РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 263 347** (13) **C2**

(51) МПК[7] **G 06 F 17/60, H 04 M 3/42**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2003132137/09, 04.11.2003**

(24) Дата начала действия патента: **04.11.2003**

(45) Опубликовано: **27.10.2005 Бюл. № 30**

(56) Список документов, цитированных в отчете о поиске: **RU 2191482 C1, 20.10.2002.**
RU 2146836 C1, 20.03.2000.
RU 2169437 C1, 20.06.2001.
US 6609150 B2, 19.08.2003.
US 6275693 B1, 14.08.2001.
US 6389541 B1, 14.05.2002.
GB 2375872 A1, 27.11.2002.
НОРЕНКОВ И.П. и др. Телекоммуникационные технологии и сети, Москва, издательство МГТУ им. Н.Э. Баумана, 1998, с 129 - 131, 134 - 136.

Адрес для переписки:
127055, Москва, а/я 11, пат.пов. Н.К.Попеленскому

(72) Автор(ы):
Дышлевой К.В. (RU)

(73) Патентообладатель(ли):
Общество с ограниченной ответственностью "Мобилити" (RU)

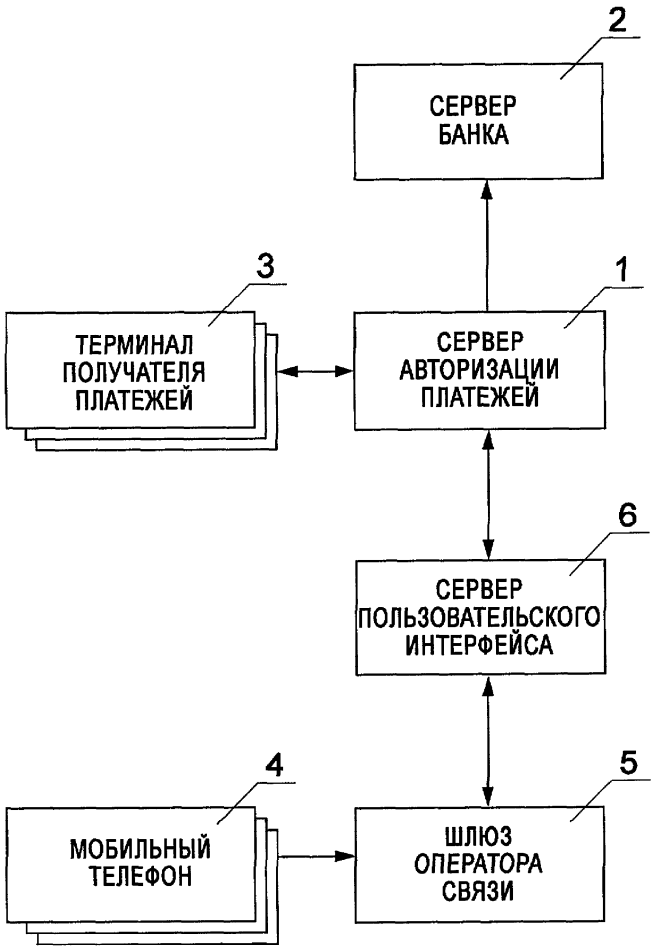
RU 2263347 C2

(54) СПОСОБ СОВЕРШЕНИЯ ПЛАТЕЖНЫХ ОПЕРАЦИЙ ПОЛЬЗОВАТЕЛЯМИ МОБИЛЬНЫХ УСТРОЙСТВ ЭЛЕКТРОННОЙ СВЯЗИ И КОМПЬЮТЕРНАЯ СИСТЕМА БЕЗНАЛИЧНОГО РАСЧЕТА ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(57) Реферат:

Изобретение относится к системам безналичного расчета для совершения платежных операций пользователями мобильных устройств электронной связи. Техническим результатом является повышение надежности и безопасности совершения платежных операций с одновременным обеспечением удобства, быстроты и простоты проведения операций. Согласно способу формируют и запоминают в сервере условия вида платежа и условие на сумму платежа, каждому виду платежа присваивают уникальный индекс, который перед совершением платежа вводят посредством мобильного устройства электронной связи, и в соответствии с введенным индексом передают в сервер системы запрос на совершение платежа, перед инициированием платежа в ответ на указанный запрос из сервера системы на мобильное устройство электронной связи передают условия указанного вида платежа с отображением этих условий на экране мобильного устройства электронной связи, после чего с мобильного устройства электронной связи в сервер передают подтвержденное платежное поручение, после получения инициируют платеж путем обращения к серверу соответствующей платежной организации. Система содержит блок работы с получателями платежей, терминал получателя платежа, блок работы с пользователями, блок работы с платежными операциями, блок генерации и сравнения псевдослучайных кодов платежных операций, запоминающее устройство. 2 н. и 30 з.п. ф-лы, 3 ил.

RU 2263347 C2



Фиг.1

RU 2263347 C2

RU 2263347 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 263 347** (13) **C2**

(51) Int. Cl.[7] **G 06 F 17/60, H 04 M 3/42**

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2003132137/09, 04.11.2003**

(24) Effective date for property rights: **04.11.2003**

(45) Date of publication: **27.10.2005 Bull. 30**

Mail address:
127055, Moskva, a/ja 11, pat.pov. N.K.Popelenskomu

(72) Inventor(s):
Dyshlevoj K.V. (RU)

(73) Proprietor(s):
Obshchestvo s ogranichennoj otvetstvennost'ju "Mobiliti" (RU)

(54) METHOD FOR PERFORMING TRANSACTIONS OF USERS OF MOBILE COMMUNICATION DEVICES AND COMPUTERIZED CASHLESS TRANSACTION SYSTEM FOR REALIZATION OF SAID METHOD

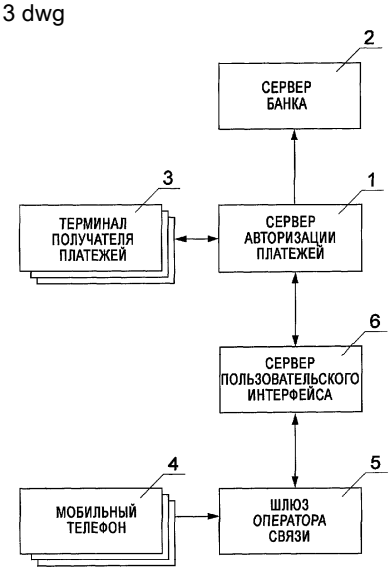
(57) Abstract:

FIELD: mobile telecommunication systems.

SUBSTANCE: method includes forming conditions of type of payment and condition on payment sum, and recording these on server, unique index is assigned to each payment type, which is inputted via mobile communication deice before transaction, in accordance to inputted index query for transaction is sent to server system, before initiation of payment in response to aforementioned query, from server system to mobile communication device conditions of aforementioned payment type are sent with displaying of these on screen of mobile communication device, after that from mobile communication device to server confirmed payment order is sent, after receipt of which payment is initiated by query to server from appropriate paying organization. System has block for working with payment receivers, payment receiver terminal, block for working with users, block for working with payment operations, block for generation and storing of pseudo-random transaction codes, recording device.

EFFECT: higher reliability, higher trustworthiness, higher speed of operation.

2 cl, 3 dwg



Фиг.1

RU 2263347 C2

RU 2263347 C2

Изобретение относится к области информационных технологий и, в частности, к способу для совершения платежных операций пользователями мобильных устройств электронной связи и компьютерной системе для его осуществления.

Уровень техники

Бурное развитие информационных технологий привело к возникновению разнообразных систем безналичного расчета, использующих линии электронной связи и ресурсы компьютерных сетей.

В публикации международной заявки WO 02/35429 описана система безналичного расчета, в которой компьютеры клиентов системы связаны посредством компьютерной сети с сайтом-посредником, организующим денежные переводы через связанный с ним банк, который, в свою очередь, связан с банками, включенными в систему. Для перевода денег от одного клиента другому плательщик должен направить в указанный сайт-посредник запрос на совершение платежа с указанием суммы, источника платежа, а также его получателя. Очевидно, что для ввода таких данных клиентом последний должен иметь компьютерный дисплей и клавиатуру.

С недавнего времени началась разработка систем безналичного расчета, ориентированных на использование в качестве пользовательских терминалов мобильных устройств электронной связи, таких как мобильные телефоны или карманные компьютеры (Personal Digital Assistant или PDA).

Одно из технических решений в данной области раскрыто в патенте Российской Федерации №2191482, рассматриваемом в качестве ближайшего аналога изобретения. В этом патенте описаны способы предложения к продаже, оформления заказов и продажи товаров и услуг с использованием сервера предложений, связанного с компьютерными терминалами продавцов товаров или услуг. Согласно этому документу продавец или сервер предложений формирует идентификацию предложений о продаже товаров или услуг, представляющую собой совокупность буквенно-цифровых знаков, то есть условный индекс, который несет в себе информацию о продавце, предлагаемом товаре, а также возможные другие сведения. Такие индексы распространяют среди пользователей мобильных устройств электронной связи. Пользователь, решивший воспользоваться предложением, вводит соответствующий индекс на своем мобильном устройстве электронной связи и на его основе передает на сервер предложений запрос на заказ или покупку соответствующего товара или услуги. Если указанный товар имеется в наличии, на мобильное устройство электронной связи пользователя направляют специальный маркер, подтверждающий оформление заказа. Этот маркер, который соответствует конкретному образцу товара, сохраняют в памяти мобильного устройства электронной связи с тем, чтобы впоследствии его можно было, например, предъявить как свидетельство оплаты для получения соответствующего товара или в качестве входного билета на некоторое мероприятие.

Использование маркеров согласно этому патенту позволяет упорядочить процесс оформления заказов благодаря созданию механизма контроля наличия того или иного вида товаров или услуг. Вместе с тем, в патенте РФ №2191482 не предусмотрены технические средства, которые страховали бы пользователя от мошенничества или ошибки ввода индекса предложения. В частности, при вводе на мобильном устройстве электронной связи индекса предложения пользователь вынужден действовать "вслепую", так как со стороны системы безналичного расчета (или сервера предложений) он не получает информации о том, за что именно и кому он платит, поскольку индекс предложения представляет собой код, понятный лишь серверу предложений. В результате может возникнуть ситуация, когда пользователь получит неверную информацию об индексе предложения или же просто допустит ошибку ввода, а неверно введенный индекс может соответствовать другому предложению. В обоих случаях в известной системе заказ будет оформлен и продажа совершена, а пользователь, инициируя оплату, не имеет возможности убедиться в том, соответствуют ли его намерениям товар, который он желает купить, продавец у которого он желает этот товар купить, и сумма, которую он готов заплатить. Более того, маркер,

полученный из сервера системы и демонстрируемый на экране мобильного устройства электронной связи, не может рассматриваться как юридически действительное доказательство совершения платежа, что может быть особенно важно в спорных ситуациях.

Сущность изобретения

Приведенный выше анализ уровня техники показывает, что в нем пока отсутствуют механизмы, страхующие пользователей мобильных устройств электронной связи, выступающих в подобного рода системах в роли плательщиков, от злоумышленных манипуляций индексами вида платежа или случайных ошибок при их передаче и распространении или ошибок ввода этих индексов на мобильном устройстве электронной связи.

Такой механизм обеспечивается предложенным способом совершения платежных операций пользователями мобильных устройств электронной связи посредством системы безналичного расчета, согласно которому формируют и запоминают в сервере указанной системы условия вида платежа, включающие в себя по меньшей мере идентификацию получателя платежей, назначение, общее для всех платежей данного вида, и условие на сумму платежа, причем конкретному виду платежа присваивают уникальный индекс. Перед совершением платежа индекс вида платежа вводят посредством мобильного устройства электронной связи, и в соответствии с введенным индексом передают в сервер системы запрос на совершение платежа. Отличие предложенного способа от ближайшего аналога изобретения заключается в том, что в ответ на указанный запрос из сервера системы на мобильное устройство электронной связи передают условия указанного вида платежа, включающие в себя по меньшей мере назначение и получателя платежа, с отображением этих условий на экране мобильного устройства электронной связи, после чего с мобильного устройства электронной связи в сервер системы передают подтвержденное платежное поручение, после получения которого посредством сервера системы инициируют платеж путем обращения к серверу соответствующей платежной организации.

Предпочтительными видами мобильного устройства электронной связи являются мобильный телефон или карманный компьютер (PDA), причем соединение между мобильным устройством электронной связи и сервером системы может устанавливаться через шлюз оператора мобильной связи. В другом варианте пользователь карманного компьютера может установить связь с сервером системы через Интернет-терминал.

Передаваемые на мобильное устройство электронной связи условия вида платежа могут включать в себя условие на сумму платежа, которое представляет собой фиксированное значение, которое впоследствии, при передаче подтвержденного платежного поручения, не подлежит изменению.

В другом случае передаваемые на мобильное устройство электронной связи условия вида платежа могут включать в себя условие на сумму платежа, представляющее собой интервал допустимых значений, при этом перед передачей подтвержденного платежного поручения с мобильного устройства электронной связи вводят конкретное значение суммы платежа, при этом проверяют нахождение введенного значения суммы платежа в указанном интервале. Такая проверка может осуществляться как аппаратно-программными средствами мобильного устройства электронной связи перед передачей подтвержденного платежного поручения в сервер системы, так и средствами сервера системы после получения указанного платежного поручения. Характерным видом платежа с интервалом допустимых значений перечисляемой суммы платежа может быть предоплата услуги, в частности услуги оператора мобильной связи. Другим примером такого вида платежа может быть взнос в благотворительный фонд.

Такой механизм выбора конкретного значения платежа в рамках заданного интервала и проверки корректности такого выбора упрощает процесс безналичного расчета, позволяя пользователю более гибко распоряжаться своими финансовыми средствами.

Условия вида платежа могут включать в себя любые из следующих элементов: комментарий получателя платежа, детальное описание компании-получателя, детальное

описание назначения платежа, изображения, трехмерные модели, видеоролики, звуковые сообщения.

Индекс вида платежа может сообщаться пользователю мобильного устройства электронной связи с использованием средств массовой рекламы и/или информационных материалов получателей платежей. Это могут быть рекламные щиты, средства передвижной наглядной рекламы, рекламные издания и публикации, телевизионная реклама и т.д. Индекс вида платежа предпочтительно указывать вместе с обозначением системы безналичного расчета, которое может быть указано перед таким индексом.

Вместе с запросом на совершение платежа или подтвержденным платежным поручением в сервер системы могут передаваться данные платежного средства пользователя, поддерживаемого указанной платежной организацией. При этом такие данные также могут храниться в запоминающем устройстве сервера системы. Платежным средством пользователя может быть банковский счет и/или кредитная карта, и в этом случае в качестве платежной организации может выступать банк. Во втором случае в качестве платежной организации может также выступать центр обслуживания кредитных карт. Кроме того, платежной организацией может быть система электронных платежей, при этом платежное средство пользователя будет представлять собой лицевой счет пользователя в указанной системе.

Для обеспечения максимального удобства ввода индекса вида платежа с мобильного устройства электронной связи этот индекс предпочтительно формировать только из цифр.

В качестве дополнительного средства безопасности совершения платежной операции после получения от пользователя подтвержденного платежного поручения посредством сервера системы может генерироваться псевдослучайный код (уникальный идентификатор) совершаемой платежной операции, который передают на терминал получателя платежа. Далее, из терминала получателя платежа указанный код операции передают непосредственно пользователю, после чего с мобильного устройства электронной связи вводят и передают код в сервер системы, в котором сравнивают значение кода платежной операции, полученного от пользователя, и значение кода платежной операции, переданного на терминал получателя платежа, причем платеж инициируют в случае совпадения указанных значений. Такому коду операции устанавливают ограниченный срок действия, по истечении которого указанный код аннулируют. Для этого, например, после генерации кода платежной операции его можно сохранить в запоминающем устройстве сервера системы на заданный отрезок времени с последующим удалением. До передачи этого кода с мобильного устройства электронной связи в сервер системы за пользователем мобильного устройства электронной связи может быть сохранено право отмены платежа посредством направления соответствующего сообщения в сервер системы.

Еще одной ступенью безопасности при осуществлении предложенного способа может быть дополнительная проверка полномочий пользователя мобильного устройства электронной связи на совершение платежа посредством ввода фиксированного пароля и/или одноразового кода аутентификации пользователя, такого как персональный идентификационный номер (PIN-код), на мобильном устройстве электронной связи. Например, если мобильное устройство электронной связи поддерживает язык J2ME (Java 2 Micro Edition), то введенный пользователем фиксированный пароль или одноразовый код аутентификации может передаваться в систему с помощью устанавливаемого на мобильном устройстве J2ME приложения (т.н. "мидлета") и через дополнительный сервер пользовательского интерфейса, поддерживающий работу с приложениями, написанными на языке J2ME и связанный с сервером системы.

В другом варианте, если мобильное устройство электронной связи поддерживает протокол WAP, введенный пользователем фиксированный пароль или одноразовый код аутентификации может передаваться в сервер системы через связанный с ним дополнительный сервер пользовательского интерфейса, поддерживающий обмен информацией с мобильными устройствами электронной связи на языке WML

Предложенный способ безналичного расчета также позволяет упростить расчеты в случае совмещения соответствующей системы безналичного расчета с различного рода информационными сервисами. В частности, индекс вида платежа может соответствовать индексу конкретного товара в базе данных товаров, обеспечивающей такой сервис. Эта база данных товаров может поддерживаться на сервере пользовательского интерфейса, причем пользователю мобильного устройства электронной связи предоставляют доступ к указанной базе данных посредством соответствующего WAP- или Ц2ME-интерфейса.

Когда получатель платежа и пользователь мобильного устройства электронной связи находятся на удалении, для обеспечения возможности связи между ними код платежной операции может передаваться на терминал получателя платежа вместе с соответствующей идентификацией пользователя, в частности, с указанием номера его мобильного телефона.

В частном случае осуществления предложенного способа видом платежа является уплата государственной пошлины за выдачу общегражданского или заграничного паспорта, при этом код платежной операции передают на терминал оператора паспортной службы с указанием фамилии, имени и отчества пользователя мобильного устройства электронной связи, а передачу этого кода пользователю осуществляют непосредственно через оператора терминала паспортной службы (при проведении собеседования с пользователем).

Вторым объектом изобретения является компьютерная система безналичного расчета для совершения платежных операций пользователями мобильных устройств электронной связи, включающая в себя сервер авторизации платежей, связанный с мобильными устройствами электронной связи, сервером по меньшей мере одной платежной организации и терминалом по меньшей мере одного получателя платежей. Отличие предложенной системы от ближайшего аналога изобретения заключается в том, что сервер авторизации платежей содержит: блок работы с получателями платежей, связанный с указанным терминалом получателя платежа с возможностью формирования условий видов платежей; блок работы с пользователями, связанный с мобильными устройствами электронной связи; блок работы с платежными операциями, связанный с сервером платежной организации и блоком работы с пользователями; и запоминающее устройство, содержащее по меньшей мере область хранения данных о пользователях и их платежных средствах и область хранения условий видов платежей, причем запоминающее устройство связано с блоком работы с получателями платежей, блоком работы с пользователями и блоком работы с платежными операциями.

Сервер авторизации платежей может содержать блок генерации и сравнения псевдослучайных кодов платежных операций, вход которого связан с блоком работы с пользователями, один выход - с блоком работы с получателями платежей, а другой выход - с блоком работы с платежными операциями, при этом запоминающее устройство сервера авторизации платежей может содержать область хранения кодов платежных операций, причем блок генерации и сравнения псевдослучайных кодов платежных операций связан с указанной областью хранения кодов платежных операций. Запоминающее устройство сервера авторизации платежей может содержать область хранения данных о получателях платежей и их счетах, связанную с блоком работы с получателями платежей.

В предпочтительном варианте предложенная система содержит дополнительный сервер пользовательского интерфейса, связывающий сервер авторизации платежей с мобильными устройствами электронной связи. Этот сервер пользовательского интерфейса предпочтительно поддерживает работу с приложениями, написанными на языке J2ME, и/или обмен информацией с мобильными устройствами электронной связи на языке WML по протоколу WAP.

Мобильное устройство электронной связи может иметь возможность связи с сервером пользовательского интерфейса по каналу безопасного соединения, в частности с применением шифрования по одному из протоколов RC6, WTLS или SSL. В рамках системы сервер авторизации платежей может быть связан с терминалом получателя

платежа, сервером платежной организации и сервером пользовательского интерфейса каналами безопасного соединения, в частности с применением шифрования по протоколу SSL.

Для повышения безопасности обмена данными сервер авторизации платежей может быть связан с сервером платежной организации и терминалами получателей платежей через устройство сетевой защиты.

Кроме того, сервер авторизации платежей может содержать блок генерации кодов аутентификации, а запоминающее устройство сервера авторизации платежей - область хранения кодов аутентификации, связанную с блоком работы с пользователями, причем блок генерации кодов аутентификации в этом случае связан с указанной областью хранения кодов аутентификации.

Посредством заявляемого изобретения достигается повышение надежности и безопасности совершения платежных операций посредством системы безналичного расчета пользователями мобильных устройств электронной связи без существенного повышения требований к этим устройствам и при одновременном обеспечении удобства, быстроты и простоты проведения указанных операций пользователями. Это позволяет осуществить массовое внедрение указанной системы безналичного расчета.

Краткое описание чертежей

На фиг.1 представлена структурная схема предложенной системы безналичного расчета.

На фиг.2 представлена структурная схема предложенной системы безналичного расчета в другом варианте осуществления изобретения.

На фиг.3 представлена структурная схема сервера авторизации платежей.

Осуществление изобретения

На фиг.1 представлена структурная схема системы безналичного расчета, в которой может быть реализован предложенный способ безналичного расчета. Стрелками обозначены каналы связи между компонентами и преимущественное направление потоков информации. Основными элементами системы являются сервер 1 авторизации платежей, сервер платежной организации (в частности, сервер 2 банка), терминал 3 получателя платежей и мобильное устройство электронной связи (в частности, мобильный телефон) 4.

Мобильный телефон 4 связан со шлюзом 5 оператора мобильной связи, через который он может обмениваться данными с сервером 1 авторизации платежей.

Взаимодействие между мобильными телефонами и сервером авторизации платежей обеспечивает дополнительный сервер пользовательского интерфейса 6, связывающий сервер 1 авторизации платежей с мобильными телефонами 4. Для обеспечения возможности работы с как можно более широким спектром моделей мобильных телефонов сервер пользовательского интерфейса 6 поддерживает работу с приложениями, написанными на языке J2ME, а также обмен информацией с мобильными устройствами электронной связи на языке WML по протоколу WAP. Как вариант, сервер пользовательского интерфейса 6 может дополнительно поддерживать базу данных товаров и/или услуг, к которой пользователи мобильных телефонов получают доступ посредством соответствующего WAP- или J2ME-интерфейса.

Терминал 3 получателя платежей предпочтительно представляет собой компьютер, соответствующим образом подключенный к компьютерной сети (например, сети Интернет), но может также быть представлен оконечным устройством другого типа, в том числе мобильным устройством электронной связи.

Как это поясняется ниже, сервер 1 авторизации платежей является основным элементом предложенной системы безналичного расчета, он связан с терминалами 3 получателей платежей и сервером 2 банка и в предпочтительном варианте представляет собой средство контроля за совершением платежных операций, используемое при совершении платежных операций, в частности для авторизации и отмены платежей. Платежные поручения пересылаются сервером 1 авторизации платежей на сервер 2 банка после подтверждения платежа в соответствии с предложенным способом совершения

платежных операций.

Сервер 1 авторизации платежей связан с сервером 2 банка, терминалами 3 получателей платежей и сервером пользовательского интерфейса 6 каналами безопасного соединения. Предпочтительным является шифрование передаваемых данных по технологии SSL. Для обеспечения безопасности при передаче данных с мобильного телефона и на него мобильный телефон 4 также связан с сервером пользовательского интерфейса 6 по каналу безопасного соединения. Для этих целей шифрование может осуществляться по одному из протоколов RC6, WTLS или SSL. Возможности использования протоколов WTLS и SSL будут рассмотрены ниже при описании работы пользователя с системой безналичного расчета, содержащей сервер пользовательского интерфейса 6.

На фиг.2 представлена структурная схема системы безналичного расчета в другом варианте выполнения, отличающемся от рассмотренного выше тем, что вместо одного сервера пользовательского интерфейса 6 в системе предусмотрены два отдельных сервера, один из которых реализует интерфейс для работы с мобильными телефонами с поддержкой J2ME (для краткости далее называемый J2ME-сераер и обозначенный на фиг.2 позицией 7), а другой - интерфейс для работы с мобильными телефонами с поддержкой WAP (для краткости далее называемый WAP-сервер и обозначенный на фиг.2 позицией 8).

Кроме того, если в варианте, отображенном на фиг.1, предполагается, что защита сервера 1 авторизации платежей может быть реализована программными средствами этого сервера, а также сервера пользовательского интерфейса 6, то в рассматриваемом варианте сервер 1 авторизации платежей связан с J2ME-сервером 7 и WAP-сервером 8, и терминалами 3 получателей платежей, а также сервером банка 2 через дополнительные устройства сетевой защиты 9 и 10 (firewall), например устройства Cisco PIX компании Cisco Systems.

Система может быть реализована в различных конфигурациях. Так, сервер 1 авторизации платежей может быть связан с сервером единственной платежной организации (сервер 2 банка на фиг.1). В этом случае предложенная система безналичного расчета может использоваться соответствующим банком для организации собственного центра обработки платежей. Сервер 1 авторизации платежей будет при этом администрироваться указанным банком. В другом варианте один сервер 1 авторизации платежей с соответствующим сервером пользовательского интерфейса 6 могут обслуживать несколько банков (фиг.2). Существует также возможность организации межбанковской системы, в которой к одному серверу пользовательского интерфейса 6 подключено несколько серверов авторизации платежей, относящихся к разным банкам.

Как показано на фиг.3, где стрелками обозначены каналы связи между компонентами и преимущественное направление потоков информации, сервер 1 авторизации платежей содержит следующие функциональные блоки: блок 11 работы с получателями платежей, который связан с терминалом получателя платежа с возможностью формирования условий видов платежей, блок 12 работы с пользователями, связанный с мобильными телефонами 4 (через шлюз 5 оператора мобильной связи), блок 13 работы с платежными операциями, связанный с сервером 2 банка и блоком 12 работы с пользователями, и запоминающее устройство 14, содержащее по меньшей мере область хранения данных о пользователях и их платежных средствах и область хранения условий видов платежей. Запоминающее устройство 14 связано с вышеупомянутыми блоком 11 работы с получателями платежей, блоком 12 работы с пользователями и блоком 13 работы с платежными операциями.

Для дополнительного подтверждения пользователем мобильного телефона совершаемого им платежа, механизм которого будет рассмотрен ниже при описании работы системы безналичного расчета, сервер 1 авторизации платежей содержит блок 15 генерации и сравнения псевдослучайных кодов платежных операций, вход которого связан с блоком 12 работы с пользователями, один выход - с блоком 11 работы с получателями платежей, а другой выход - с блоком 13 работы с платежными операциями. Для сохранения генерируемых кодов блок 15 генерации и сравнения псевдослучайных кодов платежных операций связан с запоминающим устройством 14, которое содержит область хранения

кодов платежных операций. Для идентификации получателей платежей запоминающее устройство 14 сервера 1 авторизации платежей содержит область хранения данных о получателях платежей и их счетах, связанную с блоком 12 работы с получателями платежей сервера авторизации платежей.

Для проверки полномочий пользователей мобильных устройств электронной связи на совершение платежей в составе сервера 1 авторизации платежей предусмотрен блок 16 генерации кодов аутентификации. Код аутентификации может представлять собой фиксированный пароль или одноразовый pin-код, который передается пользователю и вводится им с мобильного телефона. Запоминающее устройство 14 сервера 1 авторизации платежей содержит отдельную область хранения кодов аутентификации, связанную с блоком 12 работы с пользователями. При этом блок 16 генерации кодов аутентификации связан с областью хранения кодов аутентификации запоминающего устройства.

Сервер 1 авторизации платежей может быть выполнен в виде вычислительного устройства или системы, представляя собой аппаратный и программный комплекс, во множестве конфигураций, с учетом объема и направленности предложенной системы безналичного расчета в каждом конкретном случае. Понятие "сервер авторизации платежей" используется в данной заявке в смысле "центральный узел компьютерной системы" и, как указано выше, допускает возможность его реализации во многих вариантах. Детали аппаратного и программного воплощения сервера авторизации платежей, как и других компонентов предложенной системы безналичного расчета, не относятся к сущности данного изобретения.

В одном варианте практического воплощения сервер 1 авторизации платежей может представлять собой один мощный многопроцессорный сервер с большим объемом памяти (ОЗУ) (например, 4 гигабайт или больше) и большим дисковым пространством (т.е. с большим объемом ПЗУ). Функционирование каждого из блоков 11, 12, 13, 15, 16 может поддерживаться отдельным процессором. Для реализации каждой из вышеописанных областей памяти целесообразно использовать собственное ПЗУ, т.е. в этом варианте запоминающее устройство 14 сервера 1 авторизации платежей может состоять, например, из пяти отдельных дисковых накопителей. Представленные на фиг.3 связи между блоками сервера авторизации платежей, а также запоминающим устройством реализуются информационной шиной, например материнской (системной) платой, и, при необходимости, сетевыми кабелями в сочетании с сетевыми адаптерами известных типов.

Вместе с тем, эффективность и производительность сервера авторизации платежей можно повысить, реализовав часть его функциональных блоков в виде отдельных рабочих станций, с которыми сервер авторизации платежей может быть объединен в локальную сеть. Это особенно важно для тех блоков, которые по своей функциональности тесно связаны с работой с базами данных. Таковыми, в частности, являются блок 15 генерации и сравнения псевдослучайных кодов платежных операций и блок 12 работы с пользователями.

В настоящее время мобильный телефон 4 является наиболее распространенным типом мобильных устройств электронной связи, однако в предложенной системе равным образом применимы любые другие типы подобных устройств, которые могут поддерживать связь с Интернет-сервером системы безналичного расчета (в том числе с вышеупомянутым J2ME-сервером 7 и/или WAP-сервером 8). Кроме мобильного телефона это может быть PDA (карманный компьютер) или даже пейджер. С системой безналичного расчета мобильное устройство электронной связи может общаться посредством протокола WAP (Wireless Application Protocol) версии 1.1 или более новой, либо языка J2ME (Java 2 ME). Желательно наличие поддержки протокола GPRS (General Packet Radio Service).

Подключение к системе мобильного устройства электронной связи также может осуществляться через инфракрасные порты (IrDA), либо по технологии Bluetooth (универсальная технология беспроводной связи разнотипных микропроцессорных устройств локальной сети в диапазоне 2,4 ГГц), либо с использованием любой другой технологии локального беспроводного обмена данными между электронными

устройствами, с компьютером или любым другим электронным устройством, обеспечивающим подключение к системе, например, через глобальную сеть Интернет. Это означает, что в качестве мобильного устройства электронной связи потребителя может использоваться также карманный компьютер без функции коммуникатора (то есть без возможности подсоединения к шлюзу оператора связи), при этом достаточно наличия у такого карманного компьютера, например, инфракрасного порта.

Пользовательский интерфейс может быть реализован блоком 12 работы с пользователями либо на языке WML (Wireless Markup Language, работу с этим языком обязано поддерживать любое мобильное устройство связи, которое поддерживает протокол WAP, т.к. это взаимосвязанные технологии), либо на языке Java (J2ME). Стандарты WAP, WML, GPRS разработаны компанией Open Mobile Alliance Ltd. (OMA). Стандарты Java 2 Micro Edition (J2ME), а также Personal Java разработаны компанией SUN Microsystems.

В случае использования WML память мобильного телефона не используется, пользователь работает с системой, подсоединяясь к WAP-серверу 8 системы. Передача информации между мобильным устройством и сервером 1 авторизации платежей в этом случае осуществляется средствами протокола WAP.

В последнем же случае, когда используется Java, на мобильный телефон пользователя устанавливается приложение на языке Java (J2ME), реализующее пользовательский интерфейс (установка приложения может производиться, например, оператором связи или же самим потребителем путем загрузки приложения из сети Интернет). Взаимодействие такого приложения с сервером 1 авторизации платежей осуществляется путем непосредственного подключения мобильного устройства к сети Интернет по любому из протоколов CSD (Circuit Switched Data - технология обмена данными с использованием голосового канала, может использоваться только для работы с WAP-сайтами, в связи с чем в литературе чаще всего вместо "CSD" указывают "WAP"; мы также будем придерживаться этого обозначения) или GPRS (может использоваться как для работы с WAP-сайтами, так и для связи Java (J2ME) приложений с сервером). Важно отметить, что вариант работы с системой с помощью Java приложения (с использованием связи через GPRS) более предпочтителен, так как он требует передачи меньшего объема данных между мобильным телефоном и системой (за счет хранения приложения в памяти мобильного устройства), то есть этот способ работает быстрее, и при этом выразительные средства языка Java более развиты, поэтому пользовательский интерфейс в этом случае также и более удобен для потребителей.

Возможность реализации предложенной системы безналичного расчета обеспечивается тем, что использование протоколов WAP (CSD) и GPRS для соединения с Интернет мобильных телефонов и PDA с функцией коммуникатора поддерживается всеми крупными российскими операторами мобильной связи, в частности, МТС, "БиЛайн" и "Мегафон", их пользователям необходимо лишь иметь мобильный телефон или PDA с поддержкой WAP или GPRS. На данный момент не менее 80% продаваемых в России и за рубежом моделей мобильных телефонов поддерживают работу по протоколу WAP. Так, на основании данных Интернет-портала "sotovic" (www.sotovic.ru) можно утверждать, что среди имеющихся сейчас на рынке 121 моделей мобильных телефонов различных производителей в настоящее время 15 моделей поддерживают стандарт WAP 1.1, 11 моделей поддерживают стандарт WAP 1.2, 70 моделей поддерживают стандарт WAP 1.2.1, и 18 моделей поддерживают стандарт WAP 2.0. Язык JAVA поддерживают 49 моделей, технологию GPRS - 81 моделей. Значительная доля существующих мобильных телефонов приходится на модели с большими полноцветными экранами, наилучшим образом приспособленные для отображения условий платежа. Так, экран размером более 128×128 имеют 48 моделей, а количество моделей с 4096 цветами составляет 55. Эти цифры свидетельствуют о том, что технический уровень мобильных телефонов и PDA уже обеспечил техническую и экономическую базу для внедрения предложенных системы и способа.

Таким образом, на данный момент значительная часть пользователей мобильных

телефонов в России и за рубежом уже имеют возможность непосредственной работы с предложенной системой со своих мобильных телефонов.

Среди таких мобильных телефонов, которые в максимальной степени приспособлены для работы в предложенной системе, стоит выделить следующие модели:

Sony Ericsson P800 (GPRS, MMS, Java, Personal Java, экран 208×320);

Nokia 3650 (GPRS, MMS, Java, Personal Java, экран 176×208);

Nokia 7650 (GPRS, Java, экран 176×208);

Samsung SGH-S100 (GPRS, Java, экран 128×160);

Motorola V600 (GPRS, MMS, Java, экран 120×160);

Sharp GX1, GX10 (GPRS, MMS, Java, экран 120×160);

Panasonic GD87 (GPRS, MMS, Java, экран 120×160);

LG G8000 (GPRS, MMS, Java, экран 176×220);

NEC e525, N8 (GPRS, MMS экран 162×216).

Что касается карманных компьютеров (PDA), то любой из них, обладающий функцией коммуникатора, изначально очень хорошо подходит для непосредственной работы с системой. Это объясняется тем, что на подобных устройствах экран достаточно велик и ввод информации потребителем весьма удобен. Хотя важно отметить, что в связи с гораздо большими размерами подобные устройства пользуются гораздо меньшей популярностью по сравнению с мобильными телефонами. Поэтому основными потенциальными пользователями системы должны стать пользователи мобильных телефонов.

Среди устройств указанного здесь типа (PDA с функциями коммуникатора), с помощью которых потребители могут работать с системой, следует выделить:

Nokia 9210, 9210i, 9290 (Java, Personal Java, экран 640×200);

Motorola Accompli 008 (GPRS, Java, экран 240×320);

Motorola Accompli 008 (GPRS, Java, экран 240×160);

Motorola A388 (GPRS, Java, экран 240×320);

Blackberry 5810, 5820 (GPRS, Java, экран 160×160).

Предложенная система безналичного расчета функционирует следующим образом.

Получатель платежа (часто таковым является поставщик товаров и/или услуг) вводит через свой терминал 3 в сервер 1 авторизации платежей условия вида платежа, включающие в себя по меньшей мере идентификацию получателя платежей, назначение, общее для всех платежей данного вида, и условие на сумму платежа. Условия вида платежа могут включать в себя произвольного вида текст в качестве описания назначения платежа, а условие на сумму платежа может содержать фиксированную сумму или интервал допустимых значений в качестве суммы платежа. Условия вида платежа обрабатываются блоком 11 работы с получателями платежей и вводятся в запоминающее устройство 14, причем каждому конкретному виду платежа присваивают уникальный индекс, распространяемый среди пользователей мобильных устройств электронной связи.

Характерными видами платежей являются: уплата различных фиксированных пошлин, сборов и штрафов, оплата услуг связи, коммунальных услуг, а также оплата других товаров и/или услуг, предлагаемых поставщиками. Индексы видов платежей распространяются посредством любых доступных каналов, таких как линии телекоммуникаций (в том числе мобильной связи - через SMS-сообщения), средства массовой рекламы (рекламные щиты, передвижная наглядная реклама, рекламные издания и публикации, телевизионная реклама) или информационных материалов получателей платежей. При этом индекс вида платежа предпочтительно составляют из цифр (для облегчения набора на мобильном устройстве электронной связи) и указывают вместе с обозначением соответствующей системы безналичного расчета, поскольку параллельно могут функционировать несколько таких систем.

Для пользования ресурсами системы безналичного расчета пользователь мобильного телефона должен в ней зарегистрироваться.

Регистрация новых пользователей в системе включает в себя следующие операции:

- создание учетной записи в сервере 1 авторизации платежей или, как вариант, в сервере пользовательского интерфейса 6,

- регистрацию контактной информации пользователя;

- регистрацию банковских счетов (или других платежных средств, таких как кредитные карты), которые будут использоваться для проведения платежей.

После создания учетной записи пользователя блок 12 работы с пользователями посылает SMS-сообщение на указанный им при регистрации номер мобильного телефона. Указанное сообщение содержит WAP-ссылку для быстрого входа в систему в будущем (ссылка содержит открытый уникальный идентификатор пользователя в системе). Эту ссылку пользователь может сохранить в списке WAP-закладок, после чего для входа в систему не будет требоваться ввод идентификатора, однако пароль необходимо набирать при каждом входе в систему по этой ссылке. При работе с модулем Java2ME идентификатор пользователя потребуется ввести лишь один раз при первом входе в систему, после чего этот идентификатор будет сохранен в памяти телефона, и в дальнейшем будет автоматически подставляться в соответствующее поле; так же, как и при использовании WAP, пароль требуется вводить при каждом входе в систему.

Предусмотрено два механизма регистрации пользователей:

Первый - через Web-сайт системы безналичного расчета пользователь может зарегистрироваться только для работы с информационными ресурсами системы безналичного расчета (каталог товаров и/или услуг, поддерживаемый сервером пользовательского интерфейса 6), без возможности проведения каких-либо платежей. Соответственно, при этом доступны лишь операции создания новой учетной записи и регистрация контактной информации.

Второй - через платежную организацию (банк), включенную в систему. В этом случае пользователь сможет выполнить все три вышеуказанные операции, которые необходимы для того, чтобы получить возможность использовать все функции системы, в том числе оплачивать покупки/счета и отправлять денежные переводы.

При регистрации через банк доступны следующие две возможности:

- регистрация нового пользователя системы безналичного расчета, то есть выполнение всех трех перечисленных выше операций, при этом должны быть введены все идентификационные данные, необходимые системе, включая номер мобильного телефона.

- "дорегистрация" пользователя, то есть если пользователь уже зарегистрирован в системе (например, через Интернет), оператору банка остается зарегистрировать в системе платежное средство пользователя (счет или кредитную карту). Может быть предусмотрено, что реальные банковские реквизиты при этом остаются известными только банку, т.к. они хранятся на сервере 1 авторизации платежей, являющемся частью системы безналичного расчета и администрируемом этим банком.

Регистрационные данные пользователя обрабатываются блоком 12 работы с пользователями и сохраняются в области хранения данных о пользователях и их платежных средствах запоминающего устройства 14.

Для входа в систему через WAP-сервер 8 пользователь посредством кнопок мобильного телефона 4 выбирает упомянутую выше ссылку на WAP-сервер и нажимает "ОК", после чего вводит предпочтительно цифровой индекс вида платежа, который требуется совершить. В целом, работа пользователя с системой зависит от возможностей телефона. Так, стандарт WAP 1.1 не предусматривает никаких дополнительных (помимо предусмотренных в GSM) механизмов шифрования передаваемой в обоих направлениях между телефоном и шлюзом оператора связи информации и не предусматривает никаких удобств работы с сообщениями (отсутствует поддержка технологии WAP Push, возможности использования которой описаны ниже). Правда, немаловажно подчеркнуть, что связь между шлюзом и любым WAP-сервером осуществляется как между любыми двумя "обычными" серверами в Интернет, то есть с помощью протоколов HTTP или HTTPS (HTTP через SSL). Для обеспечения максимальной безопасности на этом участке

предпочтительно использовать именно протокол HTTPS (то есть SSL).

Следует также отметить, что помимо совершения платежей путем ввода индекса вида платежа, может использоваться механизм формирования и размещения на сервере 1 авторизации платежей или на сервере пользовательского интерфейса 6, коммерческих предложений. В частности, после установления связи с сервером 1 авторизации платежей через WAP-сервер 8 пользователь может просмотреть сохраненные ранее сформированные для него коммерческие предложения поставщиков (получателей платежей) и выбрать некоторое из них для оплаты. Например, возможна ситуация, когда пользователь общается с представителем поставщика, и последний формирует коммерческое предложение для пользователя, передавая его с терминала 3 получателя платежей в сервер 1 авторизации платежей. После этого пользователь сразу же входит в систему и выбирает первое в списке коммерческое предложение (только что полученное, так как коммерческие предложения всегда упорядочены в любом графическом пользовательском интерфейсе (GUI) по дате их выставления).

В другом случае пользователь может получить от поставщика SMS-сообщение, оповещающее его о появлении нового коммерческого предложения (например, выставлен счет на оплату коммунальных услуг), при этом сразу же или в любой момент, когда это будет ему удобно, пользователь устанавливает соединение через WAP-сервер 8 с сервером 1 авторизации платежей и находит соответствующее предложение в списке всех предложений (если он войдет в систему сразу же вслед за получением SMS-сообщения, то с высокой вероятностью соответствующее предложение будет первым в списке).

В случае осуществления расчета путем ввода индекса вида платежа запрос пользователя обрабатывается блоком 12 работы с пользователями, который обращается к запоминающему устройству 14, в частности к его области хранения условий видов платежей, и вызывает данные условий конкретного вида платежа, которому соответствует полученный от пользователя индекс. Эти данные, включающие в себя как минимум назначение платежа и идентификацию получателя платежа, направляются блоком 12 работы с пользователями на мобильный телефон 4 и отображаются на его экране средствами графического пользовательского интерфейса вместе с приглашением подтвердить совершение платежной операции. Нажимая кнопку "ОК", пользователь направляет со своего мобильного телефона в сервер 1 авторизации платежей подтвержденное платежное поручение, которое поступает через WAP-сервер 8 опять же в блок 12 работы с пользователями сервера 1 авторизации платежей.

В случае осуществления расчета по коммерческому предложению система работает аналогично. Пользователь просматривает соответствующее коммерческое предложение (счет) с помощью того же WAP-интерфейса. Просмотрев информацию о получателе платежа, назначении и, к примеру, сумме платежа, пользователь решает оплатить этот счет и нажимает соответствующую кнопку телефона.

Вышеописанный алгоритм обеспечивает надежный механизм защиты пользователей и платежных организаций как от случайных неточностей ввода индексов видов платежей, так и от злоумышленных манипуляций индексами. При распространении индексов видов платежей средствами массовой рекламы или информационными материалами получателей платежей злоумышленники могут подменить действительный индекс на другой, ссылающийся на их банковский счет. При отсутствии рассмотренного выше механизма формирования подтвержденного платежного поручения с предварительным отображением условий вида платежа на экране мобильного телефона пользователь, совершая платеж, не может быть полностью уверен в том, что его деньги будут переведены именно тому получателю, который указан в рекламе, информационном буклете и т.п. Изобретение же позволяет пользователю перед подтверждением своего намерения совершить платеж убедиться в том, что введенный им индекс вида платежа в точности соответствует предмету совершаемой сделки.

Еще одним аспектом обеспечения безопасности совершения платежей в системе безналичного расчета является проверка полномочий пользователей на совершение той

или иной платежной операции.

Известным средством аутентификации пользователей является пользовательский пароль. Однако в WAP 1.1 шифрование не поддерживается, поэтому использование фиксированного пользовательского пароля для подтверждения полномочий не обеспечивает должного уровня безопасности и, таким образом, неприемлемо.

Для решения этой проблемы может быть предусмотрен механизм использования одноразовых кодов аутентификации, или pin-кодов. Например, список (распечатку) подобных pin-кодов пользователь получает в банке или от администратора системы безналичного расчета (по согласованию с банком) в момент регистрации в системе, а также после использования или утери всех предыдущих pin-кодов (последние при этом, естественно, становятся недействительными). Стоит отметить, что pin-коды в подобном списке пронумерованы и предпочтительно представляют собой числа для удобства ввода с помощью клавиш телефона.

Полная цепочка работы с PIN-кодами выглядит следующим образом:

После того, как пользователь передал в WAP-сервер 8 запрос на совершение некоего платежа, WAP-сервер 8 связывается по SSL-каналу с сервером 1 авторизации платежей, уведомляя последний в заинтересованности указанного пользователя (при этом передается идентификатор пользователя) совершить указанный платеж (передается идентификатор счета в системе). В ответ на это сервер 1 авторизации платежей передает WAP-серверу номер в списке очередного неиспользованного одноразового PIN-кода (это не обязательно следующее по порядку в списке значение после использованного предыдущий раз). Уже с этого момента сервер 1 авторизации платежей считает соответствующий pin-код израсходованным (то есть этот pin-код уже не может быть использован для совершения какого бы то ни было платежа, кроме заявленного).

В рамках WAP-интерфейса сервер предлагает пользователю ввести одноразовый pin-код с указанным номером из имеющейся у пользователя распечатки pin-кодов.

Введенное пользователем число передается WAP-сервером 8 в сервер 1 авторизации платежей, где оно и проверяется. Только в случае совпадения этого числа с избранным ранее pin-кодом, на мобильный телефон пользователя передаются условия вида платежа для последующего формирования подтвержденного платежного поручения. Если же pin-код указан неверно, WAP-сервер 8 информируется об ошибке, избранный ранее pin-код становится недействительным даже для совершения текущего платежа. WAP-сервер 8 сообщает в этом случае пользователю об ошибке и предлагает ввести другой pin-код. При утвердительном ответе вышеописанная цепочка начинается сначала. Если три раза подряд вводятся неверные запрашиваемые pin-коды, механизм совершения платежей при помощи системы безналичного расчета для данного пользователя блокируется.

Следует отметить, что WAP-сервер 8 работаете пользователями в рамках сессий (понятие сессии тесно связано с самим WAP и соответствует одному сеансу работы с конкретным телефоном). Для одного и того же пользователя не поддерживается возможность работы с несколькими сессиями в параллель даже для работы с информацией, не говоря уже об оплате. При этом идентификаторы сессий формируются в сервере 1 авторизации платежей по запросу WAP-сервера 8.

Если мобильный телефон поддерживает протокол WAP Push, предыдущая ситуация дополняется весьма удобным и важным механизмом: получатель платежа (поставщик) получает возможность посылать на телефон пользователя специальные сообщения (WAP Push-сообщения), аналог SMS-сообщений, которые по приходу немедленно обрабатываются таким образом, что пользователю предлагается перейти по указанному указателю ресурса (URL) на указанный в таком сообщении WAP-сервер 8. Подключение к WAP-серверу 8 и переход на указанную страницу соответствующего сайта производится немедленно и автоматически после подтверждения владельцем телефона желания воспользоваться этим механизмом (единственным нажатием кнопки). В остальном работа с одноразовыми PIN-кодами не отличается от описанной выше, с той особенностью, что указание страницы поддерживаемого WAP-сервером сайта может содержать

сгенерированное сервером 1 авторизации платежей случайное значение, необходимое для работы с конкретным предложением конкретному пользователю. То есть именно пользователь, получивший такое Push-сообщение на свой телефон (сообщение посылается на телефон пользователя, номер которого зарегистрирован в системе), и именно со своего телефона вообще имеет возможность попасть на страницу работы с PIN-кодами.

Внутри сервера 1 авторизации платежей работа с PIN-кодами обеспечивается блоком 16 генерации кодов аутентификации, который передает сгенерированные pin-коды в блок 12 работы с пользователями, а также в запоминающее устройство, а именно в область хранения кодов аутентификации, связанную с блоком 12 работы с пользователями, в котором осуществляют вышеуказанное сравнение кода, выбранного системой, с кодом, переданным пользователем.

Если мобильный телефон поддерживает протокол WAP 1.2.1/2.0, принципиальным отличием WAP 1.2.1 от предыдущих версий является поддержка и WAP Push, и протокола шифрования информации WTLS (Wireless Transport Layer Security), представляющего собой WAP-эквивалент протокола SSL (Secure Sockets Layer), широко используемого в банковских сетевых решениях. Схема работы с WTLS состоит в том, что передаваемая в рамках WAP информация шифруется между мобильным телефоном 4 и WAP-шлюзом (шлюзом 5 оператора связи), а данные, передаваемые между шлюзом 5 и WAP-сервером 8, шифруются исключительно по протоколу SSL

Таким образом, WTLS-шифрование в данном случае предоставляет возможность шифровать всю получаемую от системы и передаваемую в систему информацию, что позволяет скрыть от гипотетических злоумышленников и информацию об интересах пользователя (когда он работает с базой данных товаров и/или услуг, поддерживаемой сервером пользовательского интерфейса 6), и - что особенно важно - производить все действия, связанные с оплатой, в абсолютно защищенном режиме.

Для аутентификации пользователя в этом случае достаточно использовать обычный пароль, т.к. прочитать его невозможно ни на самом телефоне (если он утерян), ни между телефоном и сервером системы. Следует также отметить, что любой телефон, поддерживающий WTLS, также поддерживает WAP Push, что позволяет реализовать рассмотренное выше преимущество стандарта WAP Push при общении поставщика (получателя платежа) с пользователем мобильного телефона перед совершением платежа. Кроме того, стандарт WAP Push можно использовать и при взаимодействии мобильного телефона 4 с сервером 1 авторизации платежей, чтобы гарантировать, что оплата действительно производится именно с телефона пользователя. То есть нажатие пользователем кнопки подтверждения коммерческого предложения поставщика в информационной части системы является триггером, инициирующим работу указанного выше сервиса, который генерирует случайное значение, посылает Push-сообщение пользователю и т.д. При этом ввод пароля необходим в любом случае, независимо от того, направляет ли пользователь запрос на совершение платежа, находясь в базе данных товаров или услуг сервера пользовательского интерфейса 6, или нет. В любом случае для передачи в сервер 1 авторизации платежей подтвержденного платежного поручения новое WAP-соединение устанавливать не нужно, так как оно уже открыто.

Более широкие возможности по обеспечению безопасности передачи данных предоставляют мобильные телефоны, поддерживающие язык Java (J2ME). В случае использования Ц2ME-приложений для работы с системой появляется возможность организации шифрования данных, не зависимого от оператора связи (как в случае с WAP и WTLS). Целесообразным является применение, например, схемы шифрования RC6, разработанной фирмой RSA Labs., для шифрования данных, передаваемых между телефоном 4 и сервером пользовательского интерфейса 6. Этот алгоритм представляет достаточный уровень безопасности и требует незначительных вычислительных ресурсов, что очень важно при использовании мобильных телефонов. Кроме того, по имеющимся данным в настоящее время разработчиками мобильных телефонов ведется работа по

включению реализации SSL в J2ME (Java 2 Micro Edition). Таким образом, можно ожидать, что через некоторое время (предположительно, через год) все телефоны, поддерживающие Java, будут изначально рассчитаны на работу по безопасному соединению через SSL Однако на ряде телефонов, обладающих достаточным объемом памяти и позволяющих установку приложений размером 200 Кб и более, уже сейчас имеется возможность обеспечить работу интерфейса системы безналичного расчета через SSL Среди подобных телефонов стоит выделить модель SonyEricsson P800. Стоит также отметить, что все PDA с функциями коммуникатора (например, Nokia 9210i Communicator) удовлетворяют этому условию, т. к. они поддерживают установку больших мидлетов (J2ME-приложений) и имеют более чем достаточный объем памяти.

Таким образом, с помощью подобного мобильного телефона или PDA пользователь сможет работать с сервером 1 авторизации платежей, используя шифрование по протоколу SSL на всех участках передачи данных. Большим достоинством этого варианта является то, что вся работа пользователя с системой является абсолютно независимой от оператора связи и его шлюза 5 (функцией оператора остается, конечно же, доставка пакетов, но их содержимое даже он не может узнать никаким образом).

Так же, как и в предыдущем случае (WAP 1.2.1/2.0), пароль пользователя узнать невозможно ни из сети, ни из самого телефона, если последний становится доступен злоумышленникам. Поэтому для аутентификации использование системного пароля пользователя здесь представляется достаточным. Следует также отметить, что рассмотренные выше механизмы обеспечения безопасности делают возможной надежную работу с системой безналичного расчета для пользователей с любыми телефонами, вообще способными работать с информацией, т.е. поддерживающими хотя бы стандарт WAP 1.1, (лишь совсем немногие из существующих моделей мобильных телефонов сейчас не удовлетворяют этому условию, и с развитием телекоммуникационных технологий доля таких моделей, несомненно, будет сокращаться). При этом, что очень важно, не требуется производить никаких изменений самих телефонов и SIM-карт. Это обеспечивает полную техническую независимость системы безналичного расчета как от производителей телефонов, так и от операторов мобильной связи и производителей SIM-карт.

Независимо от рассмотренных выше процедур аутентификации пользователей в предложенной системе безналичного расчета предусмотрен дополнительный механизм обеспечения безопасности совершения платежей, основанный на формировании сервером системы (сервером 1 авторизации платежей) для каждого совершаемого платежа уникального кода платежной операции, передаваемого на терминал 3 предполагаемого получателя платежа. Эту функцию выполняет блок 15 генерации и сравнения псевдослучайных кодов платежных операций, генерирующий псевдослучайный код (предпочтительно цифровой) в ответ на поступление из блока 12 работы с пользователями сигнала, характеризующего запрос пользователя на совершение платежа на счет конкретного получателя. Псевдослучайный код может генерироваться с использованием известных механизмов генерации псевдослучайных чисел, таких как ANSI X9.17 (ANSI85) и RSAREF 2.0 PRNG (RSA94).

В этом случае блок 15 генерации и сравнения псевдослучайных кодов платежных операций обращается к запоминающему устройству 14, в частности к области хранения данных о получателях платежей и их счетах, и вызывает данные, идентифицирующие терминал 3 указанного получателя платежа. Эти данные вместе с кодом платежной операции и идентификатором пользователя мобильного телефона (номером мобильного телефона) передаются в блок 11 работы с получателями платежей, который формирует для получателя платежа сообщение о запросе конкретного пользователя на совершение платежа на счет указанного получателя, причем это сообщение содержит код данной платежной операции и номер мобильного телефона пользователя, и передает это сообщение на терминал получателя платежей, как показано на фиг.3.

Одновременно на мобильный телефон 4 могут быть направлены условия вида платежа с сообщением о необходимости последующего подтверждения намерения совершить

платеж именно данному получателю платежа путем ввода кода платежной операции, который должен поступить от получателя платежа. Однако следует иметь в виду, что возможности осуществления изобретения не ограничены каким-либо определенным порядком выполнения этих процедур безопасности: автоматического отображения условий вида платежа на экране мобильного телефона 4 (основной механизм защиты) и передачи кода платежной операции по замкнутому контуру "сервер системы - терминал 3 получателя платежа - мобильный телефон 4 - сервер системы".

Получатель платежа передает данный код платежной операции пользователю, например, в виде SMS-сообщения, причем эта передача осуществляется в обход сервера 1 авторизации платежей, после чего пользователь вводит полученный код операции, поступающий через блок 12 работы с пользователями в блок 15 генерации и сравнения псевдослучайных кодов платежных операций, где происходит сравнение кода, полученного от пользователя мобильного телефона, с кодом, переданным на терминал 3 получателя платежа, и в случае совпадения указанных кодов в блок 13 работы с платежными операциями выдается сигнал разрешения на совершение платежа, инициирующий направление соответствующего поручения в сервер 2 банка.

Характерным примером реализации этого механизма безопасности является случай уплаты государственной пошлины за выдачу общегражданского или заграничного паспорта. Пользователь мобильного телефона видит на информационной доске объявление, что государственная пошлина может быть уплачена не только путем банковского перевода, но и через предложенную систему безналичного расчета. При этом указывается индекс данного вида платежей в системе. Пользователь мобильного телефона, являясь в этом случае получателем паспорта и плательщиком, а также будучи пользователем подобной системы, имеет возможность произвести уплату пошлины, не выходя из здания паспортного стола и не прибегая к использованию наличных денег или кредитных карт (что в государственных структурах не практикуется). Ему достаточно войти в систему (запустить соответствующее J2ME приложение или войти на страницу системы с помощью установленного на телефоне WAP-броузера; на большинстве телефонов имеется возможность настройки входа в систему единственным нажатием кнопки телефона) и ввести указанный на стенде индекс, который будет направлен в сервер 1 авторизации платежей. В ответ на введенный индекс блок 12 работы с пользователями передает на мобильный телефон 4 пользователя условия соответствующего вида платежа, и пользователь получает возможность просмотреть на экране телефона информацию о платеже (получатель - соответствующая государственная структура, назначение - оплата пошлины за оформление паспорта, также указывается конкретная фиксированная, то есть неизменяемая, сумма платежа). Проверив информацию о платеже, пользователь нажимает кнопку телефона, соответствующую оплате, и в сервер 1 авторизации платежей направляется подтвержденное платежное поручение, после чего блок 12 работы с пользователями формирует запрос на введение пароля или одноразового PIN-кода, а также направляет в блок 15 генерации и сравнения псевдослучайных кодов платежных операций команду на формирование уникального кода платежной операции и передачу этого кода через блок 11 работы с получателями платежей на терминал 3 оператора паспортной службы, с указанием фамилии, имени и отчества пользователя мобильного телефона. Далее пользователь вводит соответствующее числовое значение (например, из 4-х цифр), и в случае корректного ввода PIN-кода для завершения платежа далее запрашивается код платежной операции (также, скажем, 4 цифры), который может быть получен только от оператора терминала 3, например, во время собеседования.

Как не трудно видеть, описанная процедура оплаты довольно проста и позволяет сэкономить время плательщика (поскольку исключается необходимость похода в банк, ручного заполнения квитанции на перевод денег и стояния в очереди в банке). Кроме того, указанная схема исключает возможность мошенничества на основании подмены информации на стенде паспортного стола (т.е. указания другого индекса платежа и, соответственно, изменения получателя платежа). Подмена может быть обнаружена

плательщиком при просмотре информации о получателе платежа. И даже если плательщик отнесся к этой информации невнимательно, он все равно не сможет сделать перевод подобным мошенникам, т.к. не сможет ввести верный код платежной операции (если получателем платежа является не соответствующая государственная структура, то оператор терминала 3 не сможет получить код операции и передать его плательщику).

В предложенной системе безналичного расчета может быть предусмотрено ограниченное число получателей платежей, таких как операторы связи, для которых нет смысла использовать вышеописанное дополнительное подтверждение с помощью кодов платежных операций. Для таких платежей, ввиду их предполагаемого особенного высокого потока, могут быть выделены особые короткие индексы (например, только из 3-х цифр). При этом администратор системы должен быть уверен во всех таких получателях платежей и в том, что их индексы будут хорошо известны (и технологически не фальсифицируемыми; для оператора связи это обеспечено, т.к. при подключении пользователя оператор может предоставлять последнему брошюры с перечнем как специальных "служебных" номеров телефонов (как это уже делается сейчас), так и "служебных" индексов в системе описываемого типа для оплаты услуг этого оператора). При этом остальным получателям платежей выделяются индексы другого типа, которые невозможно спутать с предыдущими, например, их длина может быть не менее 5-ти символов (цифр). Именно для видов платежей последнего типа может быть предусмотрено обязательное использование дополнительного механизма кодов платежных операций. Для обеспечения приемлемой пропускной способности системы безналичного расчета (то есть исключения зависания в ней множества неподтвержденных платежей), а также из соображений безопасности, коду платежной операции может быть установлен ограниченный срок действия, по истечении которого указанный код аннулируют. Это может быть реализовано посредством сохранения кода в запоминающем устройстве сервера системы на заданный отрезок времени, с его последующим удалением.

Задачей вышеописанного механизма дополнительного подтверждения является защита от мошенничества или просто невнимательности или ошибки ввода: мошенники могут тем или иным образом подменить указание индекса вида платежа (например, в рассмотренном выше случае на стенде паспортного стола - вывеска с индексом платежа пошлины) для клиентов некоторой организации, а новый индекс будет соответствовать их собственному счету (описание платежа может быть любым, в том числе и точно таким же, как и у настоящего получателя, сумма может в точности совпадать, да и название получателя можно сделать похожим на название реальной организации). Кроме того, человек мог просто ошибиться и набрать неверный индекс, а затем невнимательно проверить назначение платежа.

Таким образом, когда пользователь первый раз подтвердил платеж (то есть, передал подтвержденное платежное поручение), получатель этого платежа может видеть через пользовательский интерфейс системы (реализованный, например, на языке Java (J2SE)) на своем терминале 3 подтверждение инициации платежа с указанием номера плательщика в системе и некоторых его данных (например, ФИО).

До передачи кода платежной операции с мобильного телефона в сервер системы за пользователем мобильного телефона может быть сохранено право отмены платежа посредством направления соответствующего сообщения в сервер системы. В любом случае, до тех пор, пока платеж является отменяемым, информация о нем в сервер 2 банка не передается. Платежное поручение передается из сервера 1 авторизации платежей в сервер банка только тогда, когда есть полная уверенность, что платеж должен быть совершен (т.е. для самого банка все платежи могут считаться неотменяемыми и, соответственно, проводиться без задержек, с максимально возможной скоростью).

Как было отмечено выше, условия вида платежа могут включать в себя фиксированное значение суммы платежа или интервал допустимых значений. Интервал значений целесообразно использовать для предоплаты услуг, например, оператора связи, т.е. когда пользователь решает, сколько платить. При этом проверка попадания введенного

значения в заданный интервал предпочтительно проводится до передачи подтвержденного платежного поручения. Фиксированные значения могут применяться для оплаты государственных пошлин, штрафов, причем в случае небольших размеров таких платежей сумма платежа может не входить в состав условий вида платежа, автоматически передаваемых на мобильный телефон 4 пользователя в ответ на его запрос.

Как было отмечено ранее, в качестве платежного средства пользователя мобильного телефона может использоваться зарегистрированная в системе кредитная карта. При этом платеж производится через сервер банка, который подключен к системе и занимается эквайерингом кредитных карт (т.е. авторизация пользователя при использовании карты, получение денег от компании-владельца соответствующей системы, перевод денег на счет получателя). В этом случае сам пользователь (плательщик) не имеет к указанному банку никакого отношения. В этом случае достаточно одного такого банка, работающего с системой, чтобы через систему могли платить, по крайней мере, все владельцы кредитных карт.

При этом изобретение позволяет преодолеть недостатки, присущие кредитным картам. В данном случае пользователю более не нужно носить с собой кредитную карту, рискуя ее потерять (в случае ее утери, в отличие от утери телефона, появляется реальная опасность потерять деньги, доступные через карту). Номер карты зарегистрирован в сервере 1 авторизации платежей и никуда, кроме банка, не передается, при этом платежи совершаются, и коммерческие предложения выставляются, по-прежнему на основе идентификатора пользователя в системе.

Формула изобретения

1. Способ совершения платежных операций пользователями мобильных устройств электронной связи посредством системы безналичного расчета, согласно которому формируют и запоминают в сервере указанной системы условия вида платежа, включающие в себя по меньшей мере идентификацию получателя платежей, назначение, общее для всех платежей данного вида, и условие на сумму платежа, причем конкретному виду платежа присваивают уникальный индекс, который перед совершением платежа вводят посредством мобильного устройства электронной связи, и в соответствии с введенным индексом передают в сервер системы запрос на совершение платежа, отличающийся тем, что в ответ на указанный запрос из сервера системы на мобильное устройство электронной связи передают условия указанного вида платежа, включающие в себя по меньшей мере назначение и получателя платежа, с отображением этих условий на экране мобильного устройства электронной связи, после чего с мобильного устройства электронной связи в сервер системы передают подтвержденное платежное поручение, после получения которого посредством сервера системы генерируют псевдослучайный код совершаемой платежной операции и передают его на терминал получателя платежа, из терминала получателя платежа указанный код передают непосредственно пользователю, после чего с мобильного устройства электронной связи вводят и передают этот код в сервер системы, в котором сравнивают значения кода платежной операции, полученного от пользователя, и значение кода платежной операции, переданного на терминал получателя платежа, и в случае совпадения указанных значений посредством сервера системы инициируют платеж путем обращения к серверу соответствующей платежной организации.

2. Способ по п.1, отличающийся тем, что мобильным устройством электронной связи является мобильный телефон или карманный компьютер (PDA), причем соединение между мобильным устройством электронной связи и сервером системы устанавливают через шлюз оператора мобильной связи.

3. Способ по п.1, отличающийся тем, что передаваемые на мобильное устройство электронной связи условия вида платежа включают в себя условие на сумму платежа, которое представляет собой фиксированное значение, причем при передаче подтвержденного платежного поручения это значение не подлежит изменению.

4. Способ по п.1, отличающийся тем, что передаваемые на мобильное устройство

электронной связи условия вида платежа включают в себя условие на сумму платежа, представляющее собой интервал допустимых значений, при этом перед передачей подтвержденного платежного поручения с мобильного устройства электронной связи вводят конкретное значение суммы платежа, при этом проверяют нахождение введенного значения суммы платежа в указанном интервале.

5. Способ по п.4, отличающийся тем, что видом платежа является предоплата услуги, в частности услуги оператора мобильной связи.

6. Способ по п.4, отличающийся тем, что видом платежа является взнос в благотворительный фонд.

7. Способ по любому из пп.1-6, отличающийся тем, что условия вида платежа включают в себя любые из следующих элементов: комментарий получателя платежа, детальное описание компании-получателя, детальное описание назначения платежа, изображения, трехмерные модели, видеоролики, звуковые сообщения.

8. Способ по п.1, отличающийся тем, что индекс вида платежа сообщают пользователю мобильного устройства электронной связи с использованием средств массовой рекламы и/или информационных материалов получателей платежей.

9. Способ по п.8, отличающийся тем, что в качестве средств массовой рекламы используют рекламные щиты, средства передвижной наглядной рекламы, рекламные издания и публикации, телевизионную рекламу, при этом индекс вида платежа указывают вместе с обозначением системы безналичного расчета.

10. Способ по любому из пп.1-6, 8 или 9, отличающийся тем, что с запросом на совершение платежа или подтвержденным платежным поручением в сервер системы передают данные платежного средства пользователя, поддерживаемого указанной платежной организацией, и/или хранят эти данные в запоминающем устройстве сервера системы.

11. Способ по п.10, отличающийся тем, что платежной организацией является банк, при этом платежное средство пользователя представляет собой счет в указанном банке и/или кредитную карту.

12. Способ по п.10, отличающийся тем, что платежной организацией является центр обслуживания кредитных карт, при этом платежное средство пользователя представляет собой кредитную карту.

13. Способ по п.10, отличающийся тем, что платежной организацией является система электронных платежей, при этом платежное средство пользователя представляет собой лицевой счет пользователя в указанной системе.

14. Способ по любому из пп.1-6, 8 или 9, отличающийся тем, что индекс вида платежа состоит только из цифр.

15. Способ по п.1, отличающийся тем, что коду платежной операции устанавливают ограниченный срок действия, по истечении которого указанный код аннулируют.

16. Способ по п.1, отличающийся тем, что после генерации кода платежной операции его сохраняют в запоминающем устройстве сервера системы на заданный отрезок времени, после чего удаляют.

17. Способ по п.1, отличающийся тем, что до передачи кода платежной операции с мобильного устройства электронной связи в сервер системы за пользователем мобильного устройства электронной связи сохраняют право отмены платежа посредством направления соответствующего сообщения в сервер системы.

18. Способ по любому из пп.1-6,8, 9 или 15-17, отличающийся тем, что дополнительно проверяют полномочия пользователя мобильного устройства электронной связи на совершение платежа посредством ввода фиксированного пароля и/или одноразового кода аутентификации пользователя, в частности персонального идентификационного номера (PIN-кода), на мобильном устройстве электронной связи.

19. Способ по п.18, отличающийся тем, что используют мобильное устройство электронной связи с поддержкой языка J2ME, при этом введенный пользователем фиксированный пароль или одноразовый код аутентификации передают в сервер системы

через связанный с ним дополнительный сервер пользовательского интерфейса, поддерживающий работу с приложениями, написанными на языке J2ME.

20. Способ по п.18, отличающийся тем, что используют мобильное устройство электронной связи с поддержкой протокола WAP, при этом введенный пользователем фиксированный пароль или одноразовый код аутентификации передают в сервер системы через связанный с ним дополнительный сервер пользовательского интерфейса, поддерживающий обмен информацией с мобильными устройствами электронной связи на языке WML.

21. Способ по любому из пп.1-6, 8, 9 или 15-17, отличающийся тем, что индекс вида платежа соответствует индексу конкретного товара в базе данных товаров.

22. Способ по п.21, отличающийся тем, что базу данных товаров поддерживают на сервере пользовательского интерфейса, причем пользователю мобильного устройства электронной связи предоставляют доступ к указанной базе данных посредством соответствующего WAP- или J2ME-интерфейса.

23. Способ по п.1, отличающийся тем, что код платежной операции передают на терминал получателя платежа вместе с идентификацией пользователя, в частности с указанием номера его мобильного телефона.

24. Способ по п.23, отличающийся тем, что видом платежа является уплата государственной пошлины за выдачу общегражданского или заграничного паспорта, при этом код платежной операции передают на терминал оператора паспортной службы с указанием фамилии, имени и отчества пользователя мобильного устройства электронной связи, а передачу этого кода пользователю осуществляют непосредственно через оператора терминала паспортной службы.

25. Компьютерная система безналичного расчета для совершения платежных операций пользователями мобильных устройств электронной связи, включающая в себя сервер авторизации платежей, связанный с мобильными устройствами электронной связи, сервером по меньшей мере одной платежной организации и терминалом по меньшей мере одного получателя платежей, причем сервер авторизации платежей содержит блок работы с получателями платежей, связанный с указанным терминалом получателя платежа с возможностью формирования условий видов платежей; блок работы с пользователями; блок работы с платежными операциями, связанный с сервером платежной организации; блок генерации и сравнения псевдослучайных кодов платежных операций, вход которого связан с блоком работы с пользователями, один выход - с блоком работы с получателями платежей, а другой выход - с блоком работы с платежными операциями; и запоминающее устройство, содержащее по меньшей мере область хранения данных о пользователях и их платежных средствах, область хранения условий видов платежей и область хранения кодов платежных операций, связанную с блоком генерации и сравнения псевдослучайных кодов платежных операций, причем запоминающее устройство связано с блоком работы с получателями платежей и блоком работы с платежными операциями, а блок работы с пользователями связан с мобильными устройствами электронной связи, блоком работы с платежными операциями и запоминающим устройством и выполнен с возможностью вызова условий вида платежа из запоминающего устройства и их передачи на мобильное устройство электронной связи при получении от указанного мобильного устройства запроса на совершение платежа, а также последующего приема от указанного мобильного устройства подтвержденного платежного поручения и его передачи в блок работы с платежными операциями.

26. Система по п. 25, отличающаяся тем, что запоминающее устройство сервера авторизации платежей содержит область хранения данных о получателях платежей и их счетах, связанную с блоком работы с получателями платежей.

27. Система по п. 25, отличающаяся тем, что она содержит дополнительный сервер пользовательского интерфейса, связывающий сервер авторизации платежей с мобильными устройствами электронной связи.

28. Система по п. 27, отличающаяся тем, что сервер пользовательского интерфейса

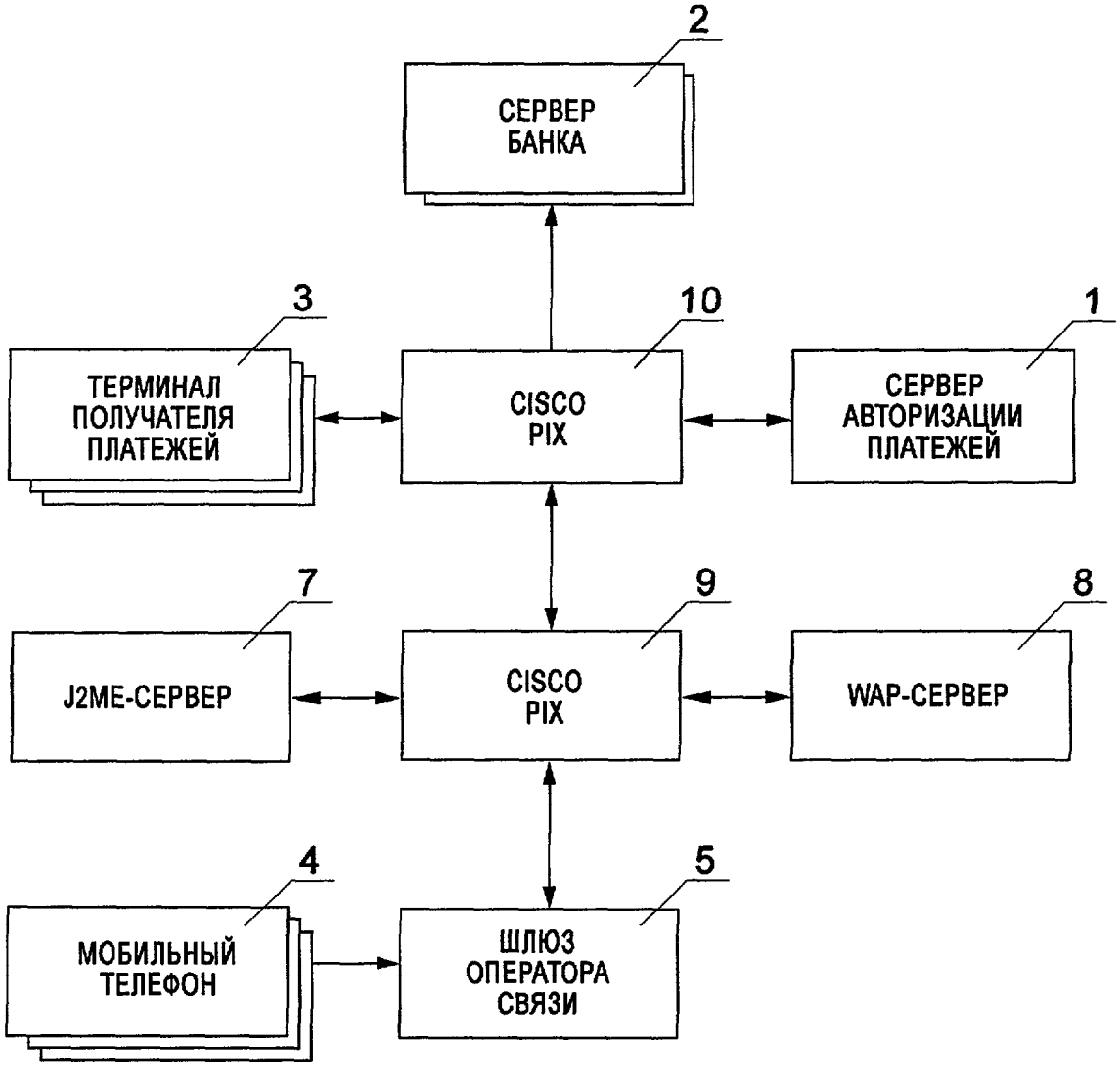
поддерживает работу с приложениями, написанными на языке J2ME, и/или обмен информацией с мобильными устройствами электронной связи на языке WML по протоколу WAP.

29. Система по п. 27, отличающаяся тем, что мобильное устройство электронной связи имеет возможность связи с сервером пользовательского интерфейса по каналу безопасного соединения, в частности с применением шифрования по одному из протоколов RC6, WTLS или SSL.

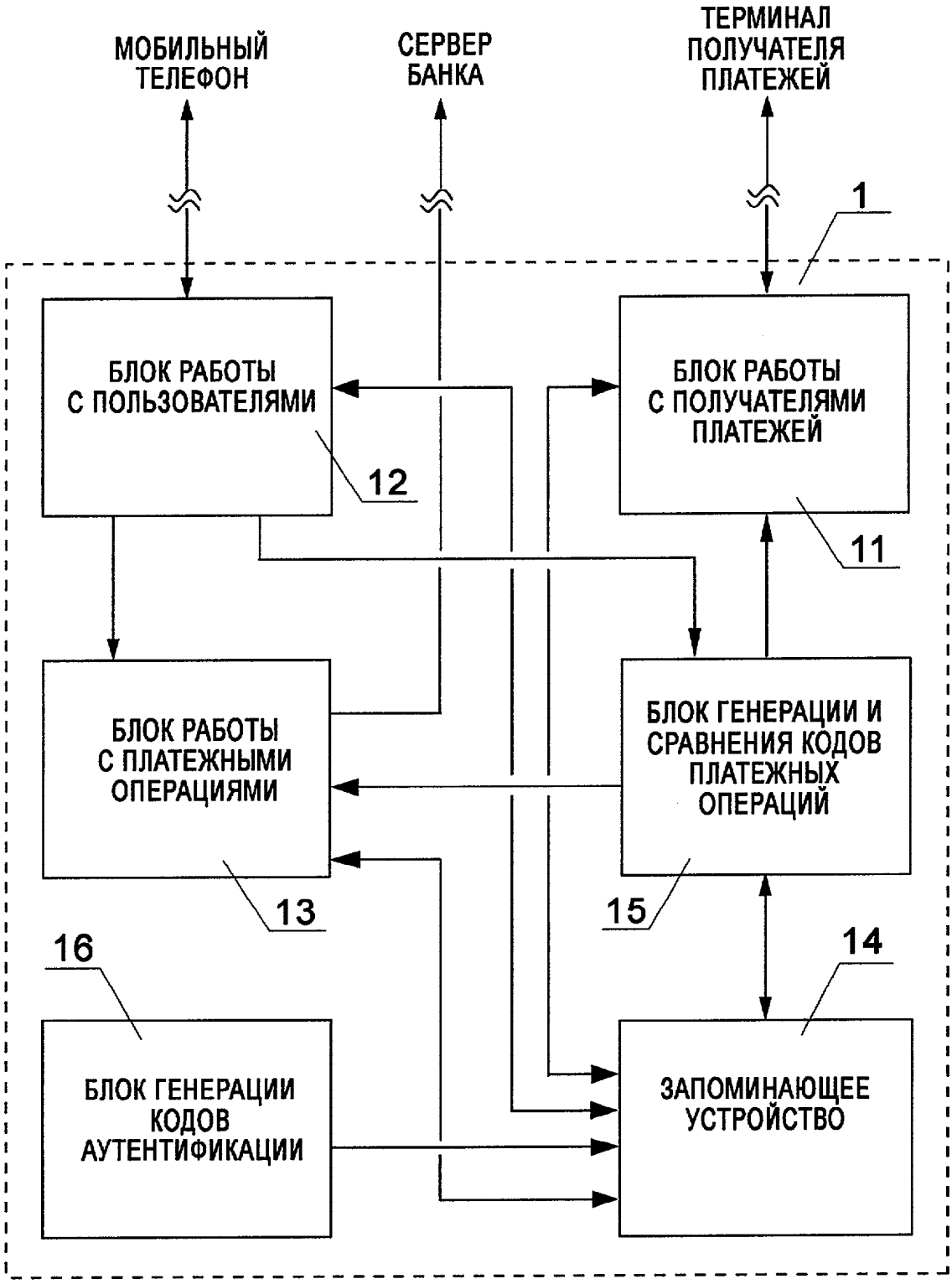
30. Система по любому из пп. 27-29, отличающаяся тем, что сервер авторизации платежей связан с терминалом получателя платежа, сервером платежной организации и сервером пользовательского интерфейса каналами безопасного соединения, в частности, с применением шифрования по протоколу SSL.

31. Система по п.27, отличающаяся тем, что сервер авторизации платежей связан с сервером пользовательского интерфейса и терминалами получателей платежей через устройство сетевой защиты.

32. Система по любому из пп. 25-29 или 31, отличающаяся тем, что сервер авторизации платежей содержит блок генерации кодов аутентификации, а запоминающее устройство сервера авторизации платежей содержит область хранения кодов аутентификации, связанную с блоком работы с пользователями, причем блок генерации кодов аутентификации связан с указанной областью хранения кодов аутентификации.


2
СЕРВЕР БАНКА
3
ТЕРМИНАЛ ПОЛУЧАТЕЛЯ ПЛАТЕЖЕЙ
10
CISCO PIX
1
СЕРВЕР АВТОРИЗАЦИИ ПЛАТЕЖЕЙ
7
J2ME-СЕРВЕР
9
CISCO PIX
8
WAP-СЕРВЕР
4
МОБИЛЬНЫЙ ТЕЛЕФОН
5
ШЛЮЗ ОПЕРАТОРА СВЯЗИ

Фиг.2


МОБИЛЬНЫЙ ТЕЛЕФОН
СЕРВЕР БАНКА
ТЕРМИНАЛ ПОЛУЧАТЕЛЯ ПЛАТЕЖЕЙ
1
БЛОК РАБОТЫ С ПОЛЬЗОВАТЕЛЯМИ
12
БЛОК РАБОТЫ С ПОЛУЧАТЕЛЯМИ ПЛАТЕЖЕЙ
11
БЛОК РАБОТЫ С ПЛАТЕЖНЫМИ ОПЕРАЦИЯМИ
13
БЛОК ГЕНЕРАЦИИ И СРАВНЕНИЯ КОДОВ ПЛАТЕЖНЫХ ОПЕРАЦИЙ
15
16
14
БЛОК ГЕНЕРАЦИИ КОДОВ АУТЕНТИФИКАЦИИ
ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО

Фиг.3