незащищенной памятью использовать в качестве платежных крайне опасно. Достаточно приобрести такую карту легально, скопировать ее память на диск, а дальше после каждой покупки восстанавливать память копированием начального состояния данных с диска, т. е. шифрование данных в памяти карты от мошенничества подобного рода не спасает.

В картах с защищенной памятью используется специальный механизм для разрешения чтения/записи или стирания информации. Чтобы провести эти операции, надо предъявить карте специальный секретный код (а иногда и не один). Предъявление кода означает установление связи с ней и передачу кода «внутрь» карты. Сравнение кода с ключом защиты чтения/записи (стирания) данных проведет сама карта и «сообщит» об этом устройству чтения/записи смарт-карт. Чтение записанных в память карты ключей защиты или копирование памяти карты невозможно. В то же время, зная секретный код (коды), можно прочитать или записать данные, организованные наиболее приемлемым для платежной системы логическим образом. Таким образом, карты с защищенной памятью пригодны для универсальных платежей, хорошо защищены и при этом недороги. Так, цена карты CPM896 составляет не более 4 долл. для тиражей свыше 5 тыс. шт.

Как правило, карты с защищенной памятью содержат область, в которую записываются идентификационные данные. Эти данные не могут быть изменены впоследствии, что очень важно для обеспечения невозможности подлога карты. С этой целью идентификационные данные на карте «прожигаются».

Необходимо также, чтобы на платежной карте были по меньшей мере две защищенные области. С учетом того что в технологии безналичных расчетов по

картам участвуют обычно три юридически независимых лица: клиент, банк и магазин, – банк вносит деньги на карту (кредитует ее), магазин снимает деньги с карты (дебетует ее), и все эти операции должны совершаться с санкции клиента. Таким образом, доступ к данным на карте и операции над ними надо разграничивать. Это достигается разбиением памяти карты на две защищенные разными ключами области – дебетовую и кредитную. Каждый участник операции имеет свой секретный ключ.

Для защиты областей данных от несанкционированного доступа предусматриваются поля, контролирующие доступ к этим данным. Существуют три типа ключей:

I-Key – ключ банка;

P-Key – ключ владельца карточки – PIN-код;

A-Keys – ключи торговых организаций или иных приложений. Использование этих ключей дает возможность доступа к чтению информации из соответствующей области или записи информации. Как правило, активизация одного ключа позволяет только читать информацию, а активизация сразу всех ключей – читать и записывать.

Правильное предъявление PIN-кода открывает доступ к карте (по чтению данных), однако не изменяет информацию, которой распоряжается кредитор карты (банк) или ее дебитор (магазин). Ключ записи информации в кредитную область карты имеется только у банка; ключ записи информации в дебетную область – у магазина. Только при предъявлении сразу двух ключей (PIN-кода клиента и ключа банка при кредитовании, PIN-кода клиента и ключа магазина при дебетовании) можно провести соответствующую финансовую операцию – внести деньги либо списать сумму покупки с карты.

Если в качестве платежных используются карты с одной защищенной областью памяти, значит, банк и магазин будут работать с одной и той же областью, применяя одинаковые ключи защиты. Если банк как эмитент карты может ее дебетовать (например в банкоматах), то магазин права кредитовать карту

не имеет. Однако теоретически такая возможность ему дана, поскольку в силу необходимости дебетования карты при покупках он знает ключ стирания защищенной зоны. То обстоятельство, что и кредитор карты, и ее дебитор (обычно разные лица) пользуются одним ключом, нарушает сразу несколько основных принципов защиты информации (в частности, принципы разделения полномочий и минимальных полномочий). Это рано или поздно приведет к мошенничеству. Не спасают ситуацию и криптографические способы защиты информации.

Из известных карт с защищенной памятью лишь упоминавшаяся уже карта CPM896 обладает двумя защищенными областями памяти и удовлетворяет требованиям по разграничению доступа к информации как со стороны банка, так и со стороны магазина.

Микропроцессорные карты. Они открывают принципиально новые возможности, поскольку имеют свою внутреннюю логику и фактически являются микрокомпьютерами.

В карту встраивается специализированная операционная система, обеспечивающая большой набор сервисных операций и средств безопасности.

Операционная система карты поддерживает файловую систему, предусматривающую разграничение доступа к информации. Для информации, хранимой в любой записи (файл, группа файлов, каталог), могут быть установлены следующие режимы доступа:

– **всегда доступна для чтения/записи.** Этот режим разрешает чтение/запись информации без знания специальных секретных кодов;

– **доступна для чтения, но требует специальных полномочий для записи.** Этот режим разрешает свободное чтение информации, но запись – только после предъявления специального секретного кода;

– **специальные полномочия для чтения/записи.** Этот режим разрешает доступ для чтения или записи после предъявления специального секретного кода, причем коды для чтения и записи могут быть различными;

– **недоступна.** Этот режим не разрешает читать или записывать информацию. Информация доступна только внутренним программам карты. Обычно этот режим устанавливается для записей, содержащих криптографические ключи.

Как правило, в такие карты встроены криптографические средства, обеспечивающие шифрование информации и выработку цифровой подписи. Кроме того, в карте имеются средства ведения ключевой системы.

Карты обеспечивают различный спектр сервисных команд. Для банковских целей наиболее интересны карты как средства ведения электронных платежей.

К специальным средствам относят возможность блокировки работы с картой. Различаются два вида блокировки: при предъявлении неправильного транспортного кода и при несанкционированном доступе.

Суть транспортной блокировки состоит в том, что доступ к карте невозможен без предъявления специального транспортного кода. Этот механизм необходим для защиты от нелегального использования карт при хищении во время пересылки карточки от производителя к потребителю. Карта может быть активизирована только при предъявлении правильного транспортного кода.

Суть блокировки при несанкционированном доступе состоит в том, что если при доступе к информации несколько раз неправильно был предъявлен код доступа, то карта вообще перестает быть работоспособной. При этом в зависимости от установленного режима карта может быть впоследствии либо активизирована при предъявлении специального кода, либо нет. В последнем случае карта становится непригодной для дальнейшего использования.

Пластиковые карты с микросхемами имеют более высокую степень защиты от мошенничества и подделок.

Несмотря на очевидные преимущества, смарт-карты до сих пор имели ограниченное применение по той причине, что такая карта на порядок дороже, чем карта с магнитной полосой. Лишь в последние годы, когда ущерб от мошенничества с магнитными картами в международных платежных системах

стал колоссальным и продолжает расти, банками было принято решение о постепенном переходе на смарт-карты.

Суперсмарт-карты. Примером может служить многоцелевая карта фирм Innovative Card Technologies и eMue Technologies (рис. 6.8). В дополнение ко всем возможностям обычной микропроцессорной карты эта карта также имеет небольшой дисплей и вспомогательную клавиатуру для ввода данных.

Рис. 6.8. Суперсмарт-карта

Эта карта объединяет в себе кредитную, дебетную и предоплатную карты, а также выполняет функции часов, календаря, калькулятора, осуществляет конвертацию валюты, может служить записной книжкой и т. д. Из-за высокой стоимости суперсмарт-карты не имеют сегодня широкого распространения, но их использование будет, вероятно, расти.

Карты оптической памяти имеют большую емкость, чем карты памяти, но данные на них могут быть записаны только один раз. В таких картах используется WORM-технология (однократная запись – многократное чтение). Запись и считывание информации с такой карты производятся специальной аппаратурой с использованием лазера (откуда другое название – лазерная карта). Технология, применяемая в картах, подобна той, которая используется в лазерных дисках. Основное преимущество таких карт – возможность хранения больших объемов информации, однако в банковских технологиях распространения они пока не получили вследствие высокой стоимости как самих карт, так и считывающего оборудования.

Владельцем платежной карты может быть как физическое лицо, имеющее в банке-эмитенте личный счет, так и юридическое лицо, которому открывается корпоративный счет.

Корпоративная карта открывается юридическим лицам и предназначена для управления счетом юридического лица. Выдается она банком-эмитентом или организацией-распространителем отдельным сотрудникам фирмы, правомочным пользоваться ее средствами, а потому на корпоративной платежной карте, кроме названия фирмы, выбивается имя пользователя, так что применять ее может только один человек, которому при оплате товаров, работ или услуг придется подтвердить свою личность.

Фирма может открывать карты для нескольких своих сотрудников, причем каждой карте будет соответствовать свой карт-счет. Ограничений на число открываемых карт внутри одной фирмы не существует.

Нужно подчеркнуть, что приобретение корпоративной карты имеет ряд преимуществ. Прежде всего это более широкий круг возможностей по оперированию счетом. Помимо командировочных расходов при помощи такой карты можно оплачивать услуги переводчиков, получать самые большие скидки в ресторанах, а иногда даже оплачивать контракты. Владелец корпоративной карточки может стать участником самых разнообразных программ своих платежных систем – от дорогостоящих медицинских страховок до компенсационных выплат за задержки рейсов и потерю багажа. Помимо этого, стоит упомянуть тот факт, что сумма денег, находящаяся на счете и выдаваемая банкнотами налично, по корпоративной карте гораздо больше, чем по личной.

Ответственность за ненадлежащее использование корпоративной карты перед банком несет юридическое лицо – владелец, а физическое лицо-пользователь в свою очередь отчитывается перед бухгалтерией фирмы за все расходы, произведенные по корпоративной карте.

В настоящее время в Беларуси получили достаточно широкое распространение так называемые ***«зарплатные» карты***. Сотрудник фирмы, офор-

мивший такой тип карты, может получать заработную плату не наличными деньгами, а путем ее перечисления на карточный счет.

Кроме того, у предприятия появляется гораздо больше возможностей вовремя выдать деньги, поскольку в случае возникновения временного денежного затруднения оно имеет больше шансов получить в банке кредит, который пойдет на зарплату сотрудникам. Ведь банк, предоставляющий предприятию услугу в виде выдачи «зарплатных» карт, не должен перечислять выдаваемые деньги на счета других кредитных организаций. В расчете на то, что часть средств будет некоторое время храниться на карточных счетах сотрудников, банк может предоставить предприятию-клиенту и более льготные условия получения заемных средств.

Защита пластиковых карт от подделки

Пластиковая карта как основной носитель информации для АКА и оборудования POS является притягательным объектом для злоумышленника. Поэтому перед выпуском таких карт необходимо четко представлять степень их защиты от различных воздействий. Существует два основных требования к банковским картам: уникальность и необратимость.

Первое требование означает, что среди всех выпущенных банком карт не должно быть ни одной одинаковой по характеристикам. Воспроизведение подобной карты должно быть исключено для злоумышленника. Согласно второму требованию, не может быть восстановлена первоначальная информация на карте.

Для реализации этих требований каждая фирма-изготовитель предусматривает свои схемы защиты, все тонкости которых она хранит в секрете.

Метод магнитных водяных знаков предусматривает нанесение на магнитную ленту, расположенную на карте, специального рисунка. Этот рисунок наносится при помощи магнитного поля и выполняет ту же самую функцию, что и обычные водяные знаки на ценных бумагах. При изготовлении карточка подвергается воздействию сильного электромагнитного поля под углом 45^0 к

продольной оси. Затем на нее воздействует специальное записывающее устройство, которое преобразует направленность магнитных полей на карточке к особому виду.

Проверка карты с нанесенными магнитными водяными знаками осуществляется специальными устройствами. Этот метод защиты не влияет на информацию, которая записана на информационных дорожках (1 – 3), а добавляет на дорожку 0 от 50 до 100 разрядов дополнительной информации. Эти знаки используются для дополнительной проверки.

Метод «сэндвича» является альтернативой методу водяных знаков и заключается в том, что одна лента содержит участки с различными уровнями намагниченности, причем участок с меньшей намагниченностью расположен ближе к головке чтения/записи. Для записи информации на карту используется сильное магнитное поле. В считывателе информации карта вначале проходит через стирающее поле. При этом на участке со слабой намагниченностью информация стирается, а с сильной намагниченностью – не изменяется. Затем информация с ленты считывается обычным образом.

Надежность этого метода защиты основана на двух предположениях: во-первых, если злоумышленник использует одинарную ленту для подделки карты, то вся информация на ней будет затерта стирающим полем; во-вторых, для записи на двухслойную ленту требуется специальное оборудование для создания необходимого по величине магнитного поля.

Современные пластиковые карты имеют несколько степеней (уровней) защиты. Например, карты системы VISA имеют семь уровней защиты:

1. Торговое имя продукта, которое идентифицирует тип Visa-карты вместе с символом защиты.

2. Вокруг панели расположена кайма впечатанных кодов идентификации банка.

3. Поле fine-line в области идентификации продукции содержит:

– символ защиты;

– идентификатор банка над символом защиты;

– голубь (эмблема Visa), который видим только в ультрафиолетовых лучах;

– трехмерная голограмма голубя.

История злоупотреблений по пластиковым картам началась с момента появления первых кредитных карт. Мошенники пользовались потерянными или украденными картами. Тогда же появились и первые подделки. Информация о счете, эмбоссированная на карте, удалялась бритвенным лезвием, а на ее место наклеивался новый номер, срезанный с другой карты. Этот простейший метод получил настолько широкое распространение, что для него даже родилось специальное название shave & paste («сбрить и наклеить»).

В конце 70-х гг. XX ст. появилась очень распространенная сегодня схема мошенничества, получившая название «белый пластик», явившаяся по сути дальнейшим развитием метода shave & paste. Номера настоящих карточек эмбоссировались на заготовках пластиковых карточек, не имевших «опознавательных знаков» банка и платежной системы (отсюда и название «белый пластик»). Чтобы воспользоваться «белым пластиком», преступникам приходилось вступать в сговор с кассирами торговых предприятий. Кассиры делили с мошенниками доходы от операции после оплаты фальшивого счета банком. Кроме того, в практике мошенничества по схеме «белый пластик» нередко создавались целые фиктивные предприятия. Эквайерам торговых точек необходимо быть очень осторожными в выборе клиентов.

В 1981 – 1982 гг. стали массовыми подделки карт. Изображение наносилось на карты методом шелкографии. На полученных таким образом поддельных картах эмбоссировались номера действительных. При достаточно высоком качестве подделки эти карты можно было использовать без сговора с кассирами. Индустрия пластиковых карт быстро приняла меры по борьбе с этим видом мошенничества: изображение на карточки стали нано-

сить методом литографической печати и дополнять его сложными для подделки элементами, например голограммами.

Серьезной проблемой стал перехват карт, отправляемых держателям по почте. В этом случае мошенники получают в руки настоящую карту, а банк-эмитент или держатель узнают о случившемся только после получения первой выписки о состоянии счета. Сегодня для борьбы с этой проблемой многие эмитенты проводят окончательную персонализацию карт лишь после того, как они попадут к законным владельцам.

С развитием рынка розничных безналичных платежей умножилось и число способов мошенничества с пластиковыми картами. Значительное распространение, например, получили мошенничества с картами в сфере телемаркетинга.

Введение магнитной полосы на пластиковых картах преподносилось прессой как средство, которое сведет уровень мошенничества к нулю. Однако оказалось, что развитие техники мошенничеств практически не отстает от развития техники обеспечения безопасности. В качестве меры защиты информации на магнитной полосе эмитенты стали применять специальные проверочные коды. Примерами их могут служить код CVV (Card Verification Value) в системе Visa и код CVC (Card Verification Code) в системе MasterCard. Введение CVV и CVC существенно снизило возможность использования карт с поддельной магнитной полосой. Однако эти коды явились слабой защитой от копирования магнитной полосы. Голограммы также стали предметом подделок, сегодня карты с поддельными голограммами массово изготавливаются в Азии.

С началом проведения банками расчетных операций по международным платежным картам появились новые виды мошенничества. Так, например, ***«овердрафт с мошенническим применением карты»*** основан на том, что банки и магазины сдают слипы в банк-эквайер раз в две недели, там их обрабатывают и направляют для отчета в банк-эмитент. Мошенник, имея карту с небольшой суммой на счете, в короткий срок проводит через банки и процессин-

говый центр как можно больше операций по выплате денег со счета до того момента, как начнется перевод полученных слипов.

Кроме того, мошенники, досконально знающие банковские процедуры, связанные с обработкой пластиковых карт, пользуются неопытностью и невнимательностью работников банков. Например, компьютерная программа, с помощью которой проводилась авторизация, была рассчитана на полную сумму с указанием долларов и центов. Оператор при запросе не указывал центы, и компьютер воспринимал две последние цифры как центы, уменьшая таким образом сумму при проверке наличия денег на счете на два порядка и позволяя выплату средств, в сотни раз превышающих имеющиеся на счете.

За рубежом в банках и среди специалистов, работающих с сетями передачи транзакций, широко вошло в обиход новое словосочетание ***«шолдер-серфинг»***. Им обозначают использование мощной видеоаппаратуры для определения PIN-кодов, вводимых клиентами при получении наличных в банкоматах, методом ***«подглядывания через плечо»***. Сам факт столь высокого технического оснащения этого метода – один из признаков освоения мошенниками нового рынка. Зная PIN-код держателя карты и определив по брошенной неподалеку квитанции номер карты, преступники получают все необходимые данные для изготовления фальшивых карт. В результате таких мошенничеств зарубежные банки и их клиенты потеряли десятки тысяч долларов.

Принято считать, что банкоматные карты с защитой PIN-кодом безопасны, поскольку потерянную или украденную карточку невозможно использовать (если только держатель карты не записал на ней PIN-код) (рис. 6.9). Другое дело дебетные карты, допускающие авторизацию в режиме off-line (до определенного лимита стоимости покупок), которые служат лишь средством идентификации и не требуют ввода PIN-кода. В последнем случае мошенник может воспользоваться украденной или потерянной картой в торговых организациях. Разумеется, если держатель карты сообщит об ее утере или краже, она может быть немедленно аннулирована.

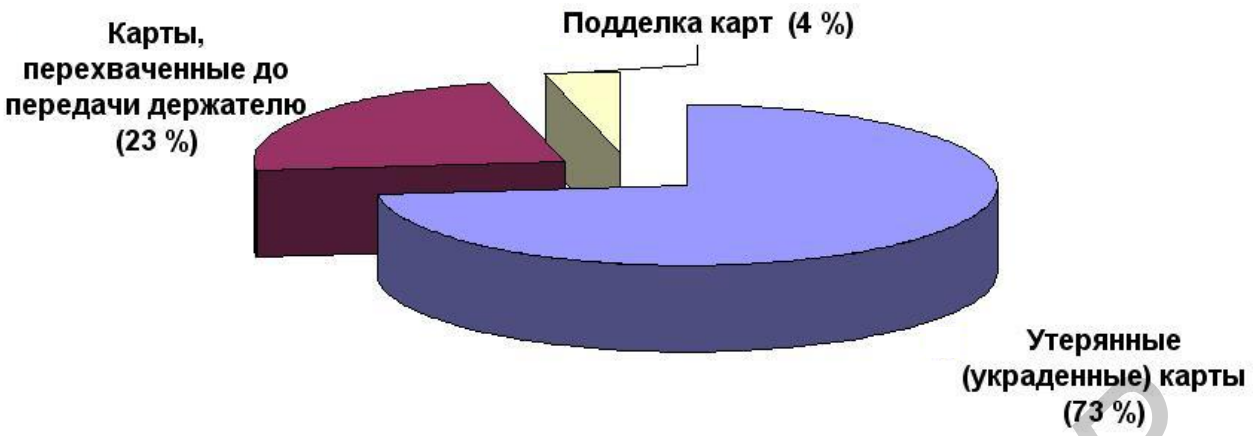


Рис. 6.9. Мошенничества с пластиковыми картами по данным Visa

Безусловно, забота о предотвращении мошенничеств способствует технологическому совершенствованию банкоматных и дебетных карт – появляются микропроцессорные карты.

Электронные карты (смарт-карты) обладают двумя важными качествами, обеспечивающими защиту от различного рода злоупотреблений. Во-первых, электронная карта располагает энергонезависимой программируемой постоянной памятью. В эту память заносится текущая информация, и она сохраняется даже после отключения источника питания. В нее может быть записана стоимость каждой покупки, а также сумма всех затрат, и поэтому клиент, делая покупки, не может превысить установленную сумму. Во-вторых, в каждую карту вмонтирован свой процессор, который при соответствующем выборе архитектуры обеспечит работу карты таким образом, чтобы определенные части памяти были недоступны никому, кроме фирмы, эмитировавшей карту.

С помощью процессора карта сама может сравнить названный ей пароль с правильным, который хранится в секретной зоне ее памяти. Карта может не открывать своего пароля никакой внешней системе. На самом деле даже компании-эмитенту карты не обязательно знать ее пароль. При эмиссии карты ее будущий владелец может сам ввести пароль в память, воспользовавшись специальным терминалом, читающим и записывающим данные в карту. После того как пароль введен (владелец должен ввести его дважды или трижды, чтобы ис-

ключить возможные ошибки) и проверен, карта запоминает его в «секретной зоне» своей памяти.

Кроме пароля в «секретной зоне» хранится также текущий баланс владельца, серийный номер карты, а также последовательность определенных букв и цифр, выбранная фирмой-эмитентом для последующей проверки карты. В другой зоне программируемой постоянной памяти, которая называется открытой зоной, могут быть записаны имя владельца, его адрес, номер телефона и номер его счета. Данные, содержащиеся в открытой зоне, можно прочесть при помощи любого считывающего устройства, работающего с подобными картами, однако изменить эти данные нельзя – центральный процессор откажется выполнить любую команду на изменение информации в открытой зоне. Всякий раз, когда при помощи карты совершается какая-нибудь покупка, такие сведения, как стоимость покупки, название и адрес торгующей организации, а также дата записываются в другую область памяти, называемую рабочей зоной. Данные в эту область могут быть записаны только при соблюдении определенных условий (например когда карточка вставлена в законный кассовый аппарат), причем чтение и запись могут быть произведены только с разрешения владельца карты.

Поскольку широкое распространение смарт-карт в ближайшем будущем вряд ли возможно, упор сегодня делается на организационные меры предотвращения мошенничеств. В частности, в США администраторы сетей банкоматов обращаются к руководству Федеральной резервной системы с просьбой разрешить печатать на квитанциях, выдаваемых банкоматами, неполные номера карт. Входит в практику проверка карт в режиме on-line (даже если ее не требуют эмитенты).

Преступность в сфере пластиковых карт развивается параллельно с самой индустрией карт. Опыт международных платежных систем по внедрению «карточных» программ в разных странах показал, что развитие мошенничества подчиняется определенным закономерностям.

Чисто теоретически мошенничество может произойти на любой стадии выпуска и функционирования карты:

– в банке-эмитенте;

– в банке, обслуживающем торгово-сервисную сеть;

– в торгово-сервисной сети;

– непосредственно в среде держателей карт;

– в компаниях, обслуживающих информационный обмен между участниками платежной системы.

Свою роль здесь играют и чисто технические особенности пластиковых карт, такие, как степени защиты карты, технологические особенности карты (магнитная полоса или микросхема), коммуникационные возможности банка-эмитента и банка-эквайера, техническое оснащение и технологическое обеспечение торгово-сервисной сети.

Основные потери от мошенничества с пластиковыми картами несут банки-эмитенты, так как практически все известные методы мошенничества построены именно на несанкционированном списании средств со счетов клиентов эмитента. Банки, обслуживающие торгово-сервисную сеть, несут убытки только в случае нарушения формальных правил обслуживания пластиковых карт. Если в случае мошенничества формальные правила приема карт платежной системы не были нарушены, возмещение потерь банку-эмитенту происходит либо по решению арбитража платежной системы, либо по взаимной договоренности банков (обычно за счет торговой точки).

Все случаи возникновения потерь банка можно разделить на три категории:

1. Потери из-за мошеннических действий вне системы банка:

– овердрафт на счету клиента из-за мошеннических действий клиента при массовых закупках по карточке ниже авторизационных лимитов магазинов;

– списание средств со счетов клиентов по поддельным картам;

– списание средств со счетов клиентов по утраченным картам;

– списание средств со счетов клиентов по фальшивым финансовым документам.

2. Потери из-за мошеннических действий в системе банка:

– несанкционированная установка на карту кредитного лимита, позволяющая увеличить авторизационный остаток на карт-счете с последующим снятием средств;

– несанкционированная установка в авторизационной системе специального статуса счета, позволяющего в определенных пределах снимать средства с карты (фактически кредитный лимит);

– несанкционированное пополнение счета карты;

– выпуск параллельной карты-двойника;

– несанкционированный выпуск новых пластиковых карт (например с нулевым балансом и пр.).

3. Потери из-за технологических сбоев и ошибок:

– несоблюдение требований платежной системы по оформлению платежей;

– несоблюдение требований платежной системы по передаче информации.

Если говорить о минимизации потерь банка-эмитента, то можно выделить следующие основные моменты обеспечения безопасности:

– обеспечение физической и технологической безопасности процесса производства карт, процессинга транзакций и обеспечения процесса авторизации;

– обеспечение оптимального уровня проверки персональных данных потенциальных держателей пластиковых карт;

– обеспечение информационно-аналитической деятельности по раннему выявлению мошеннических действий с пластиковыми картами.

6.4. Автоматические кассовые аппараты

В настоящее время на автоматические кассовые аппараты (АКА) возлагаются следующие задачи [3]:

– идентификация и аутентификация клиента;

– выдача наличных денег;

– оповещение о состоянии счета клиента;

– перевод денег клиента с одного счета на другой;

– регистрация всех произведенных операций и выдача квитанций.

Основная задача АКА – выдача наличных денег клиенту. Так как внутри АКА, кроме различных устройств, находятся и наличные деньги, то должна быть предусмотрена его серьезная физическая защита.

При рассмотрении дальнейшей защиты хранимой в АКА информации предполагается, что нарушение его внешней физической защиты маловероятно.

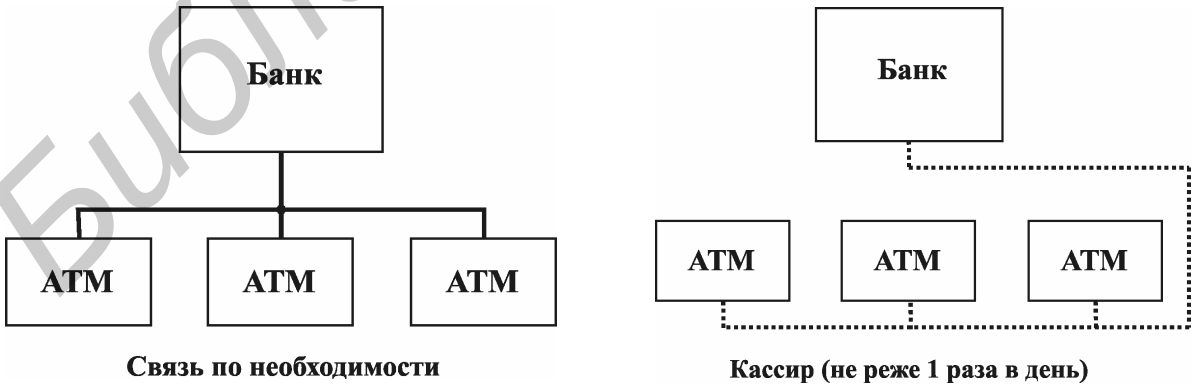
Режимы работы АКА

Автоматический кассовый аппарат может работать в одном из двух режимов:

1. Off-line (автономный режим). В автономном режиме АКА функционирует независимо от компьютеров банка. При этом запись информации о транзакциях производится на внутренний магнитный диск и выводится на встроенный принтер.

2. On-line (режим реального времени). Для работы в этом режиме АКА должен быть подсоединен (непосредственно либо через телефонную сеть) к главному компьютеру банка. При этом регистрация транзакций осуществляется непосредственно на главном компьютере, хотя подтверждение о транзакции выдается на принтер АКА.

Рассмотрим подробнее эти два способа функционирования (рис. 6.10).



а б

Рис. 6.10. Режимы работы АКА: а) On-line; б) Off-line

Как автономный режим работы АКА, так и режим реального времени обладают своими достоинствами и недостатками (табл. 6.1).

Преимуществами автономного режима АКА является его относительная дешевизна и независимость от качества линий связи. Это особенно важно в отечественных условиях, когда качество телефонных линий, мягко говоря, не идеально. В то же время низкая стоимость установки напрямую обуславливает высокую стоимость эксплуатации этих аппаратов. Ведь для того чтобы обновлять списки потерянных карточек, «черные списки» необходимо хотя бы раз в день специально выделенному человеку обновлять в месте расположения АКА. При значительном количестве таких устройств подобное обслуживание затруднительно. Отказ от ежедневного обновления списков может привести к большим потерям для банка в случае подделки карты или при пользовании украденной картой.

Таблица 6.1

Сравнительная характеристика режимов работы АКА

	Режимы работы АКА	
	Автономный	Реального времени
Метод идентификации и аутентификации	Алгоритмический	Алгоритмический и неалгоритмический
Ограничения по суммам выдачи денег на одну карту	Нет	Есть
Устойчивость к потере карты	Слабая. Определяется частотой смены списка потерянных карт и «черного списка»	Сильная. Это обеспечивается централизованным ведением списков и централизованной проверкой идентификаторов
Управление счетом клиента	Нет	Есть
Хранение секретной информации	На магнитной карте и внутри АТМ	Возможно хранение секретной информации только в главном компьютере
Наличие линии связи	Не требуется	Наличие обязательно
Необходимость защиты линии связи	Не требуется	Защита обязательна
Стоимость	Средняя	Высокая

Сложности возникают также и при идентификации (аутентификации) клиента. Для защиты информации, хранящейся на магнитной карте, применяется ее шифрование. Для того чтобы АКА одного и того же банка воспринимали пластиковые карты, в них для шифрования/расшифрования должен быть использован один ключ. Компрометация его хотя бы на одном из АКА приведет к нарушению защиты на всех АКА.

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

Однако этот режим работы возможен лишь при наличии надежных каналов связи между АКА и банком (банками), что делает его довольно дорогим.

Наличие канала связи порождает и другие угрозы безопасности по сравнению с автономным режимом работы: анализ трафика и имитация работы главного компьютера. При первой угрозе анализируются данные, передаваемые АКА главному компьютеру, и полученная на их основе информации о счетах, суммах, условиях платежей и т. д. При второй угрозе главный компьютер может быть имитирован компьютером злоумышленника и на запрос АКА о результатах идентификации/ аутентификации выдавать положительный ответ.

В том случае, когда АКА работают в режиме реального времени, для осуществления идентификации они обмениваются с главным компьютером банка тремя сообщениями (рис. 6.11).

Для АКА, работающих в режиме реального времени, такую защиту организовать довольно просто. Если три попытки ввода PIN оказались неудачными,

то в платеже клиенту отказывается. Ранние системы после трех неудачных попыток не возвращали карту, однако такое решение проблемы, особенно с кредитными картами, не вызвало восторга клиентов.

Для АКА, работающих в автономном режиме, возврат карты в случае трехкратного неудачного ввода PIN является весьма опасным, так как позволяет дальше подбирать PIN.

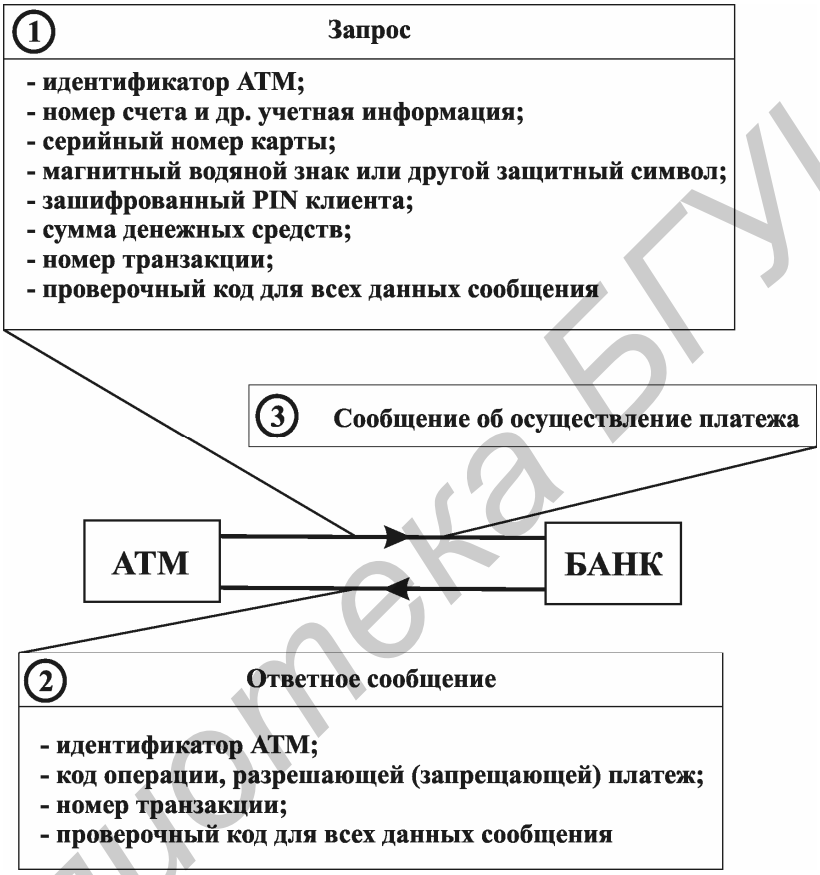


Рис. 6.11. Процесс обмена сообщениями между АТМ и банком

Разделяемые сети АКА

Кроме одиночных АКА в настоящее время эксплуатируются и сети АКА, в которых участвуют несколько банков. Участники такой сети преследуют следующие цели:

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

– уменьшение стоимости операций для участников;

– придание оказываемым услугам общенационального характера и соответственно повышение их субъективной ценности для потребителя;

– возможность для региональных банков, так же как и для банков, расположенных в финансовых центрах, немедленно получить выгоду от либерализации законодательства, регулирующего выход на рынки других стран;

– преодоление имеющихся географических ограничений, которых не существует для небанковских учреждений.

В настоящее время США «покрыты» тремя общенациональными сетями:

1. MasterCard/Cirrus;

2. Plus System;

3. Visa U.S.A.

При совместном использовании банками сети АКА появляется новая проблема – защита конфиденциальной информации банков друг от друга (ключи шифрования, списки номеров запрещенных к использованию карточек и т. д.). Для ее успешного решения была предложена схема централизованной проверки PIN каждым банком в своем центре связи с АКА. При этом также усложняется система распределения ключей между всеми участниками сети.

Рассмотрим подробнее схему прохождения платежа между АКА, банком, которому принадлежит АКА («Получатель»), и банком, который выпустил карточки («Эмитент») (рис. 6.12).

На этом рисунке показан вариант расчета между банками (Банк №1 и Банк №2) в некоторой гипотетической сети АКА. Предположим, что в ней клиент Банка №1 обратился к АКА Банка №2. При этом в сети происходят следующие действия:

1. Считывающее устройство АКА считывает информацию, записанную на банковской карточке, предъявленной клиентом, и затем АКА определяет, имеет ли клиент счет в Банке №2.

2. В том случае, когда клиент не имеет счета в Банке №2, транзакция направляется на сетевой маршрутизатор, который, используя номер идентифика-

ции банка (Bank Identification Number, BIN), направляет ее на главный компьютер Банка №1 или производит проверку PIN для Банка №1.

3. Если проверка PIN производится в самом компьютере Банка №1, то компьютер получает полную информацию о транзакции и проверяет достоверность PIN.

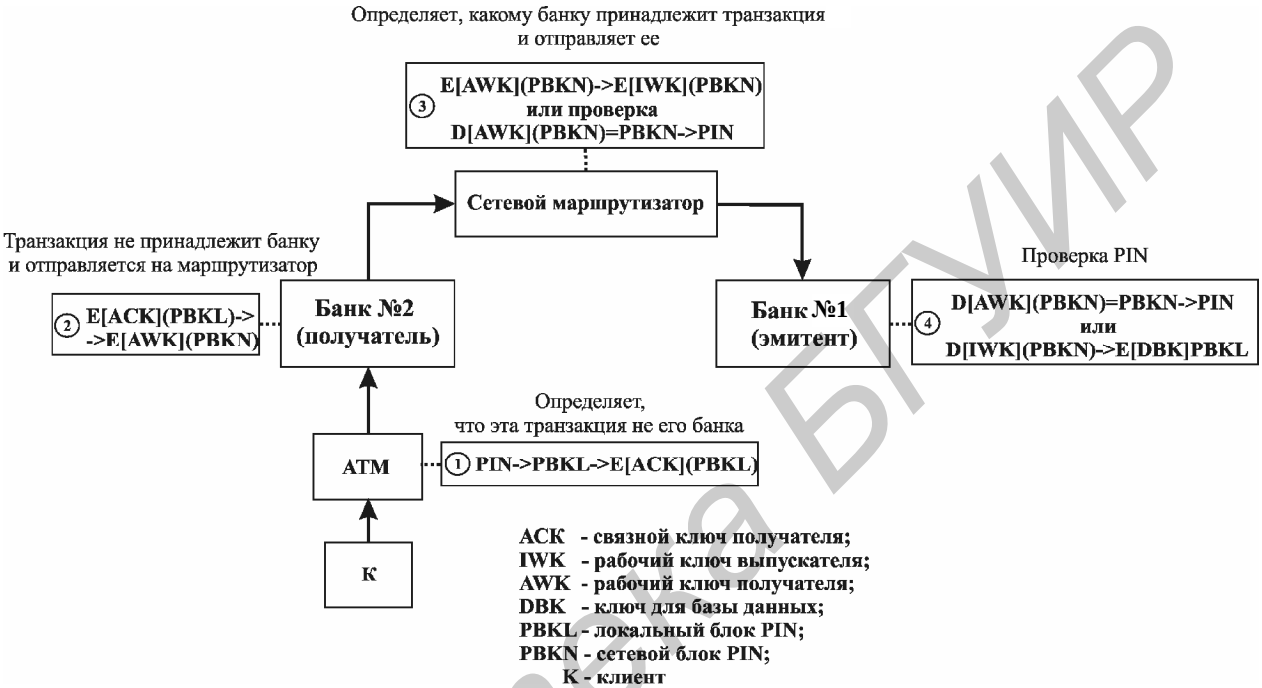


Рис. 6.12. Схема прохождения платежа между АКА, банком–владельцем АКА, банком-эмитентом

4. Вне зависимости от того, с каким результатом завершилась проверка, компьютер Банка №1 пересылает сообщение с результатом проверки через сетевой маршрутизатор компьютеру Банка №2.

Этот пример показывает, что к Эмитенту предъявляются следующие требования:

– выпускаемые им карточки должны восприниматься всеми АКА сети;

– он должен обладать технологией проверки собственных обменных PIN (если в АКА используется встроенная проверка принадлежности транзакции, то главный компьютер должен выполнять результаты проверки в таком же формате).

К Получателю в свою очередь предъявляются другие требования:

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

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

Для защиты взаимодействия компьютеров банков между собой и с АКА применяется оконечное (абонентское) шифрование информации, передаваемой по линиям связи.

Наиболее часто используется следующий метод: вся сеть АКА разбита на зоны и в каждой из них используется свой главный зональный управляющий ключ (Zone Control Master Key; ZCMK). Он предназначен для шифрования ключей при обмене между сетевым маршрутизатором и главным компьютером банка. Ключ индивидуален для всех участников сети. Обычно он случайно генерируется маршрутизатором и неэлектронным способом передается в банк. Раскрытие ключа приведет к раскрытию всех PIN, которые передаются между маршрутизатором и главным компьютером банка.

Для шифрования информации, поступающей от главного компьютера Эмитента на маршрутизатор, используется рабочий ключ Эмитента (Issuer Working Key; IWK). Его сообщает главному компьютеру банка маршрутизатор в зашифрованном (на уникальном ZCMK) виде. Ключ может меняться по запросу пользователя в процессе работы. Аналогичный по назначению ключ для обмена между Получателем и маршрутизатором называется рабочим ключом Получателя (Acquirer Working Key; AWK). Для шифрования информации при передаче от АКА к главному компьютеру банка используется коммуникационный ключ Получателя (Acquirer Communication Key; ACK).

Рассмотренная выше схема обеспечения безопасности взаимодействия компьютеров в сети базируется на алгоритме DES. Именно в связи с этим налагаются жесткие требования на распространение ZCMK. Применение систем

шифрования с открытым ключом позволяет несколько упростить ключевую систему и как следствие взаимодействие между АКА и главными компьютерами.

В неразделяемой сети достаточно на всех АКА использовать один открытый ключ, а на главном компьютере банка – закрытый ключ. Это позволит шифровать запрос и подтверждающее сообщение и проверять подлинность отчетного сообщения из банка, так как обеспечение конфиденциальности ответного сообщения не обязательно. Особого внимания заслуживает проблема защиты запроса от активных атак (изменения или введения ложного запроса). Но и она в случае неразделяемой сети может быть решена с использованием пароля для идентификации АКА.

В случае сети совместно используемых АКА применение системы шифрования с открытым ключом позволяет отказаться от зональных ключей и дорогостоящей процедуры их смены. Однако в этом случае схема идентификации АКА по паролю не будет работать. Эта проблема может быть решена в том случае, когда каждый АКА вместе с запросом будет пересылать и свой открытый ключ, заверенный банком.

6.5. Особенности расчета в точке продажи

Системы POS [5] предназначены для сокращения расходов по обработке бумажных денег и для уменьшения риска покупателя и продавца, связанного с этой обработкой. Схема системы POS представлена на рис. 6.13.

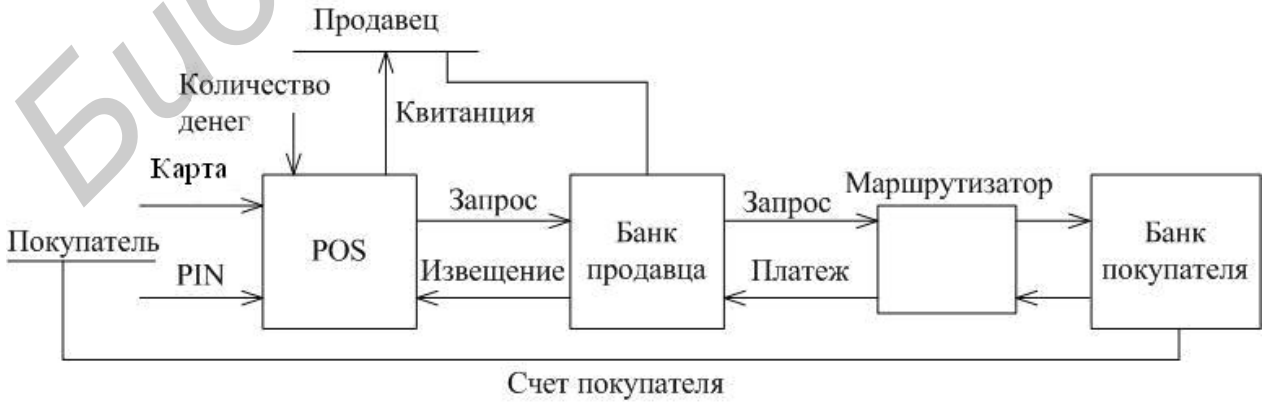


Рис. 6.13. Схема системы POS

Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карту и для подтверждения личности вводит PIN. Продавец со своей стороны вводит сумму, которую необходимо уплатить за покупку или за услуги.

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

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

Для защиты системы POS должны соблюдаться следующие требования:

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

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

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

В связи с этим предположением возникают новые типы угроз для терминала. Они связаны с раскрытием секретного ключа, который находится в тер-

минале POS и служит для шифрования информации, передаваемой терминалом в банк продавца. Угроза вскрытия ключа терминала весьма реальна, так как они устанавливаются в таких неохраняемых местах как магазины, автозаправочные станции и пр. Эти угрозы получили следующие названия:

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

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

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

Метод ключа транзакции (transaction key)

Информация, передаваемая между каждым терминалом и каждым эмитентом карточек, должна быть зашифрована на уникальном ключе, который в свою очередь должен изменяться от транзакции к транзакции. Однако применение этого метода для большого количества терминалов и эмитентов карточек делает затруднительным управление ключами. Поэтому в подавляющем большинстве практических приложений он применяется не к связи «терминал-эмитент карт», а к связи «терминал-получатель», так как каждый получатель имеет ограниченное количество доступных терминалов.

При генерации нового ключа используются следующие составляющие: однонаправленная функция от значения предыдущего ключа; содержание транзакции и информация, полученная с карточки. При этом подразумевается, что

предыдущая транзакция завершилась успешно. Такая схема обеспечивает защиту как от обратного трассирования, так и от прямого. Раскрытие одного ключа не дает возможности злоумышленнику вскрыть все предыдущие или все последующие транзакции.

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

Метод выведенного ключа (derived key)

Этот метод более прост в использовании, однако и менее надежен. Он обеспечивает смену ключа при каждой транзакции независимо от ее содержания. Для генерации ключа здесь используется однонаправленная функция от текущего значения ключа и некоторое случайное значение. Метод обеспечивает защиту только от «обратного трассирования». Процесс получения ключа для шифрования транзакции показан на рис. 6.14. Вершиной дерева является некое начальное значение ключа. Для того чтобы получить ключ с номером S, число S представляется в двоичном виде. Затем, начиная со старшего разряда, идет анализ двоичного представления числа S. Если разряд равен единице, то к текущему значению ключа применяется односторонняя функция FX(K), где X – номер рассматриваемого разряда. В противном случае переходят к рассмотрению следующего разряда без применения односторонней функции. Последняя реализована на основе алгоритма DES. Для увеличения скорости обычно ограничивают количество единиц в двоичном представлении числа S (не более десяти).

Применение открытых ключей

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

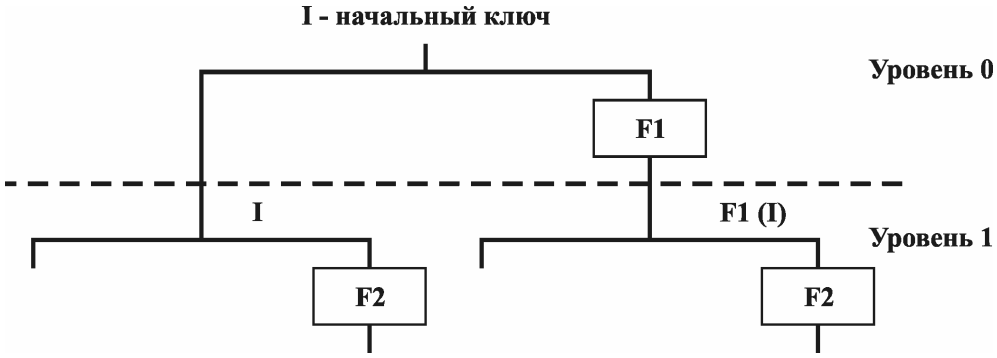


Рис. 6.14. Процесс получения ключа шифрования транзакции

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

6.6. Электронные чеки

Электронный чек (electronuc cheque) является электронным эквивалентом банковского чека, применяемым для платежа. Чек может быть применен как в POS-системах, так и в АКА. Формат электронного чека приведен на рис. 6.15 [3].

Электронный чек состоит из трех частей, включающих сведения о банке, клиенте и чеке. Первые две части – постоянные. В них указаны даты, по истечении которых общий ключ банка и общий ключ клиента становятся недействительными. Переменная часть чека содержит информацию о платеже, получателе и о самом чеке. Информация о чеке необходима для того, чтобы избежать повторений.

Для организации платежей с использованием электронных чеков используются так называемые «электронные бумажники» (electronic wallet), реализованные на базе интеллектуальных карточек.

Рис. 6.15. Структура электронного чека

Электронные чеки в первую очередь предназначены для платежей в точках продажи, которые работают в автономном режиме. Терминал собирает все предъявленные ему чеки за определенный период и обращается в банк, предъявляя их к оплате.

Для удостоверения электронных чеков используется цифровая подпись, выполненная по методу открытого ключа. Подписывается не сам документ, а хэш (hash, битовая строка фиксированной длины) от отдельных его блоков, каждая сторона подписывает только свои блоки. При этом используется один из алгоритмов шифрования с открытым ключом (RSA или DSA). Стойкость этих алгоритмов достаточно велика, для того чтобы подписывать чеки на огромные суммы денег. Пару отрытый/секретный ключ получают в центре сертификации.

Вся индустрия электронного чека основывается на доверии банков и получателей денег к цифровой подписи плательщика. Если секретный ключ будет украден, то ничто не мешает злоумышленнику создавать поддельные чеки, неотличимые от настоящих. Поэтому так важно обеспечить сохранность закрыто-

го ключа. Для этого предназначены устройства, называемые ***электронными чековыми книжками***. Они выдаются банком при создании счёта для выплаты чеков и имеют в своём составе смарт-карту, на которой хранится секретный ключ, информация о владельце, его данные о банковском счёте и сертификат, подписанные банком.

Весь процесс простановки цифровой подписи на чеке проходит внутри смарт-карты; таким образом, секретный ключ не покидает карты и не подвергается риску быть похищенным. Более того, невозможно извлечение секретного ключа из книжки без повреждения последней. Помимо проставления цифровой подписи, чековая книжка выполняет следующие функции:

– добавляет данные о плательщике и его банковском счёте;

– ведёт историю всех выписанных чеков, что может понадобиться при обнаружении фальшивок;

– генерирует случайную строку и добавляет её в начало блока перед хэшированием;

– добавляет в электронный чек свой уникальный заводской номер, проводит их последовательную нумерацию, что гарантирует уникальность номера.

При инициализации банком карты внутри неё происходит генерация пары ключей, затем открытый ключ извлекается и включается в состав сертификата, который подписывает банк. Секретный ключ остается не известен даже банку.

Карта защищается PIN-кодом, без которого невозможно подписание/подтверждение чека. Для каждой карты существует три PIN-кода, открывающих один из нижеперечисленных режимов пользования:

– создание и подписание/подтверждение чека;

– администрирование – открывается возможность изменять системный журнал, сертификат, считывать данные о держателе и его открытый ключ. Также из этого режима можно разблокировать карту, блокированную неправильными действиями пользователя;

– инициализация. Доступна генерация пары ключей и запись личных данных держателя.

6.7. Видеоконтроль POS- и ATM-терминалов

Специфика видеоконтроля кассовых операций

Наиболее часто POS-терминалы применяются в крупных магазинах. Обеспечение безопасности предприятий торговли играет важную роль, так как финансовые и материальные потери составляют значительную часть их бюджета.

По статистике, персонал – кассиры и сотрудники залов – это субъекты, которые приносят убытки предприятиям сферы торговли и услуг. С их участием совершается, по некоторым оценкам, до 50 % краж, что превосходит ущерб, наносимый посетителями.

При потерях магазина 0,3 – 0,5 % оборота особых мер безопасности не требуется, но если потери превышают 1,5 %, необходимо пересмотреть меры обеспечения безопасности торгового предприятия.

Демонстрируя одинаковую структуру потерь в торговле, США и страны Европы разошлись в их величине (рис. 6.16, а, б).

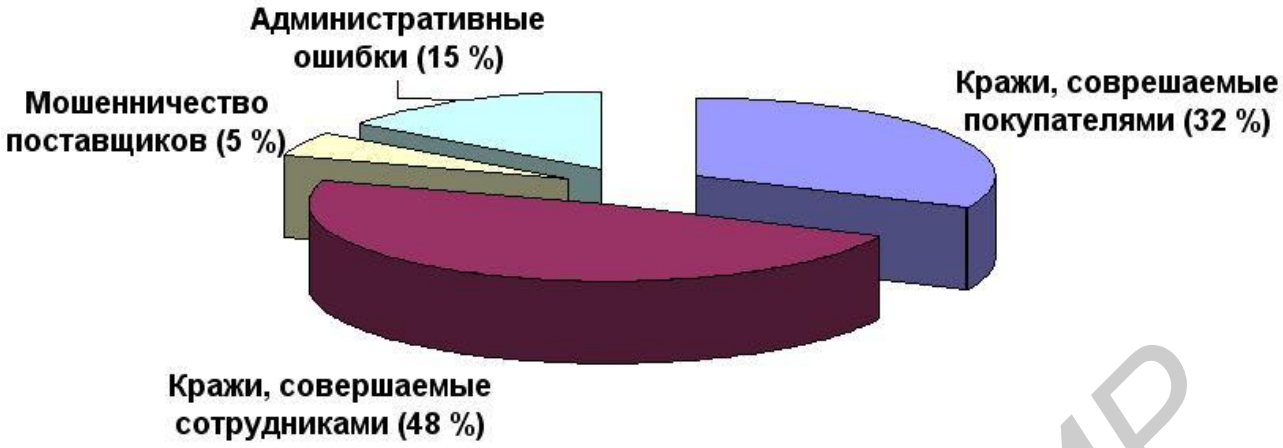
Что касается совершений краж сотрудниками, некоторые специалисты по потерям руководствуются следующей схемой: 10 % сотрудников магазина не станут воровать ни при каких условиях, 10 % будут воровать всегда, а остальные 80 % могут повести себя так или иначе в зависимости от обстоятельств.

Для предотвращения потерь в США используются следующие технические средства безопасности:

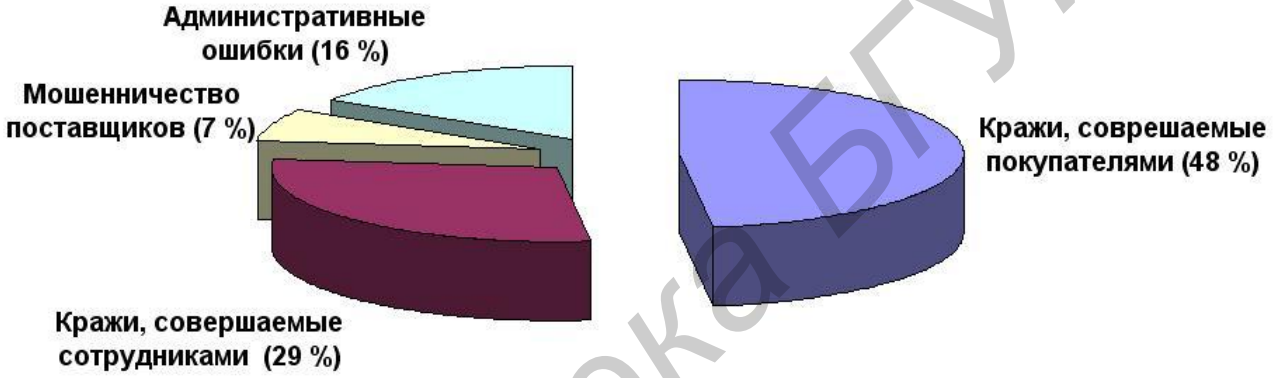
– охранная сигнализация;

– системы охранного телевидения;

– специализированное программное обеспечение для кассовых терминалов.



а



б

Рис. 6.16. Структура потерь в торговле:
а – в США; б – в Западной Европе

Для сотрудников службы безопасности и менеджеров, занимающихся предотвращением потерь компаний розничной торговли, главными целями являются:

– увеличение коэффициента окупаемости инвестиций, сделанных в системы охранного телевидения;

– недопущение ложных тревог;

– сокращение количества краж, совершаемых служащими с использованием своего служебного положения, и повышение общей эффективности круглосуточного хранения товара на складе;

– снижение расходов.

Пока не существует идеального решения, позволяющего улучшить коэффициент окупаемости инвестиций систем видеонаблюдения, можно предло-

жить ряд мер, которые могли бы способствовать качественному изменению систем охранного телевидения:

– повышение качества видеоизображения, что достигается улучшением условий освещения, расположения и качества видеокамеры;

– применение методов дистанционного управления и мониторинга систем охранного телевидения;

– применение цифровых видеорегистраторов и устройств видеопамяти для снижения времени анализа и поиска необходимой записанной видеоинформации;

– применение сетевых технологий для доступа к видеоданным, записанным или передающимся в реальном масштабе времени. IP-протокол позволяет использовать существующую сетевую инфраструктуру.

Системы видеонаблюдения могут быть использованы не только для обеспечения безопасности, но и для других целей, например:

– для отклонения надуманных судебных исков к торговой организации;

– для отслеживания движения потока покупателей;

– при проектировании склада и планировании размещения товаров;

– для отслеживания наличия очередей и улучшения качества обслуживания покупателей.

Другим преимуществом использования систем видеонаблюдения является возможность не только реагировать на правонарушения, но и предотвращать их.

Применение цифровых систем позволяет записывать изображение на жесткий диск и осуществлять поиск нужного фрагмента мгновенно, а также воспроизводить его ускоренно, замедленно или в обратном направлении.

Один оператор следит за несколькими видеокамерами, и потенциальный вор знает, что в данный момент оператор может наблюдать за ним.

Именно поэтому наряду с настоящими работающими видеокамерами применяют и их муляжи, которые внешне похожи на видеокамеры, но по сути вообще не являются оптическими приборами и стоят во много раз дешевле.

Также в магазине может существовать проблема порчи товара прямо в торговом зале, без прохода через кассу. В этом случае может помочь лишь система охранного телевидения.

Системы охранного телевидения не имеют себе равных и по еще одному параметру: они дают отличный способ уличить пойманного вора, предоставив факты совершенного им правонарушения. Современные системы видеонаблюдения позволяют передавать видеосигнал по компьютерным сетям, в том числе по Интернету – видеонаблюдение становится удаленным.

Таким образом, видеонаблюдение превосходит иные методы обеспечения безопасности по эффективности борьбы с воровством, позволяет решить проблему хищений, совершаемых работниками торговых залов и подсобными рабочими. Тем не менее остается проблема преступных махинаций, совершаемых кассирами, которые имеют непосредственный доступ к деньгам.

Существуют угрозы, связанные с мошенничеством кассиров путем осуществления платежа за приобретаемый товар с последующим возвратом денежных средств плательщику. Причем товар обратно в торговое предприятие не возвращается, а остается у покупателя, что адекватно краже товара.

В отсутствие системы видеоконтроля кассовых операций обнаружить эту махинацию было бы невозможно, разве что случайно. Применение на практике систем видеоконтроля приобретает характер систематического исследования. Оператору достаточно настроить свою систему так, чтобы она мгновенно сообщила ему о том, что произошел «возврат товара». На титрах оператор увидит, что операция эта относилась к определенному товару, а на видеоизображении – как этот товар остался у «покупателя». Пример изображения, получаемого с помощью системы видеоконтроля кассовых операций, приведен на рис. 6.17.

Рис. 6.17. Изображения, получаемые на экране системы видеоконтроля кассовых операций

Система ведет базу данных, в которую входит не только содержимое чека, но и различные события, происходящие на кассе. В этой базе можно вести поиск и собирать статистику. Число критериев, по которым делается такой поиск, огромно. Поиск чека возможен по номеру или по времени, когда он был выдан, возможно найти все чеки за определенный период, чеки, содержащие определенный товар, или чеки, в которых итоговая денежная сумма превышает некий заданный порог, а также все чеки с такой-то фамилией кассира или номером кассы. При поиске вместе с чеком будет найдена, разумеется, и запись из видеоархива.

Очень важным является поиск чеков по видам содержащихся в них операций, а также поиск событий на кассе. Так, наметив себе какую-либо опера-

цию, которую кассиры часто используют для мошенничества, можно найти все случаи использования этой операции за любой период. Вот лишь некоторые виды операций, которые представляют интерес с этой точки зрения: возврат чека, отмена чека, предоставление покупателю скидки, отказ в предоставлении скидки.

К отдельной группе критериев для поиска относятся многие события на кассе, например, открытие ящика с деньгами без пробития чека или попытка войти в кассу с правами администратора. Система позволяет множеством способов группировать те события, которые происходят на кассе и находят свое отражение в чеке.

Все это означает, что возможно анализировать многодневный ход событий на кассах, выявляя различных мошенников. Система соберет любую статистику по всем кассам, поможет выявить подозрительное в поведении отдельного кассира.

Система видеоконтроля кассовых операций позволит также противостоять обману кассиром покупателя, когда, например, кассир пробивает один и тот же товар дважды.

С помощью видеоконтроля кассовых операций кассиры лишены возможности мошенничества по отношению к предприятию и покупателю. Применение данных систем не ограничивается торговыми предприятиями, а также возможно на автозаправочной станции, в ресторане и в развлекательном центре.

Системы видеоконтроля кассовых операций призваны свести к минимуму потери торгового предприятия, связанные с действиями недобросовестного персонала.

Специфика видеоконтроля АТМ-терминалов

Средства видеоконтроля и сигнализации АТМ-терминалов играют важную роль в обеспечении их безопасной эксплуатации, осуществляя видеонаблюдение места установки АТМ, регистрацию и хранение информации в видеоархиве, а также оперативное оповещение при возникновении нештатных ситуаций.

Каждый из возможных сценариев действий злоумышленников (с целью овладения наличными денежными средствами, хранящимися в терминале, акты вандализма по отношению к самому АТМ, попытки мошенничества при выполнении операций по снятию наличных) предъявляет свои специфические требования к составу и характеристикам средств видеоконтроля и сигнализации АТМ. С учетом этих требований должны быть предусмотрены использование широкого спектра различных датчиков, устанавливаемых непосредственно в банкомате (сейсмодатчик, термический датчик, датчик открытия сейфового замка), установка нескольких видеокамер, обеспечение долговременного хранения видеоархива и ряд других мер, в большинстве случаев регламентированных требованиями международных платежных систем.

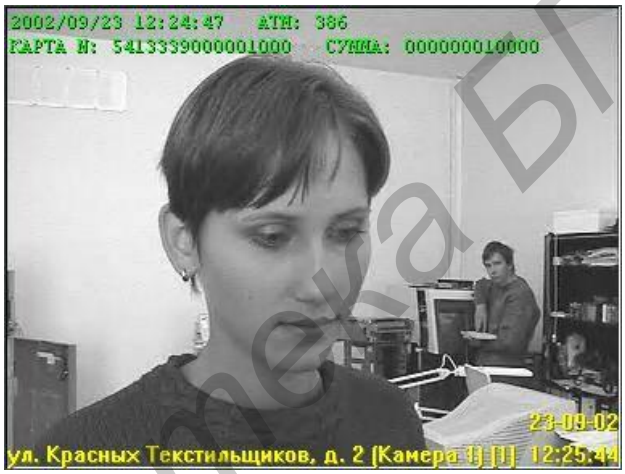
Кроме того, для эффективной и надежной работы средств видеоконтроля банкоматов должны быть задействованы дополнительные средства, обеспечивающие защиту самих средств видеоконтроля банкоматов от воздействия со стороны злоумышленников: ослепление видеокамер, затемнение места установки банкомата и т. д.

Специфика банкомата как объекта видеоконтроля устанавливает определенные требования и к функции видеозаписи. Последняя должна предусматривать видеозапись одновременно с нескольких видеокамер, инициализацию видеозаписи по срабатыванию детектора движения или датчиков охранной сигнализации с обеспечением возможности «отката» времени начала записи, циклический режим записи (стирание устаревших архивов и запись на их место новых при условии обеспечения требуемого срока хранения архивных записей).

Число подключаемых к системе охранного телевидения видеокамер определяется спецификой места установки и режимом эксплуатации банкомата (в помещении банка или вне его, время работы банкомата, характеристики сервисной зоны и т. д.) Минимально предусматривается подключение двух видеокамер: одна обеспечивает фронтальный обзор, фиксируя внешность клиента, вторая обеспечивает обзор зоны выдачи наличных средств и зоны карт-ридера

банкомата, фиксируя факт выдачи наличных и данные об используемой карте (рис. 6.18).

а



б

Рис. 6.18. Изображения с видеокамер банкомата:
а – зоны карт-ридера и выдачи банкнот; б – с фронтальной камеры

Для обеспечения защиты видеокамер от внешнего воздействия со стороны злоумышленников (ослепление видеокамер, затемнение места установки банкомата) используются светофильтры и устройства инфракрасной подсветки. В подобных случаях датчики, установленные непосредственно в банкомате, обеспечивают оперативное оповещение системы об обнаруженных ими признаках попыток затруднить работу средств видеонаблюдения, а также немедленное включение сигнализации. Такая система является основным компонентом локальной видеоохранной сети. В функции этой системы входят: запись видеоинформации в видеоархив, предоставление оперативной видеоинформации опера-

тору, просмотр видеоархива и взаимодействие с системой централизованного видеоконтроля сети банкоматов.

Варианты подключения системы видеоконтроля

Существует несколько вариантов подключения системы видеоконтроля к POS- и ATM-терминалам. У каждого варианта подключения имеются свои особенности.

Использование систем видеоконтроля является уже устоявшимся на рынке решением. При этом оператор системы видеонаблюдения в реальном времени видит на экране чек, пробиваемый кассиром, либо транзакции, произведенные клиентом ATM-терминала.

Можно использовать три варианта физического подключения системы видеоконтроля к POS- или ATM-терминалу:

– через чековый принтер или свободный COM-порт (RS–232);

– через компьютерную сеть;

– напрямую к POS- или ATM-серверу.

Первый и наиболее старый вариант (рис. 6.19) – подключение системы видеоконтроля в разрыв чекового принтера или к свободному COM-порту терминала. Для подключения в разрыв используется Y-разветвитель. Этот способ работает по принципу считывания текстовой информации с чека.

В таком случае каждый терминал является самостоятельной единицей и напрямую отсылает данные в систему видеоконтроля. Данный вариант, как правило, используется, когда невозможна (например в силу технических причин) модернизация программного обеспечения (ПО) для работы через телекоммуникационную сеть. Таким образом принимаются данные, отправляемые на чековый принтер.

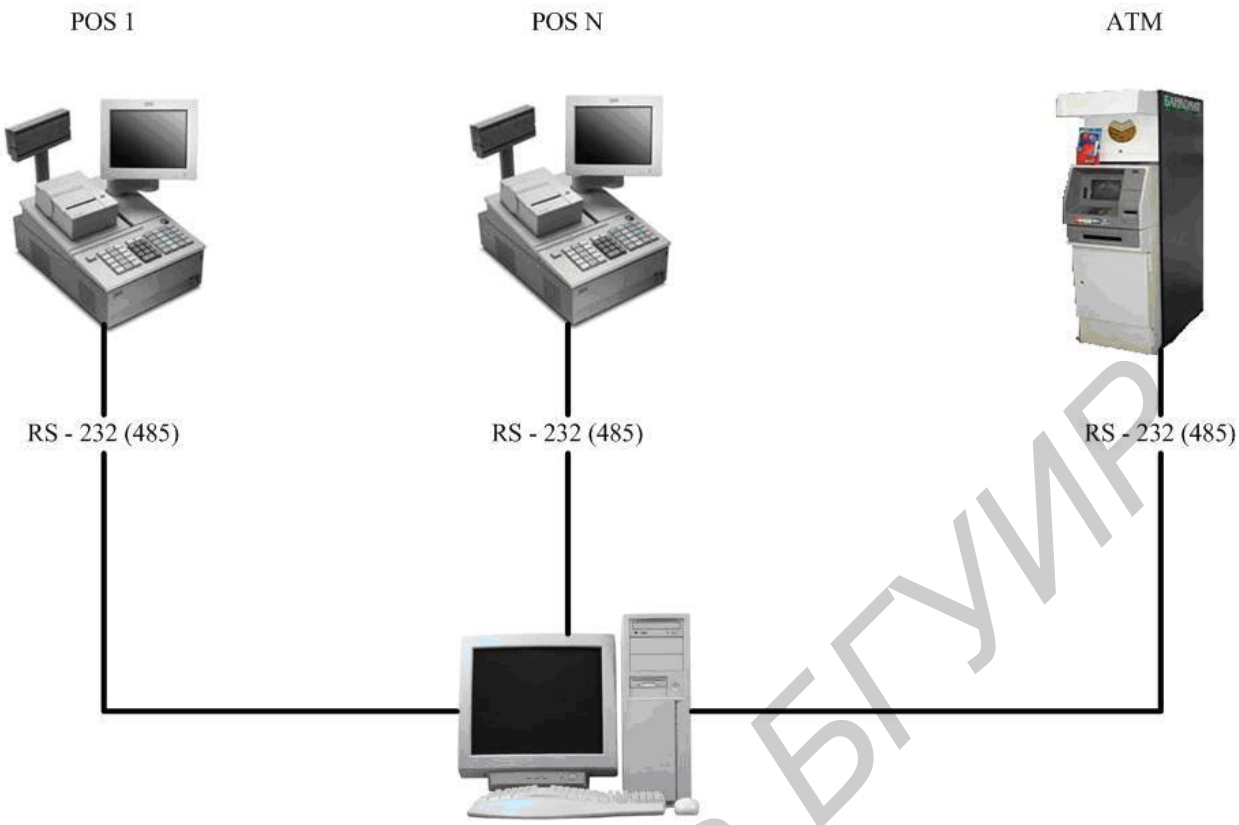


Рис. 6.19. Подключение системы видеоконтроля в разрыв чекового принтера или к свободному COM-порту

Этот вариант стал уже классическим. Так подключались к POS- и ATM-терминалам первые системы видеоконтроля. Недостатки данного подхода выявляются на этапе инсталляции: необходимо прокладывать отдельный кабель от терминала до видеосервера. При этом стандарт RS–232 накладывает жесткие ограничения на длину кабеля, что делает невозможной установку видеосервера на расстоянии свыше 100 м от терминала, что актуально, например, для больших магазинов. Для решения этой проблемы можно использовать пару конвертеров RS–232/485. В таком случае расстояние от терминала до видеосервера может составлять более 1 км.

Другим, более изящным решением является использование преобразователей COM-порта в сеть. В этом случае преобразователь располагается максимально близко к терминалам. Он получает данные от терминалов через RS–232,

далее преобразует сигнал и отсылает по сети на видеосервер. На видеосервере в свою очередь устанавливается драйвер для данного устройства, который создает в системе дополнительные виртуальные COM-порты, соответствующие числу каналов этого преобразователя. Программное обеспечение видеосервера работает с вновь созданными виртуальными COM-портами, как с обычными COM-портами.

Далее данные, полученные с терминалов, подвергаются обработке уже в системе видеоконтроля. Эти данные представляют собой просто текст чека. Как правило, большинство систем ограничивается очисткой чека от служебных символов. Затем информация сохраняется в базе данных, с которой впоследствии работает оператор. При таком подходе возможности пользователя по ведению аналитической работы с архивными данными сильно ограничены. Как правило, поиск по архиву сводится в этом случае к полнотекстовому поиску по подстроке.

Самым существенным недостатком такого варианта является то, что на чековый принтер попадают не все данные, отражающие происходящее на терминале. Более того, большинство таких событий никогда не печатается в чеке. Например, в чек, как правило, не попадают следующие события, которые представляют интерес для службы безопасности магазина:

– попытка отмены товара в чеке;

– отмена позиции;

– открытие денежного ящика;

– вход в режим налогового инспектора;

– попытка выхода из кассовой программы.

Второй способ подключения – использование существующей инфраструктуры магазина или банка (рис. 6.20).

Суть данного способа – в получении информации на основе событий (событийная интеграция). В этом случае видеосервер подключается в одну сеть с терминалами и принимает данные через телекоммуникационную сеть.

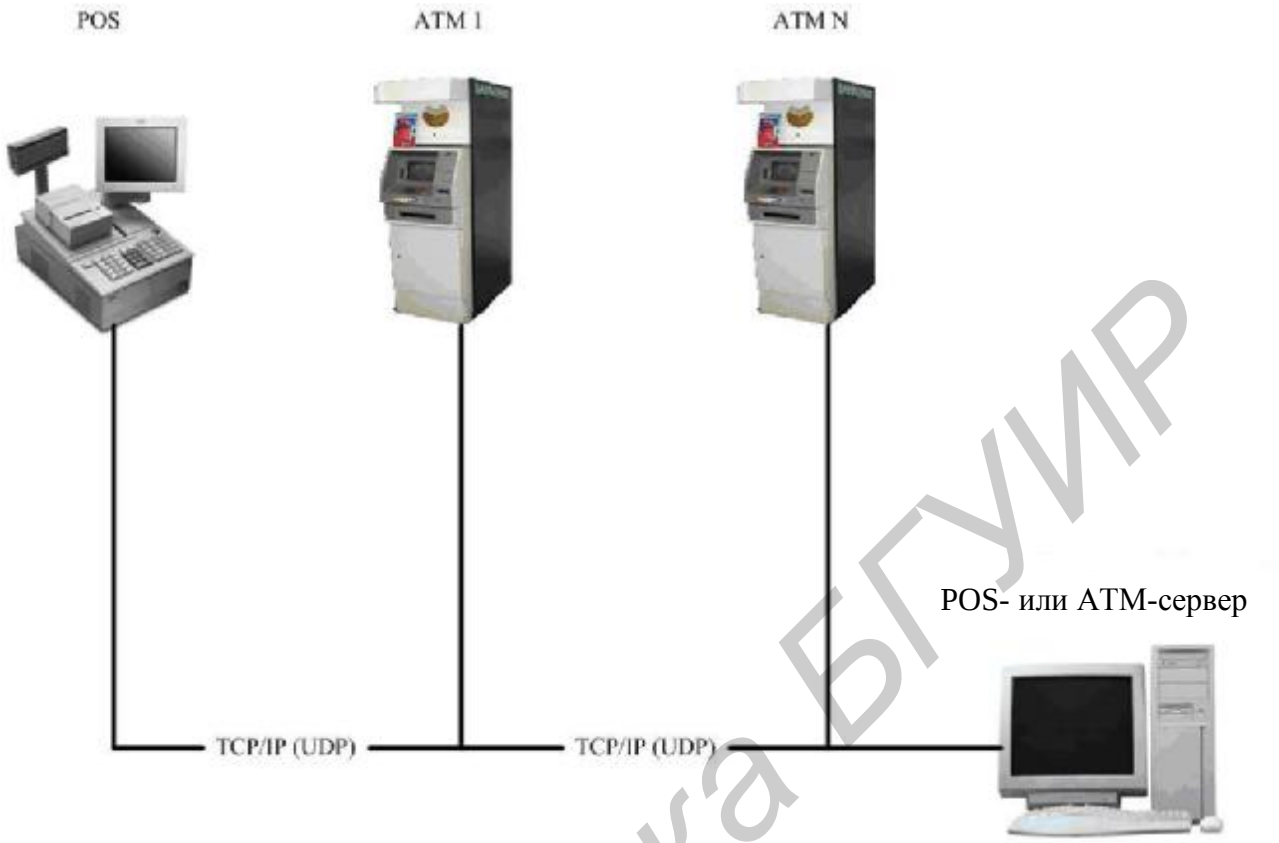


Рис. 6.20. Подключение системы видеоконтроля в компьютерную сеть

На физическом уровне построения системы здесь возможны два варианта:

– данные принимаются от каждого терминала отдельно;

– данные по всем терминалам отсылает один сервер.

Как правило, чаще используется первый вариант, поскольку возможны случаи, когда сервер находится не в режиме постоянной связи с терминалами, а только периодически к ним подключается. Кроме того, во втором случае возможна задержка по времени, хотя и незначительная, когда данные пересылаются от терминала на сервер, обрабатываются там и передаются видеоподсистеме.

Как правило, подключение терминала к системе видеоконтроля через сеть требует доработки ПО. В этом случае видеосервер принимает события, а программа на терминале является клиентом по отношению к нему. В случае ис-

пользования протокола TCP/IP важно предусмотреть, чтобы в программе были средства для восстановления связи.

Важно отметить, что не всегда возможна доработка ПО терминала, функционирующего под управлением DOS, для работы через сеть. В таком случае можно также использовать XML-протокол, но передавать все данные через дополнительный COM-порт. В ПО, написанном для Windows или Linux, добавить поддержку отправки событий не представляет особых сложностей.

Рис. 6.21. Подключение системы видеоконтроля к POS или ATM серверу

Третий вариант подключения показан на рис. 6.21. В этом случае происходит не обмен данными, а использование системой программного модуля для взаимодействия с сервером. Данный подход нужен, как правило, при подключении к системе видеоконтроля какой-либо legacy-системы, т. е. системы, которая уже устарела, но еще используется заказчиком. Доработка такой системы

обычно не представляется возможной, но в этом случае систему видеоконтроля можно подключить напрямую к серверу для их совместной работы. Рассмотрим варианты реализации систем видеоконтроля POS- и ATM-терминалов на практике.

Система видеоконтроля «POS-Интеллект»

Система «POS-Интеллект» (Россия) позволяет контролировать процесс обмена товара на денежные средства, объединяя видеоизображение с данными кассового терминала. Система видеонаблюдения работает совместно с кассовым терминалом, в цифровом видеоархиве фиксируются все события и чеки.

В итоге оператор системы получает информацию о событиях, происходящих на кассовом узле, в виде титров, наложенных поверх видеоизображения. При этом происходит одновременная запись видеоархива и данных.

Сравнение чека с видеозаписью того, что происходило около кассы, принципиально меняет ситуацию с мошенничеством кассиров, сводит возможность их злоупотреблений к минимуму.

Поиск в видеоархиве ведется по множеству разных критериев. Предусмотрена также возможность составления абсолютно любых отчетов по работе каждой кассы. Статистика, собранная за день, позволит без труда выявить кассу, в работе которой есть что-то нестандартное, подозрительное.

Оператору системы предоставлены все возможности. Это простой дружественный интерфейс, удаленный доступ, разграничение прав пользователей, макрокоманды и даже внутренний язык программирования для реализации сложной реакции на событие, происходящее на кассе.

На рынке давно существует аппаратное решение, которое объединяет аналоговый сигнал видеокамеры и данные с кассового аппарата и на выходе выдает видеосигнал с наложенным текстом. Главные его недостатки – невозможность поиска по контекстной информации, постоянное отображение титров, отсутствие событийной модели для принятия решений.

Кроме того, сейчас в магазинах существующая инфрастуктура все чаще используется для передачи данных от касс по сети. В этом случае данные отсылает либо кассовая программа, либо кассовый сервер. И тогда для получения видеоизображения можно использовать либо сетевую видеокамеру, либо сетевой видеосервер. Это в значительной степени уменьшит проблемы с прокладкой кабеля.

Поскольку в системе кассового видеонаблюдения большое значение имеет разрешение установленной видеокамеры, то открываются перспективы для использования в ней мегапиксельных сетевых видеокамер. Кроме того, заложенная в системе «POS-Интеллект» возможность записи видеоизображения синхронно со звуком позволяет получить достоверную картину всего, что происходит на кассе и возле нее.

В системе видеоконтроля также возможно наложение поверх изображения с одной видеокамеры титров сразу от нескольких кассовых терминалов. Оператор системы по своему желанию может включить и выключить отображение данных только от тех касс, которые его интересуют в данный момент. Таким образом, наложение титров не будет мешать просмотру видеоизображения и анализу архива.

Одна из особенностей системы «POS-Интеллект» – возможность построения единой системы видеонаблюдения для всего магазина, в том числе и для прилегающей территории. Например, внутри магазина может функционировать кассовый видеоконтроль, на входе будет установлен модуль распознавания лиц, а на парковке – система распознавания автомобильных номеров. Все это будет контролироваться с рабочего места оператора.

Уникальность системы заключается в том, что она, получая на вход просто текст чека, выделяет из него нужные составляющие и сохраняет их в базе данных. Фактически неструктурированный чек приводится к структурированному виду.

Таким образом, если есть возможность подключиться к данному типу кассового терминала по сети или через последовательный интерфейс (RS–232), то система будет работать с ним (рис. 6.22).

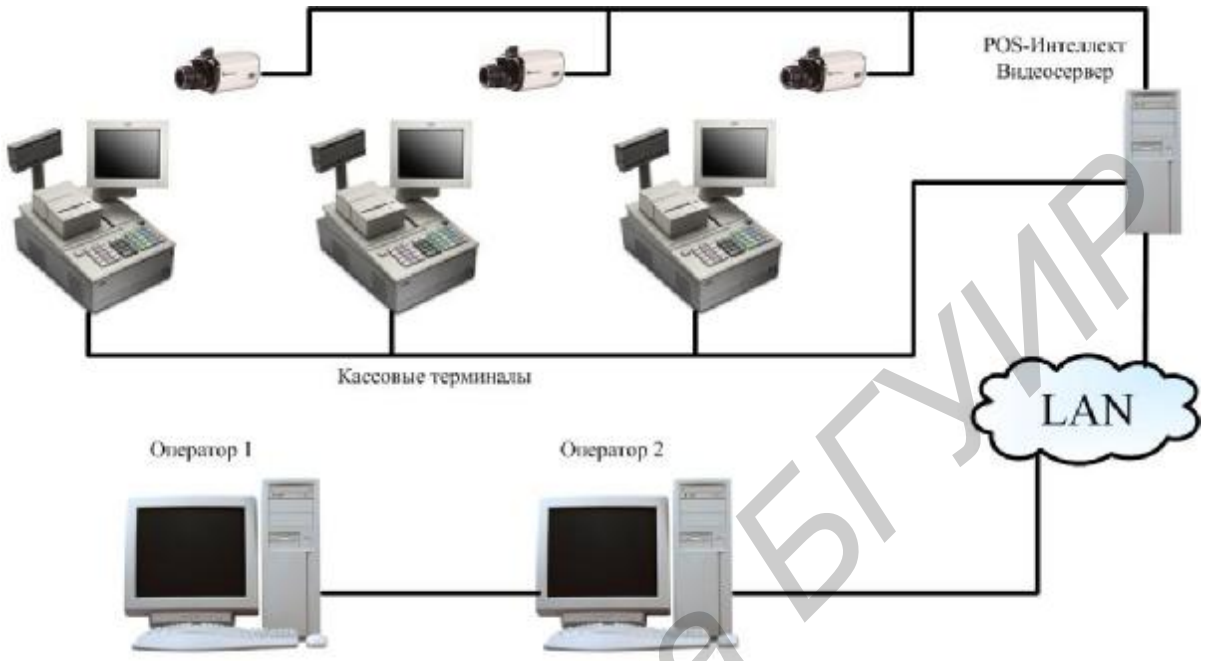


Рис. 6.22. Схема системы POS-Интеллект

Интеграция двух систем подключения реализована на уровне сетевой передачи данных, в результате чего информация о чеке передается по внутренней кассовой сети, что существенно снижает затраты на монтаж кабеля и дополнительное оборудование. Основное преимущество интеграции: такая система позволяет передавать на видеосервер дополнительную служебную информацию, которая не отображается в чеке при печати. Эта информация позволяет отследить все подозрительные операции кассира над чеком, такие, как «Отмена», «Возврат», «Удаление», и полностью предотвратить попытки мошенничества на кассе. Интерфейс рабочей среды программного обеспечения «POS-Интеллект» показан на рис. 6.23.

С помощью системы «POS-Интеллект» можно не только выявлять тех, кто злоупотребляет своим положением, но и тех, кто работает добросовестно.

Система поможет руководителю собрать данные, на основании которых он определит лучших кассиров, чтобы премировать их.

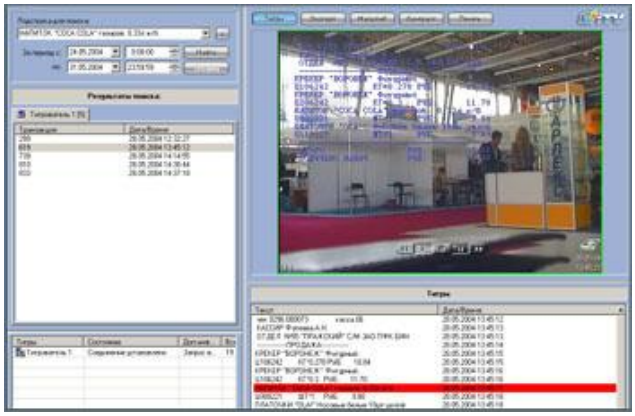


Рис. 6.23. Интерфейс программного обеспечения «POS-Интеллект»

Система видеоконтроля «АТМ-Интеллект»

Система «АТМ-Интеллект» (Россия) выводит защиту банкоматов на качественно новый уровень, поскольку в ней реализована интеграция систем безопасности транзакций, видеонаблюдения и тревожной сигнализации. Эта система является распределенной, охватывающей единой сетью все защищаемые банкоматы и те подразделения службы безопасности банка, которые отвечают за их сохранность.

Важнейшей особенностью системы «АТМ-Интеллект» является синхронизация данных о транзакциях банкомата с видеоархивом, получаемым с телекамер, которые установлены в банкомате.

Одна телекамера снимает все, что происходит возле банкомата. Она показывает лицо человека, который стоит перед этим банкоматом. При этом видно, чем он занят – вставляет карточку, вспоминает PIN-код. Другая камера крупным планом снимает верхнюю часть лицевой стороны банкомата. В поле зрения этой камеры попадает вставляемая в считыватель карточка, на которой можно прочитать все ее реквизиты, а также увидеть деньги, извлекаемые из банкомата. Клавиатура, с которой вводится PIN-код, наоборот, не видна, и сделано это специально, ибо знать PIN-код вкладчика вправе только он сам (рис. 6.24).

Внутри банкомата помещается компьютер, который принимает видеоизображение с обеих телекамер и записывает его на встроенные жесткие диски. На них размещается видеоархив. Систем, которые делают аналогичную работу, немало. «АТМ-Интеллект» отличается от них, в частности, тем, что в ней производится привязка видеоархива к записи транзакций, совершаемых через банкомат.

Рис. 6.24. Интерфейс программного обеспечения «АТМ-Интеллект»

Для разбора жалоб держателей банковских карт в системе «АТМ-Интеллект» создаются автоматизированные рабочие места (АРМ). Оператор такого АРМ может быстро получать информацию по данным транзакции, с которой связана жалоба, и удаленно находить в видеоархиве запись событий, происходивших в момент совершения спорной транзакции.

Возможность организации АРМ является второй существенной особенностью системы «АТМ-Интеллект». Кроме разбора претензий, АРМ создаются и для того, чтобы оперативно получать информацию о неисправности системы. В этом случае они размещаются в сервисной компании, которая обслуживает банкоматы.

АРМ связаны единой распределенной сетью с банкоматами банка. По этой сети оператор АРМ может послать запрос в компьютер, установленный в банкомате. В этом запросе он укажет, какая транзакция или какой момент вре-

мени его интересует, и в ответ получит выдержки из видеоархива в виде отдельных кадров. По ним он сможет узнать, что произошло.

Для соединения банкоматов с АРМ и далее с единым центром, из которого можно контролировать работу всей системы «АТМ-Интеллект», отдельных линий связи не прокладывают. Вместо этого используются штатные каналы связи банкоматов, т. е. каналы, по которым производятся транзакции. Такое двойное использование каналов является еще одной отличительной особенностью системы «АТМ-Интеллект».

В состав территориально-распределенной системы «АТМ-Интеллект» входят:

– локальные системы видеонаблюдения банкоматов;

– пульты дистанционного видеоконтроля группы банкоматов;

– пульт контроля технического состояния системы видеонаблюдения.

Локальная система видеонаблюдения помещается в месте расположения банкомата. Она может находиться внутри самого банкомата или рядом с ним, а если банкомат стоит в банке, то для локальной системы видеонаблюдения выделяется специальная комната.

Основой локальной системы видеонаблюдения служит компьютер, который управляет настройками видеокамер, ведет запись получаемого с них изображения в архив, передает оператору на пульты дистанционного видеоконтроля сигналы тревоги с датчиков и запрашиваемые им выдержки из видеоархива, принимает запросы от оператора.

В одну локальную систему входят, как указывалось выше, две видеокамеры, хотя в принципе их может быть и больше. Видеокамеры снабжены инфракрасной подсветкой и светофильтрами. Это не только улучшает условия съемки, но и защищает телекамеры от тех злоумышленников, которые знают о наличии системы видеонаблюдения и могут попытаться их ослепить или отключить освещение того места, где установлен банкомат.

Видеоархив ведется на жестких дисках компьютера локальной системы видеонаблюдения. Объем архива одного банкомата задается в пределах от 40 до 100 ГБайт. В него обычно записывается черно-белое изображение разрешением 384x288. Запись видеоизображения в архив происходит по циклу: когда диск заполнился, компьютер продолжает вести новую запись поверх старой.

Данные о транзакциях в банкомате поступают в компьютер локальной системы видеонаблюдения. Эти данные включают в себя номер транзакции и реквизиты пластиковой карты.

Данные о транзакциях привязываются по времени к записи видеоархива. При просмотре записи поверх кадра выводятся дата и время, когда она сделана. На записи, относящейся к моментам совершения транзакций, на изображение накладываются параметры этой транзакции. По этим параметрам, а также по дате и времени в видеоархиве можно вести поиск.

Несколько локальных систем видеонаблюдения связаны по сети с пультом дистанционного видеоконтроля, который расположен в подразделении службы безопасности банка. На пульт приходят сигналы тревоги от локальных систем, в нем происходит визуализация этих сигналов. Здесь же формируются запросы на поиск видеоизображения в видеоархивах локальных систем. С пульта эти запросы передаются в локальные системы, после чего оттуда на пульт поступают результаты поиска.

Пульт дистанционного видеоконтроля и локальные системы видеонаблюдения взаимодействуют между собой по протоколам TCP/IP или X.25, причем для этого могут использоваться не только штатные сети банкоматов, но и отдельные специально проложенные каналы.

В подразделении банка или в сервисной компании размещается пульт контроля технического состояния охранной системы видеонаблюдения банкоматов. С него ведется контроль технического состояния всей системы «АТМ-Интеллект». Данные о ее состоянии поступают по сети передачи данных

по протоколу TCP/IP сначала на пульты дистанционного видеоконтроля, а оттуда – на пульт контроля технического состояния.

Вопросы для самоконтроля

1. Чем различаются формы организации персональных платежей?
2. Какое назначение персонального идентификатора?
3. Какие существуют алгоритмы идентификации клиента?
4. Какие существуют альтернативы персональному идентификатору?
5. Какое назначение электронных пластиковых карт?
6. По каким критериям классифицируют пластиковые карты?
7. Какие используют типы ключей для защиты областей памяти пластиковой карты от несанкционированного доступа?
8. Какие методы защиты пластиковых карт широко используют на практике?
9. Каково назначение автоматических кассовых аппаратов?
10. В чем отличие режимов работы автоматических кассовых аппаратов?
11. Чем вызвана необходимость использования разделяемых сетей автоматических кассовых аппаратов?
12. Каково назначение POS-терминалов?
13. Выполнение каких требований необходимо для защиты POS-систем?
14. В чем сущность технологии применения электронных чеков?
15. В чем заключается специфика видеоконтроля кассовых операций?
16. В чем заключается специфика видеоконтроля АТМ-терминалов?
17. Какие существуют варианты подключения систем видеоконтроля к оконечному банковскому оборудованию, и в чем их преимущества?
18. Какие достоинства системы видеоконтроля «POS-Интеллект»?
19. Какие достоинства системы видеоконтроля «АТМ-Интеллект»?

7. ЗАЩИЩЕННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

7.1. Система SWIFT

Сообщество SWIFT было организовано в 1973 г., и в 1977 г. начали осуществляться первые операции с использованием сетей связи. Члены сообщества находятся в Южной, Центральной и Северной Америке, Европе, Африке, Австралии и на Дальнем Востоке. На сегодняшний день оно объединяет 3200 пользователей из 84 стран мира [6].

Система SWIFT предлагает пользователям следующие преимущества:

– повышение эффективности работы банков за счет стандартизации и современных способов передачи информации, способствующих развитию автоматизации и рационализации банковских процессов;

– надежный обмен платежными сообщениями;

– сокращение операционных расходов по сравнению с телексной связью;

– удобный прямой доступ пользователей SWIFT к своим корреспондентам по всему миру (доставка сообщения с обычным приоритетом в любую точку мира – 20 мин, доставка срочного сообщения – 5 мин);

– использование стандартизованных сообщений SWIFT, позволяющее преодолеть языковые барьеры и свести к минимуму различия в практике осуществления банковских операций;

– повышение конкурентоспособности банков–членов SWIFT за счет того, что международный и кредитный обороты все более концентрируются на пользователях SWIFT.

Стоимость передачи сообщений членами сообщества определяется по единому тарифу и зависит от количества соединений, адреса, объема сообщения. За счет высокой интенсивности трафика (более 1 млн сообщений в день) стоимость передачи одного сообщения оказывается ниже, чем в других средствах связи (телекс, телеграф). Дополнительно к основной функции (обмену со-

общениями) система SWIFT также выполняет роль форума для выработки соглашения о стандартах представления и передачи данных.

Существует две системы SWIFT: SWIFT I (введена в строй в 1977 г.) и SWIFT II (внедряется с 1990 г.). Хотя по архитектуре эти системы различны, на практике пользователь не отличает сообщений, полученных по SWIFT I или SWIFT II. Рассмотрим архитектуру и защиту системы SWIFT II.

Архитектура системы SWIFT II

В архитектуре SWIFT можно выделить четыре основных уровня иерархии (рис. 7.1):

Рис. 7.1. Архитектура системы SWIFT II

– банковский терминал, который устанавливается в банке и предназначен для доступа персонала банка в сеть. Терминалами системы SWIFT обычно являются персональные компьютеры. Смонтированное оборудование может сдаваться «под ключ» (на базе мини-ЭВМ компаний Unisys и NCR) или интегрироваться в существующую банковскую систему (например на базе семейства мини-ЭВМ VAX компании DEC);

– региональный процессор (РП), основным назначением которого является организация взаимодействия пользователей некоторой ограниченной области (республики, страны, группы стран). Места расположения РП заранее не оп-

ределяются. Как правило, РП оснащаются сдублированными ЭВМ фирмы Unisys (Unisys A Series);

– слайс-процессор (СП), необходимый для обмена сообщениями между подключенными к нему РП, краткосрочного или длительного архивирования сообщений и генерации системных отчетов. Система SWIFT может сохранять передаваемые сообщения до 14 дней.

Это помогает избегать проблем, связанных с трактовкой текстов сообщений. На сегодняшний день существует два СП, каждый из них которых оснащен тремя машинами A12 фирмы Unisys, одна из которой является резервной. Один СП может может обработать до 1,5 млн сообщений в день. Допускается включение в сеть дополнительных СП; процессора управления системой (ПУС), выполняющего функции монитора системы, управления системой и сетью. Существует два ПУС, один из которых находится в Голландии, а второй – в США. Каждый ПУС может контролировать состояние и управлять работой СП и РП, работой сетевых программ и оборудования, подключением пользователей и их рабочими сеансами, включая выбираемые пользователем прикладные задачи. ПУС – единственный уровень системы, который не занят обработкой сообщений, а предназначен исключительно для управления системой SWIFT в целом.

На рис. 7.2 показаны пути передачи сообщений и платежей в наиболее общем случае.

Сообщения системы SWIFT содержат поля, идентифицирующие всех участников передачи информации и платежей.

Банк заказчика операции информирует банк-отправитель о необходимости послать сообщение и переводит ему соответствующую сумму. Банк получателя при приеме сообщения переводит эту сумму на счет расчетного банка, который осуществляет платежи.

Расчеты между банком-отправителем и банком-получателем осуществляются с помощью счета, который открывается в одном из них для другого. Кто

для кого открывает счет, зависит от типа валюты, в которой производятся расчеты. Если платежи осуществляются в валюте государства, в котором находится банк-получатель, то он вносит соответствующую сумму в дебет счета банка-отправителя в своем банке. Наоборот, если платежи осуществляются в валюте государства, в котором находится банк-отправитель, то он открывает у себя счет банка получателя и предоставляет ему кредит на соответствующую сумму.

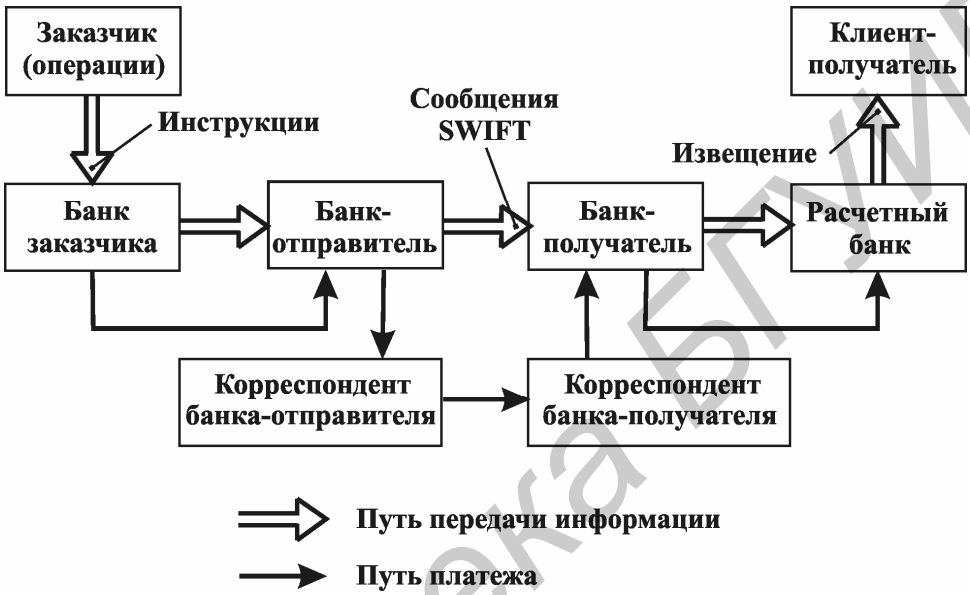


Рис. 7.2. Процесс передачи сообщений и осуществления платежей

В некоторых случаях платежи проходят более длинный путь, чем сообщения – через банки-корреспонденты, что зависит от конкретных условий платежей. Уведомление банков корреспондентов о платежах осуществляется специальными сообщениями. Если в организации связи участвуют четыре банка-посредника, то в сообщении идентифицируются банк заказчика, расчетный банк и корреспонденты отправителя и получателя. При этом идентификаторы отправителя и получателя в тексте сообщения не указываются, так как они находятся в его заголовке.

Обеспечение безопасности системы SWIFT

Безопасность в системе SWIFT обеспечивается применением организационных, программных и технических мер.

В системе SWIFT существует строгое разделение ответственности за поддержание безопасности системы: банк, подключенный к системе, отвечает за правильную эксплуатацию и физическую защиту терминалов, модемов и линий связи; региональный процессор – за правильное оформление сообщения при передаче его в сеть и наличие работоспособных терминалов. Всю остальную ответственность за передачу сообщений несет администрация системы. Управление защитой осуществляется управлением главного инспектора. Контроль защищенности системы осуществляется через случайные промежутки времени, чтобы убедиться, что все требования безопасности поддерживаются на должном уровне.

Защита банковских терминалов предусматривает разграничение доступа пользователей к нему по паролю и специальной пластиковой карточке. При входе пользователя в систему производится взаимное опознавание терминала и системы. Автоматическое отключение от SWIFT происходит в следующих случаях:

– при обнаружении помех или обрыве соединения;

– при неоднократном обнаружении ошибки при передаче данных или в принятом сообщении;

– при сбое РП, к которому подсоединены терминалы.

Сведения о подключении и отключении терминала регистрируются в специальном журнале.

Для обеспечения конфиденциальности передаваемых сообщений используется шифрование при помощи специальных устройств (STEN), устанавливаемых в тракте передачи «банковский терминал – региональный процессор». Для шифрования информации используются три типа ключей: главный (64 бита), вторичный (128 бит) и шифрования данных (64 бита). Главный и вторичный ключи устанавливаются представителями SWIFT. Ключ шифрования данных генерируется специальным шумовым источником в процессе работы. Смена модулей, содержащих первичный и вторичный ключи, осуществляется периодически по указанию Главного инспектора системы. Банкам предоставляет-

ся возможность устанавливать собственные устройства шифрования для защиты линии связи (естественно, после консультаций с представителями SWIFT). Обеспечение конфиденциальности сообщений не является самой главной задачей системы, хотя ей также уделяется серьезное внимание.

Для аутентификации пользователей и обеспечения целостности сообщений в системе SWIFT существует оригинальный алгоритм аутентификации, детали которого держатся в секрете. Как и для любого такого алгоритма, базовыми требованиями являются надежное распределение ключей между двумя абонентами и защита их от остальных. Тщательная аутентификация достигается за счет четкого распределения ответственности. Ключи рассылаются банкам попарно, другие банки и персонал сети доступа к ним не имеют; рассылается также руководство по управлению ключами: процедура и время замены ключей и т. д. Кроме того, SWIFT может использоваться для обмена конфиденциальной информацией между сообществом банков, однако в этом случае ответственность за обеспечение безопасности ложится на участников обмена.

В то же время аутентификации взаимодействующих организаций недостаточно для надежной работы сети, так как она не предполагает защиты от подмены, уничтожения или задержки сообщений.

Для обеспечения целостности потока передаваемых сообщений применяется механизм номеров сообщений. Соединения между SWIFT и пользователями поддерживаются двумя (входной и выходной) последовательностями номеров. Входная последовательность обрабатывается слайс-процессорами системы, выходная – получателями сообщений. Такой механизм обеспечивает полный контроль за последовательностью переданных и полученных сообщений для любой пары оконечных пользователей. Он удостоверяет, что ни одно сообщение не уничтожено и не продублировано.

Еще одна задача защиты – предотвращение передачи ложных сообщений, не искажающих последовательности номеров и имеющих истинную аутентификацию. Эта задача решается банками – оконечными пользователями систе-

мы. Именно они ответственны за корректность переданных от их имени сообщений. Кроме того, на пунктах обработки и передачи сообщений также существуют механизмы защиты от подделки сообщений.

Для центральной части SWIFT, состоящей из слайс-процессоров, региональных процессоров и линий связи, защита сообщений является задачей администрации системы. Доступ к системе, программное обеспечение и сообщения пользователей строго контролируются, как и доступ на территорию машинных залов. Международные линии связи, соединяющие слайс-процессоры между собой, слайс-процессоры и региональные процессоры, имеют надежную криптозащиту. Персонал системы SWIFT не имеет доступа к содержимому пересылаемых сообщений.

7.2. Система CHAPS

Клиринговая система CHAPS осуществляет поддержку электронных платежей между небольшой группой банков Лондона, большинство из которых представляют собой отделения иностранных банков, использующих Лондон в качестве расчетного центра. Системой используется концепция расчетов «same-day» (в тот же день) с помощью счетов этих банков в Bank of England. Помимо CHAPS, все банки могут работать с любой другой доступной сетью по своему усмотрению [3].

Архитектура системы CHAPS

В отличие от SWIFT система CHAPS (рис. 7.3) не имеет своих операционных центров, а использует общую сеть коммутации пакетов (Packet Switch Stream – PSS). Высокая доступность системы обеспечивается шлюзами, которые реализованы на компьютерах Tandem, рассчитанных на непрерывную работу.

Система CHAPS предоставляет своим пользователям полный комплекс услуг, обеспечивающий надежное обращение электронных денег.

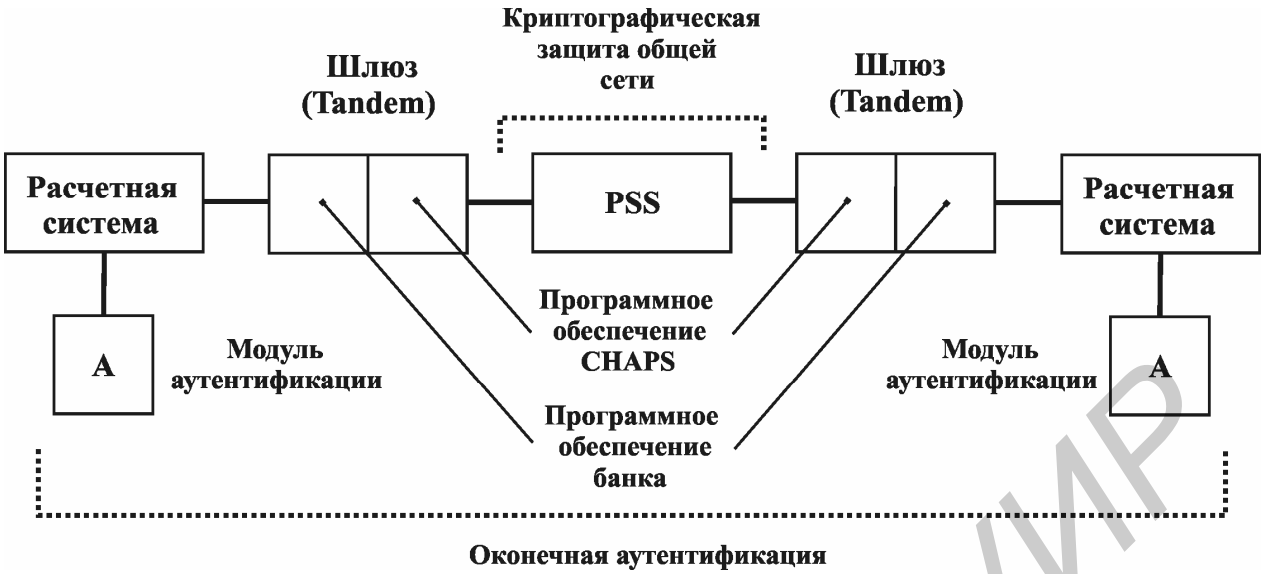


Рис. 7.3. Архитектура системы CHAPS

Обеспечение безопасности системы CHAPS

Основное внимание в защите CHAPS уделено аутентификации абонентов системы и поддержанию конфиденциальности передаваемых сообщений.

Аутентификация абонентов в системе CHAPS осуществляется с помощью алгоритма DES в режиме сцепления блоков. Шифрование реализовано аппаратно в защищенном от физического воздействия модуле, в котором также хранятся ключи шифрования.

Управление ключами отражает специфику системы CHAPS, которая должна обеспечить конфиденциальность соединения между двумя любыми банками, входящими в ее состав. Существует два ключа шифрования: главный и сеансовый. Главный ключ предназначен для шифрования сеансового ключа. Сеансовый ключ передается по линии связи между взаимодействующими банками.

Безопасность осуществления платежей в системе CHAPS достигается за счет аутентификации сообщений в точке посылки и их верификации (проверки) в точке приема. Эти функции выполняются участниками расчета.

Для контроля целостности потока сообщений применяется нумерация передаваемых пакетов. Каждому пакету соответствует некоторый номер (authentication

sequence number, ASN). Для каждой пары отправитель – получатель нумерация пакетов уникальна. Последовательности номеров различны для платежных и неплатежных сообщений. Последовательность номеров должна быть инициализирована в момент смены сеансового ключа для определенной пары отправитель – получатель. Сама аутентификация и ее проверка осуществляются внутри модуля защиты от подделки CHAPS (CHAPS tamper resistant module; TRM).

Вопросы для самоконтроля

1. Какие преимущества имеет система SWIFT по сравнению с аналогичными системами?

2. В чем сущность иерархического построения системы SWFIT?

3. Какие методы и средства защиты используются для обеспечения безопасности в системе SWIFT?

4. Каково назначение системы CHAPS?

5. Чему уделяется особое внимание при обеспечении безопасности системы CHAPS?

8. БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ В ИНТЕРНЕТ

8.1. Классификация типов мошенничества в Интернет-коммерции

Высокий уровень мошенничества в Интернет является сдерживающим фактором развития электронной коммерции (ЭК), поскольку покупатели, торговля и банки боятся пользоваться этой технологией из-за опасности понести финансовые потери [7].

Приведем классификацию возможных типов мошенничества через Интернет согласно с 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;

– создание магазинов, возникающих, 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;

– создание магазинов и торговых агентов (Acquiring Agent), чьей целью является сбор информации о реквизитах карт и других персональных данных покупателей.

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.

8.2. Протокол SSL

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 (OSI). Это, с одной стороны, означает возможность использования протокола для организации защищенной сессии между программами, работающими по различным протоколам прикладного уровня OSI (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 особенный 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 (рассмотрим 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 байт;

– набор поддерживаемых клиентом симметричных криптографических и хэш-алгоритмов, используемых при формировании кода для проверки целостности передаваемого сообщения (MAC – Message Authentication Code);

- набор поддерживаемых алгоритмов сжатия (все реализации протокола SSL должны поддерживать метод Compression Method null).

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, 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 про-

верки 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 RAND_CL 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 Pre_MasterSecret, посланную КЛИЕНТУ на предыдущем шаге случайную последовательность RAND_SERV и полученную от него случайную последовательность RAND_CL;

– используя MasterSecret, вычисляет криптографические параметры SSL-сессии: формирует общие с клиентом сеансовые секретные ключи одноключевого алгоритма шифрования и секрет для вычисления MAC;

– переходит в режим защищенного взаимодействия.

Поскольку при формировании параметров SSL-сессии КЛИЕНТ и СЕРВЕР пользовались одними и теми же исходными данными (согласованны-

ми 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.

5. 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 и посылок, полученных от СЕРВЕРА на этапе 1, 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, посылок, полученных от КЛИЕНТА на этапе 1, 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.

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 OSI, 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.

Достоинства протокола:

1. Широкое распространение протокола SSL, которое 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;

2. Простота протокола для понимания всех участников ЭК;

3. Хорошие операционные показатели (скорость реализации транзакции). Последнее достоинство связано с тем, что протокол в процессе передачи данных использует только симметричные протоколы шифрования.

Недостатками протокола SSL в приложении к ЭК являются:

1. Отсутствие аутентификации клиента интернет-магазином, поскольку сертификаты клиента в протоколе 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.

2. Протокол SSL не позволяет аутентифицировать клиента обслуживающим банком.

3. При использовании протокола SSL торговое предприятие (ТП) аутентифицируется только по своему адресу в Интернете (URL). Это значит, что клиент, совершающий транзакцию ЭК, не аутентифицирует ТП в полном смысле. 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 на основании только своих учредительных документов.

4. Протокол SSL не поддерживает цифровой подписи, что затрудняет процесс разрешения конфликтных ситуаций, возникающих в работе платежной системы (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 затратно с точки зрения ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение клиентом товара.

5. При использовании SSL не обеспечивается конфиденциальность данных о реквизитах карты для ТП.

8.3. Протокол SET

Для операций с кредитными карточками используется протокол SET (Secure Electronic Transactions), разработанный совместно компаниями Visa, MasterCard, Netscape и Microsoft.

В отличие от SSL протокол SET узко специализирован. Целью SET является обеспечение необходимого уровня безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция реализуется через Интернет.

На базовом уровне SET осуществляет следующие функции:

Аутентификация. Все участники кредитных операций идентифицируются с помощью электронных подписей. Это касается клиента-покупателя, продавца, банка, выдавшего кредитную карточку, и банка-продавца.

Конфиденциальность. Все операции производятся в зашифрованном виде.

Целостность сообщений. Информация не может быть подвергнута модификации по дороге, в противном случае это будет сразу известно.

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

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

На более высоком уровне протокол SET поддерживает все возможности, предоставляемые современными кредитными карточками:

– регистрацию держателя карточки;

– регистрацию продавца;

– запрос покупки;

– авторизацию платежа;

– перевод денег;

– кредитные операции;

– возврат денег;

– отмену кредита;

– дебитные операции.

Окончательная версия протокола SET была выпущена в мае 1997 г. Протокол работает с четырьмя субъектами: владельцем кредитной карты, банком-эмитентом, эту карту выпустившим, продавцом и банком-эквайером, где помещен счет продавца. Помимо этих функциональных субъектов в процессе обычно (опционно) участвуют центры сертификации, в задачу которых входит подтверждение подлинности предъявляемых параметров аутентификации, причем в случае крупных сделок с этими центрами должны взаимодействовать все участники. Основной целью сертификатов является подтверждение того, что присланный общедоступный ключ прибыл от настоящего отправителя.

Схема взаимодействия субъектов при использовании протокола SET показана на рис. 8.1 (взаимодействия с центром сертификации не показаны).

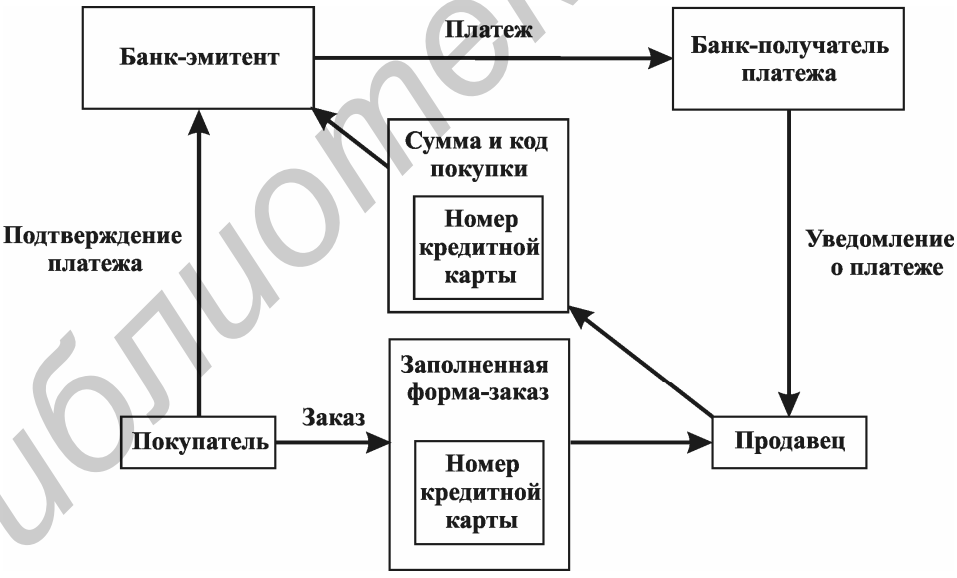


Рис. 8.1. Схема взаимодействия субъектов при использовании протокола SET

Протокол SET помогает реализовать следующие процедуры.

1. Покупатель инициализирует покупку. При этом покупатель выбирает продавца, просматривает его web-сайт, принимает решение о покупке, заполняет бланк заказа. Все это делается до вступления в дело протокола SET. Взаимо-

действие участников сделки регламентируется протоколом IOTP. SET начинает свою работу, когда покупатель нажимает клавишу оплаты. При этом сервер посылает ЭВМ покупателя сообщение, которое и запускает соответствующую программу. Процедура эта может быть реализована с помощью PHP- или CGI-скрипта, или JAVA-аплета.

2. Программа клиента посылает заказ и информацию об оплате. Для этого формируется два сообщения, одно содержит данные о полной стоимости покупки и номере заказа, второе – номер кредитной карточки покупателя и банковскую информацию. Сообщение о заказе шифруется с использованием симметричного метода (например DES) и вкладывается в цифровой конверт, где используется общедоступный ключ продавца. Сообщение об оплате шифруется с привлечением общедоступного ключа банка (эмитента кредитной карты). В результате продавец не получает доступа к номеру кредитной карточки покупателя. Программа генерирует хэш-дайджест (SHA1) обоих сообщений с использованием секретного ключа покупателя. Это позволяет продавцу и банку проконтролировать целостность сообщения, но препятствует прочтению части, ему не предназначенной (например номера кредитной карты продавцом).

3. Продавец выделяет часть, адресованную банку, и направляет ее по месту назначения. Программа SET web-сервера продавца генерирует запрос авторизации серверу банка, где находится счет продавца. При формировании запроса авторизации используется электронная подпись продавца, базирующаяся на его секретном ключе, что позволяет однозначно его идентифицировать. Этот запрос шифруется с помощью ключа сессии и вкладывается в цифровой конверт, где используется общедоступный ключ банка.

4. Банк проверяет действительность кредитной карточки, расшифровывает запрос авторизации продавца и идентифицирует продавца. После этого осуществляется проверка авторизации покупателя. При этом посылается запрос авторизации, снабженный электронной подписью, банку, выпустившему кредитную карточку.

5. Банк, выпустивший карточку, выполняет авторизацию и подписывает чек, если кредитная карточка покупателя в порядке. Отклик, снабженный соответствующей подписью, посылается банку продавца.

6. Банк продавца авторизует данную операцию и посылает подтверждение, подписанное электронным образом, web-серверу продавца.

7. WEB-сервер продавца завершает операцию, выдавая клиенту подтверждение на экран, и заносит результат операции в соответствующую базу данных.

8. Продавец осуществляет подтверждение выполнения операции своему банку. Деньги покупателя переводятся на счет продавца.

9. Банк, выпустивший карточку, посылает счет покупателю, и SET уведомляет покупателя об изменениях на его счету (раз в месяц).

Итак, каждый шаг реализации протокола SET сопровождается аутентификацией. Это препятствует какому-то внешнему субъекту стать посредником и видоизменять сообщения. Для нормальной работы протокола SET все участники должны зарегистрироваться и снабдить партнеров своим общедоступным ключом.

8.4. Сравнительная характеристика протоколов SSL и SET

В табл. 8.1 приведены результаты сравнения протоколов SET и SSL по отношению к наиболее вероятным типам мошенничества в ЭК.

Таблица 8.1

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

Из табл. 8.1 следует, что 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. Проведенные исследования показали, что время, затрачиваемое компьютером покупателя на криптографические операции при использовании SSL, на порядок меньше аналогичной величины при применении протокола SET.

Несмотря на убедительные преимущества протокола SET, его внедрение связано с возникновением различного рода 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 SET Co 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.

К другой проблеме 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 инвестировать средства в новое решение. Это хорошо видно на примере Дании, являющейся одним из лидеров по внедрению протокола SET, компании которой при заключении договоров на обслуживание предлагают интернет-магазинам обе технологии – SSL и SET. Количество заключенных договоров на работу по технологии SSL в 10 раз больше, чем по стандарту SET.

Кроме того, отсутствие инфраструктуры интернет-магазинов, использующих стандарт SET, сдерживает банки-эмитенты от инвестиций в SET.

Таким образом, на сегодняшний день большинство платежных интернет-систем используют протокол SSL и различного рода технологические решения для уменьшения уровня мошенничеств при проведении транзакций.

Вопросы для самоконтроля

1. Какие типы мошенничества существуют в интернет-коммерции?
2. Каково назначение протокола SSL?
3. Какие режимы аутентификации поддерживает протокол SSL?
4. Каким образом вырабатываются сеансовые ключи шифрования при использовании протокола SSL?
5. Какие функции выполняет протокол SET на базовом уровне?
6. Какие достоинства и недостатки протокола SSL?
7. Какие достоинства и недостатки протокола SET?

ЛИТЕРАТУРА

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

2. Петренко, С. А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М. : Компания АйТи, 2006. – 400 с.

3. Гайкович, В. Безопасность электронных банковских систем / В. Гайкович, А. Першин. – М. : Единая Европа, 1994. – 360 с.

4. Гинзбург, А. И. Пластиковые карты / А. И. Гинзбург. – СПб. : Питер, 2004. – 128 с.

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

6. Международная телекоммуникационная система SWIFT: учеб. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2002. – 56 с.

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

Св. план 2008, поз. 93

Учебное издание

Лыньков Леонид Михайлович
Борботько Тимофей Валентинович
Мухуров Николай Иванович и др.

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

Учебно-методическое пособие

Редактор *Т. П. Андрейченко*
Компьютерная верстка и дизайн обложки *Е. Г. Бабичева*

Подписано в печать 30.06.2009. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Печать ризографическая. Усл. печ. л. 11,63. Уч.-изд. л. 11,0. Тираж 100 экз. Заказ 396.

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