А. Б. Вавренюк, В. В. Макаров, И. В. Чугунков, В. С. Трофимова

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ НА ОСНОВЕ ЦИФРОВЫХ ДЕНЕГ

Введение

Электронная коммерция (ЭК) — это разновидность коммерческой деятельности, в которой взаимодействие между ее участниками на всех или некоторых ее этапах осуществляется электронным способом. Иначе говоря, электронная коммерция предполагает взаимодействие между партнерами с использованием информационных технологий (в первую очередь сетевых), что существенно повышает гибкость, эффективность и масштабность бизнес-процессов. ЭК — одна из двух базовых составляющих электронного бизнеса. Электронный бизнес — совокупность технологии поддержания внешних бизнес-контактов (электронной коммерции) и комплексной автоматизации внутренней деятельности компании.

Развитие систем электронного бизнеса невозможно без решения следующих задач защиты информации:

- аутентификация участников информационного взаимодействия;
- обеспечение конфиденциальности и целостности коммерческой информации (документов, удостоверяющих факт сделки, платежных документов, счетов, заказов и пр.) при ее передаче по каналам связи;
- обеспечение невозможности отказа от факта получения какого-либо сообщения;
- обеспечение юридической значимости пересылаемых электронных документов.

Решение указанных задач, в свою очередь, невозможно без применения стохастических методов [1].

Электронная платежная система — аналог традиционной платежной системы, обеспечивающий денежные расчеты между поставщиками и потребителями в электронном виде (без шелеста купюр, рукописных подписей и пр.).

Участники электронной платежной системы:

- банки, объединенные договорными обязательствами;
- предприятия торговли и сервиса, образующие сеть точек обслуживания клиентов;
- процессинговые центры;
- держатели платежных средств.

Кроме перечисленных выше задач ОБИ, которые решаются традиционными методами, существуют также задачи, актуальные именно при построении электронных платежных систем. В первую очередь речь идет об анонимности и неотслеживаемости электронных платежей.

При осуществлении оплаты за товар необходимо обеспечить конфиденциальность платежных данных потребителя, платежная информация (номер пластиковой карточки, номер счета и т. п.) должна быть известна только тому, кто имеет законное право ее знать, например банку-эмитенту платежного средства. Безопасная транзакция требует, чтобы поставщик не знал платежные данные потребителя.

Проблема конфиденциальности тесно связана с проблемой анонимности потребителя при осуществлении коммерческой транзакции. Анонимность потребителя включает в себя анонимность платежа и анонимность взаимодействия. Анонимность платежа предполагает отсутствие взаимосвязи между платежом и личностью инициирующего его потребителя. Неотслеживаемость платежей означает, что два платежа, совершенные одним и тем же потребителем, не могут быть соотнесены друг с другом ни при каких условиях.

1. Цифровые деньги

Уже достаточно давно банки и другие коммерческие структуры используют при проведении деловых операций электронный обмен данными EDI (Electronic Data Interchange) и электронный перевод денежных средств EFT (Electronic Funds Transfer). В современных платежных системах весь процесс от начала до конца происходит в электронной (цифровой) форме. При этом для обеспечения безопасности и признания законности (конфиденциальности пересылаемых электронных документов, аутентификации участников информационного обмена) повсеместно используются криптосистемы с открытым ключом для шифрования и формирования электронной подписи.

Учитывая, что традиционные денежные купюры есть не что иное, как защищенный от подделки документ, логичным представляется переход к использованию *цифровых денег*. Защиту от подделки при этом может обеспечить электронная подпись банка, которая, очевидно, имеет большую надежность, чем традиционные водяные знаки, металлические полосы и т. п.

Когда владелец кредитной карточки с ее помощью делает покупки, оплачивает налоги и т. д., где-то в базе данных всегда делается отметка об этом событии. Соединив вместе эти в отдельности малозначимые данные, можно собрать большое количество информации о конкретном человеке. При этом последний не в состоянии выяснить, кому и что известно о его частной жизни; не в состоянии управлять точностью этой информации или определять, кто может ее получать. Необходимо реализовать такую систему доступа к ресурсам и услугам, в которой одновременно с решением задач идентификации, аутентификации и авторизации претендента решена задача обеспечения *анонимности* последнего. Обычные бумажные деньги обеспечивают все эти свойства. Если запрашиваемым ресурсом является какой-либо товар, то наличие у покупателя достаточного количества купюр служит доказательством его права на доступ к ресурсу. Хотя каждая из купюр имеет уникальный номер, отслеживать купюры по номерам практически невозможно. Итак, проблема состоит в том, чтобы сделать электронные платежи в такой же степени анонимными, как и расчет с помощью обычных денег. Иначе говоря, возникает задача обеспечения *неотслеживаемости* электронных документов, и в частности цифровых денег.

«Отцом» цифровых денег с полным основанием можно назвать Д. Чаума, основателя и исполнительного директора фирмы DigiCash и одновременно признанного специалиста в области криптографии. DigiCash разработала и запатентовала криптографическую технологию безопасных электронных платежей.

Выглядит цифровая купюра приблизительно так, как показано на рис. 1. Документ содержит номинал и номер купюры, а также подпись банка-эмитента, которая получена на его секретном ключе. При этом *электронная подпись надежно защищает купюру от подделки, но совершенно не защищает от копирования*. Чтобы избежать превращения цифровой купюры в «неразменный пятак» (см. Стругацкий А. Н., Стругацкий Б. Н. Понедельник начинается в субботу), банк-эмитент должен контролировать каждую сделку.

Рис. 1. Цифровая купюра

Рассмотрим возможную процедуру осуществления платежей с использованием цифровых денег (рис. 2).

Клиент А (будущий покупатель), желающий получить определенную сумму цифровых денег, посылает в банк-эмитент, в котором у него имеется счет, «полуфабрикат» цифровой купюры, имеющий вид, аналогичный показанному на рис. 1. Только подписан этот документ самим клиентом А. Так как А является клиентом банка, там знают его открытый ключ, а значит, могут проверить подпись. Убедившись, что именно А заказал цифровые деньги, банк удаляет его подпись, ставит свою, вычитает со счета А сумму, равную номиналу купюры, и отсылает последнюю А.

Получив электронную купюру, А может потратить ее сам, переслав (или передав) ее в обмен на товар продавцу B_1 в магазине, принимающем цифровые деньги, либо переслать (или передать) ее другому человеку B_2. Чтобы осуществить процесс передачи цифровой купюры, участники обмена А и В, а также банк-эмитент С должны одновременно находиться на связи. Перед передачей купюры В участник А подписывает ее своим секретным ключом. Получив купюру, В проверяет подпись, а затем, убедившись в ее подлинности, удаляет ее и ставит свою, после чего отправляет в банк-эмитент. Банк проверяет, не получал ли он уже эту банкноту (защита от копирования!), т. е. ищет ее номер в специальном списке купюр, предъявленных к оплате ранее. Если банкнотой никто раньше не пользовался, ее номер заносят в список использованных купюр (второй раз ее к оплате не примут!) и переводят сумму, равную номиналу цифровой купюры, на счет своего клиента В.

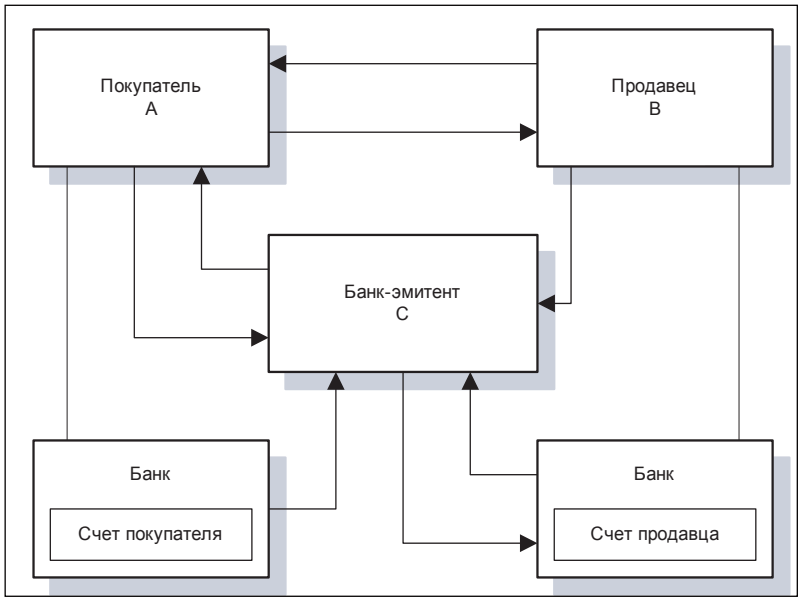

Рис. 2. Схема расчета цифровыми деньгами

Покупатель перечисляет деньги в банк-эмитент либо напрямую, либо через банк — участник системы. Взамен покупатель получает цифровые деньги. Получив их при оплате товара, продавец, проверив их подлинность, отдает товар, перечисляет цифровые деньги банку-эмитенту, а тот переводит обычные денежные средства на счет продавца.

Рассмотренная схема пока не обеспечивает неотслеживаемости электронных платежных средств, так как позволяет проследить за движением денег от А к В. Когда клиент А присылает заявку на цифровую купюру достоинством допустим 100 у.е., банк узнает номер купюры. В результате, когда эту купюру предъявляет к оплате клиент В, банк узнает, что А заплатил В 100 у.е. Таким образом, данная схема не обеспечивает анонимность платежей, банк в состоянии составить полное досье на любого своего клиента: кто, сколько и кому платил, сколько и от кого получал.

Для того чтобы сделать электронную купюру эквивалентной обычной бумажной того же номинала, Д. Чаум предложил *протокол слепой подписи* (blind signature). Заказывая цифровую купюру, клиент А создает «полуфабрикат» купюры, в которой указывает номинал и серийный номер купюры. Затем «затемняет» номер и посылает «полуфабрикат» купюры банку. Банк подписывает его и возвращает А. Получив подписанный банком «полуфабрикат», А снимает «затемнение» и получает полноценную купюру, формат которой соответствует показанному на рис. 1. Если впоследствии эта купюра будет предъявлена банку, банк будет вынужден принять ее, так как на ней стоит его подпись. Банк, так же как и раньше, заносит ее номер в список купюр, предъявленных к оплате, но у него нет возможности узнать, от кого получена эта купюра. Когда банк ее подписывал, он не мог видеть ее номер.

Рассмотренная система платежей, требующая участия банка во всех транзакциях, называется *централизованной*. В отличие от нее *автономная система платежей* предполагает, что продавец В сам, без обращения к банку С, проверяет подлинность предъявленной покупателем А электронной наличности. Понятно, что в этом случае банк идет на определенный риск, так как используемые схемы обеспечивают обнаружение злоупотреблений со стороны А постфактум. Основная идея соответствующих протоколов — однозначно идентифицировать нарушителя.

2. Защита информации в ЭПС на основе цифровых денег

Цифровые деньги (цифровая наличность) — это защищенное от подделки электронное платежное средство. Более того, это единственное платежное средство, обеспечивающее анонимность и неотслеживаемость платежей. Ни одно из множества других электронных платежных средств (платежные карты, электронные чеки и пр.) такими свойствами не обладает.

Проблемы информационной безопасности, которые необходимо решить:

- как защититься от кражи купюры (задача защиты прав собственника информации);
- как защититься от повторного использования купюры, учитывая, что электронный документ и ЭЦП можно копировать сколь угодно много раз;
- как защититься от подделки номинала цифровой купюры, учитывая, что ЭЦП банка-эмитента ставится только на номере купюры;
- как обеспечить анонимность и неотслеживаемость платежей, иначе говоря, как получить полный электронный аналог бумажных денег, обладающих такими свойствами.

В таблице 1 приведены методы решения, из таблицы видно, что три из четырех задач решаются стохастическими методами.

Таблица 1. Методы защиты

Задача	Механизм решения	Участник платежной системы, обеспечивающий решение
Защита прав владельца цифровой купюры	Стохастический метод решения — хеширование случайного прекурсора для получения номера цифровой купюры	Будущий владелец купюры
Защита от повторного использования цифровой купюры	Поддержание списка номеров ранее использованных цифровых купюр и его анализ при авторизации	Банк

Защита от подделки номинала цифровой купюры	Стохастический метод решения — использование для каждого возможного номинала своей пары ключей формирования и проверки ЭЦП	Банк-эмитент
Обеспечение анонимности и неотслеживаемости платежей	Стохастический метод решения — схема слепой электронной подписи	Будущий владелец купюры, банк-эмитент

3. Слепая электронная подпись

Целями абонента А, инициатора протокола, являются, во-первых, формирование серийного номера S цифровой купюры, во-вторых, получение цифровой подписи абонента С (банка) на документе, в качестве которого в рассматриваемой ситуации выступает S, таким образом, чтобы абонент С не узнал содержимого документа. Пусть $N = \rho q$, , где p и q — два больших различных простых числа; e — открытый ключ (ключ проверки подписи), а d — закрытый ключ (ключ формирования подписи) абонента С, при этом

$ed \equiv 1 \ mod[\rho-1)(q-1)]$.

В результате для любого положительного $x < N$ справедливо $x^{ed} \ modN=x$. Пусть $H(x)$ — общеизвестная хеш-функция.

Схема слепой электронной подписи

1) Абонент А формирует случайное число S', называемое прекурсором (precursor). Хешируя прекурсор, А формирует серийный номер купюры $S = H(S')$. Такая последовательность формирования S необходима для защиты прав владельца будущей купюры, так как только он в силу свойств функции $H(x)$ в случае возникновения споров может предъявить арбитру прекурсор, на основе которого сформирован серийный номер.

2) Абонент А формирует случайное число R — затемняющий множитель, единственное требование к которому — существование обратного $R^{-1} \bmod N$. Затем А шифрует затемняющий множитель на открытом ключе абонента С, умножает результат на S и посылает получившееся сообщение

$$y_A = S \times R^e \bmod N$$

абоненту С.

3) Абонент С, получив сообщение y_A, подписывает его на своем секретном ключе и посылает сформированное сообщение

$$y_C = \left(S \times R^e \bmod N\right)^d \bmod N = S^d \times R^{ed} \bmod N = S^d \times R \bmod N$$

обратно абоненту А.

Абонент А снимает действие затемняющего множителя, вычисляя

$$y_c \times R^{-1} \bmod N = S^d \bmod N,$$

и получает в результате серийный номер, подписанный С, при этом абонент С ничего не узнал о содержимом подписанного им документа.

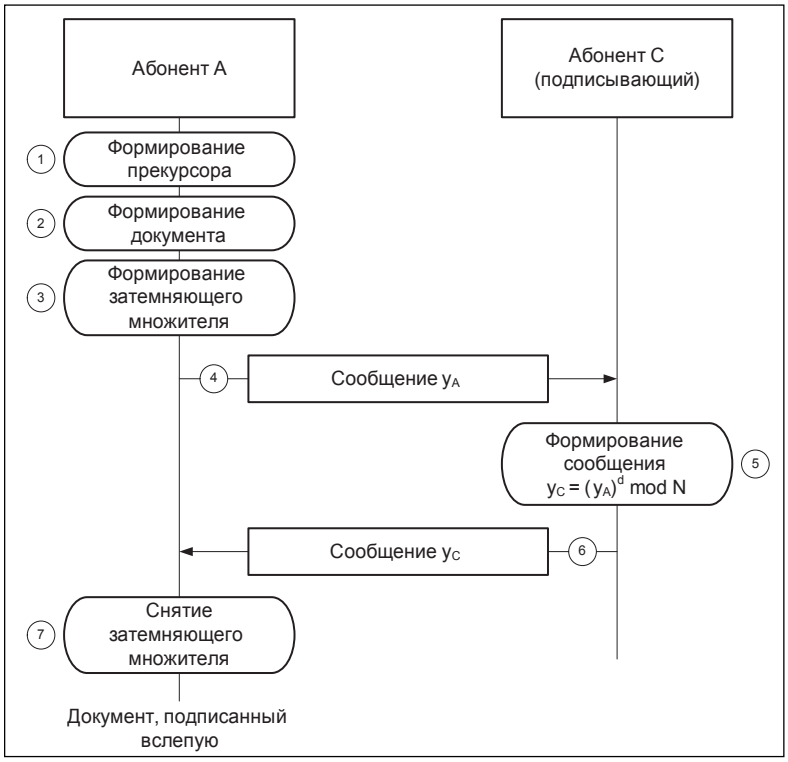

Рис. 3. Протокол слепой ЭЦП RSA

4. Структура централизованной платежной системы на основе цифровой наличности. Анализ жизненного цикла цифровой купюры

Рассмотрим централизованную (on-line) платежную систему на основе цифровой наличности [1]. Проанализируем жизненный цикл цифровой купюры на примере ситуации (рис. 4), когда покупатель (абонент А) и продавец (абонент В) являются клиентами некоего банка (абонент С). Этот же банк является эмитентом цифровой наличности.

Предположим, стоимость представлена 4-разрядным двоичным кодом. Пусть клиент хочет приобрести две цифровые купюры, каждая достоинством 15 условных единиц. Первая купюра имеет серийный номер S_1, вторая — S_2. Соответствующие затемняющие множители равны R_1 и R_2.

Банковская открытая экспонента для представления купюры максимального достоинства равна

$h = 11 \times 7 \times 5 \times 3$.

Рассмотрим случай, когда абонент A после получения цифровых купюр совершает две покупки — одну на сумму 10 у.е., а другую — на сумму 12 у.е.

Транзакция снятия со счета

Шаг 1. Абонент А с помощью генератора псевдослучайных чисел (ПСЧ) формирует два прекурсора S_1' и S_2', осуществляет их хеширование с целью получения номеров $S_1 = H(S_1)$ и $S_2 = H(S_2)$ двух цифровых купюр. Абонент В с помощью генератора ПСЧ формирует два затемняющих множителя R_1 и R_2.

Шаг 2. Абонент А формирует «полуфабрикаты» купюр, скрывая их номера с использованием затемняющих множителей, и посылает их в банк для простановки слепой подписи. Сообщение, посылаемое в банк, есть конкатенация двух запросов:

$(S_1 \times R_1^h) \bmod N \,\|\, (S_2 \times R_2^h) \bmod N$,

где $N = pq$, p и q — различные простые числа.

Шаг 3. Банк (абонент С) снимает со счета абонента А соответствующую сумму (30 у.е.), подписывает вслепую купюры и затем возвращает составное сообщение

$$\left(\left(\mathrm{S}_1 \times R_1^h\right)^{1/h}\right) \bmod N \,\|\, \left(\left(\mathrm{S}_2 \times R_2^h\right)^{1/h}\right) \bmod N =$$

$$= \left(S_1^{1/h} \times R_1\right) \bmod N \,\|\, \left(S_2^{1/h} \times R_2\right) \bmod N$$

Инверсия $1/h$ есть банковская секретная экспонента (секретный ключ SK_C), которая вычисляется по формуле

$h \times (1/h) = 1 \; mod \; [(\rho - 1)(q - 1)]$.

Эта экспонента, так же как и открытая, определяет общую стоимость купюры.

Шаг 4. Абонент А снимает действие затемняющих множителей и получает две полноценные цифровые купюры достоинством 15 у.е., подписанные банком-эмитентом, соответственно $S_1^{1/h} \bmod N$ и $S_2^{1/h} \bmod N$.

Транзакция покупки 1

Шаг 5. При выполнении платежа первой купюрой за товар (или услугу) стоимостью 10 единиц (двоичное представление 1010) абонент А использует экспоненту 7×3 в своем запросе. Он составляет сообщение для отправки абоненту В (продавцу) в следующем виде

$$S_1^{1/h(7\times3)} \bmod N = S_1^{1/(1\times5)} \bmod N .$$

Для получения «сдачи» абонент А становится неотслеживаемым кредитором для банка в соответствии с вышеописанным протоколом. Абоненту А необходимо удержать остаток в 5 условных единиц. Для этого он формирует число T (по сути вторую цифровую купюру) и скрывает его с помощью затемняющего множителя R_{A1}, зашифрованного с использованием экспоненты 7×3, соответствующей сумме в 5 условных единиц

$$\left(T \times R_{A1}^{(7\times3)}\right) \bmod N .$$

Покупатель (абонент А) хочет заплатить продавцу (абоненту В) 10 условных единиц. Для этого абонент А формирует составное сообщение

$$S_1^{1/(11\times5)} \bmod N \,\|\, \left(T \times R_{A1}^{(7\times3)}\right) \bmod N$$

и посылает его абоненту В.

Шаг 6. Абонент В пересылает это сообщение банку.

Шаг 7. Банк проверяет номер S_1, обращаясь к списку номеров ранее использованных купюр. В случае положительного результата сравнения на счет В переводится сумма в 10 у.е.

Шаг 8. Банк возвращает абоненту В купюру T, подписанную с использованием экспоненты $1/(7 \times 3)$

$$\left(T^{1/(7\times3)} \times R_{A1}\right) \bmod N .$$

Шаг 9. Абонент В пересылает это сообщение (по сути сдачу) абоненту А.

Шаг 10. Абонент А снимает действие затемняющего множителя и получает подписанную банком купюру достоинством 5 условных единиц

$$T^{1/(7\times3)} \bmod N .$$

Транзакция покупки 2

Шаг 11. Допустим, второй платеж осуществляется на сумму в 12 условных единиц (двоичное представление 1100), открытая экспонента в этом случае равна 11×7. Составное сообщение от А к В с использованием затемняющего множителя R_{A2} в этом случае будет иметь вид

$$S_2^{1/(11\times7)} \bmod N \,\|\, \left(T^{1/(7\times3)} \times R_{A2}^{(5\times3)}\right) \bmod N .$$

Шаг 12. Абонент В пересылает это сообщение банку.

Шаг 13. Банк проверяет номер S_2, обращаясь к списку номеров ранее использованных купюр. В случае положительного результата сравнения на счет В переводится сумма в 12 у.е.

Шаг 14. Банк возвращает абоненту B купюру T, подписанную с использованием экспоненты $1/(5 \times 3)$

$\left(T^{1/(7\times3)(5\times3)} \times R_{A2}\right) \bmod N$.

Шаг 15. Абонент B пересылает это сообщение абоненту A.

Шаг 16. Абонент A снимает действие затемняющего множителя и получает подписанную банком купюру с «накопленным» достоинством $(5 + 3)$ условных единиц

$T^{1/(7\times3)(5\times3)} \bmod N$.

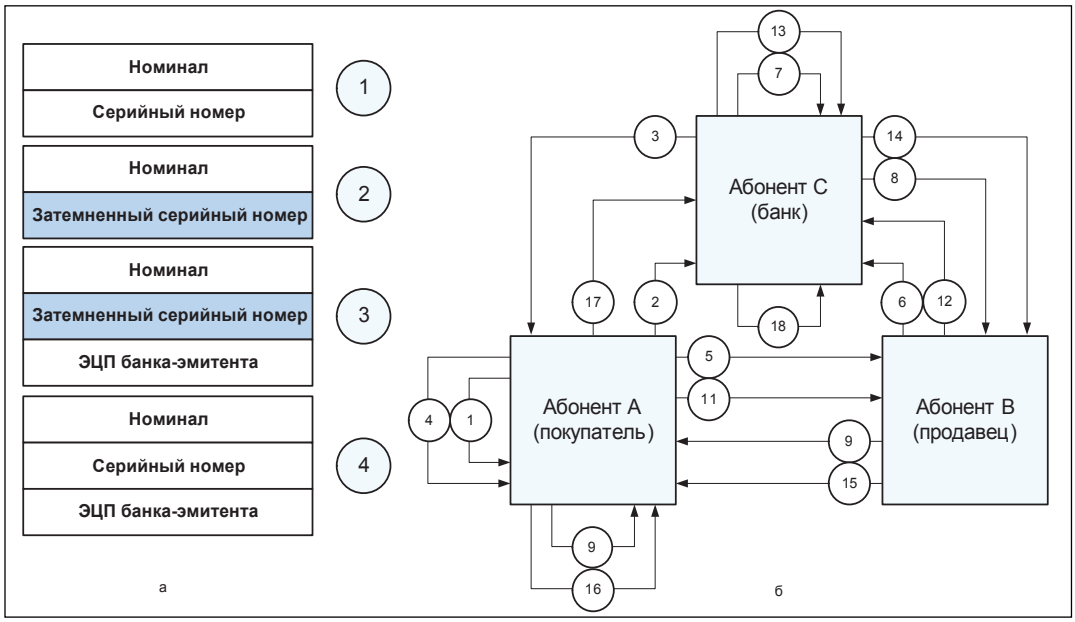

Рис. 4. Централизованная платежная система:
а — формат цифровой купюры; б — жизненный цикл цифровой купюры — обмен с использованием цифровых купюр различного достоинства и получением сдачи

Транзакция зачисления на счет

Шаг 17. В транзакции депозита абонент A может положить накопленную сумму на свой счет. Для этого он посылает в банк сообщение

$T^{1/(7\times3)(5\times3)} \bmod N$,

указывая при этом значение накопленной суммы.

Шаг 18. Банк проверяет, не использовалась ли ранее купюра-накопитель, вычисляет накопленную сумму и переводит ее на счет абонента A.

Выводы

Рассмотрены вопросы обеспечения безопасности электронных платежных систем на основе цифровых денег. Описаны механизмы защиты интересов банка-эмитента, покупателя и продавца. Приведен жизненный путь цифровой купюры: транзакции снятия со счета, покупки и зачисления на счет.

СПИСОК ЛИТЕРАТУРЫ:

1. *Sherif M. H.* Protocols for Secure Electronic Commerce. London: CRC Press, 2000.
2. *Иванов М. А., Михайлов Д. М., Чугунков И. В.* Защита информации в электронных платежных системах. М.: КНОРУС, 2010.