



УКРАЇНА

(19) UA (11) 40645 (13) C2

(51) 7 G06F17/60//G06F157:00

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА ВІНАХІД

**(54) СИСТЕМА ДЛЯ ВІДКРИТОГО ЕЛЕКТРОННОГО БІЗНЕСУ, ДОВІРЕНІ АГЕНТИ, ЩО У НІЙ ВИКОРИСТОВУЮТЬСЯ, І СПОСІБ ЗДІЙСНЕННЯ ВІДКРИТОГО ЕЛЕКТРОННОГО БІЗНЕСУ ЗА ДОПОМОГОЮ ТАКОЇ СИСТЕМИ**

(21) 96103989

(22) 28.03.1995

(24) 15.08.2001

(31) 08/234.461

(32) 28.04.1994

(33) US

(86) PCT/US95/03831, 28.03.1995

(46) 15.08.2001, Бюл. № 7, 2001 р.

(72) Розен Шолом С., US

(73) СІТІБЕНК, Н.А., US

(56) 6. WO 93/10503 A1, 27.05.93

7. WO 91/9370 A1, 27.06.91

8. US 4977595 A, 11.12.90

9. RU 2022350 C1, 30.10.94

10. RU 2024930 C1, 15.12.94

(57) 1. Система для открытого электронного бизнеса, содержащая первый и второй денежные модули, **отличающаяся** тем, что в ней предусмотрены доверенный агент покупателя и доверенный агент продавца, причем доверенный агент продавца выполнен с возможностью установления первого криптографически безопасного сеанса связи с доверенным агентом покупателя и передачи электронного товара при первом криптографически безопасном сеансе связи доверенному агенту покупателя, а также с возможностью предоставления второму денежному модулю второй информации о платеже, доверенный агент покупателя выполнен с возможностью предоставления первому денежному модулю первой информации о платеже, первый денежный модуль выполнен с возможностью осуществления безопасной связи с доверенным агентом покупателя и передачи при втором криптографически безопасном сеансе связи второму денежному модулю электронных денег в количестве, соответствующем первой и второй информации о платеже, а также с возможностью информирования доверенного агента покупателя об успешной передаче электронных денег и второй денежный модуль выполнен с возможностью осуществления безопасной связи с доверенным агентом продавца и установления второго криптографически безопасного сеанса связи с первым денежным модулем, а также с возможностью информирования доверенного агента продавца об успешном получении электронных денег.

2. Система по п.1, **отличающаяся** тем, что первая информация о платеже содержит сумму платежа,

а вторая информация о платеже содержит данные проверки суммы платежа.

3. Система по п.1, **отличающаяся** тем, что вторая информация о платеже содержит суммы платежа, а первая информация о платеже содержит данные проверки суммы платежа.

4. Система по п.1, **отличающаяся** тем, что электронный товар содержит электронный билет.

5. Система по п.1, **отличающаяся** тем, что электронный билет содержит следующие разделы: идентификатор, компоненты, подпись эмитента, сертификат эмитента, предысторию передачи и подписи отправителей.

6. Система по п.5, **отличающаяся** тем, что электронный билет является удостоверяющим билетом.

7. Система по п.5, **отличающаяся** тем, что электронный билет является транспортным билетом.

8. Система по п.5, **отличающаяся** тем, что электронный билет является билетом на мероприятие.

9. Система по п.5, **отличающаяся** тем, что электронный билет является билетом на услуги связи.

10. Система по п.5, **отличающаяся** тем, что электронный билет является билетом физического объекта.

11. Система по п.1, **отличающаяся** тем, что электронный товар содержит зашифрованный электронный объект и связанный с ним электронный билет расшифровки.

12. Система по п.11, **отличающаяся** тем, что электронный билет расшифровки содержит следующие разделы: идентификатор, компоненты, подпись эмитента, сертификат эмитента, предысторию передачи и подписи отправителей.

13. Система по п.1, **отличающаяся** тем, что доверенный агент покупателя и первый денежный модуль образуют устройство транзакций покупателя, в котором предусмотрены первый центральный процессор и первая шина, через которую доверенный агент покупателя и первый денежный модуль соединены с первым центральным процессором.

14. Система по п.1, **отличающаяся** тем, что доверенный агент продавца и второй денежный модуль образуют устройство транзакций продавца, в котором предусмотрены второй центральный процессор и вторая шина, через которую доверенный агент продавца и второй денежный модуль соединены со вторым центральным процессором.

15. Система по п.1, **отличающаяся** тем, что доверенные агенты продавца и покупателя содержат прикладные программы.

16. Система по п.1, **отличающаяся** тем, что первый и второй денежные модули содержат прикладные программы.

17. Доверенный агент покупателя для использования при безопасной покупке электронного товара с помощью доверенного агента продавца и первого и второго денежных модулей, способных устанавливать второй криптографически безопасный сеанс связи, **отличающийся** тем, что он содержит процессор, выполненный с возможностью установления первого криптографически безопасного сеанса связи с доверенным агентом продавца, с возможностью осуществления безопасной связи с первым денежным модулем, относящимся к доверенному агенту покупателя, с возможностью получения электронного товара от доверенного агента продавца и условного его сохранения при первом криптографически безопасном сеансе связи и с возможностью предоставления информации о платеже первому денежному модулю, который выполнен с возможностью передачи при втором криптографически безопасном сеансе связи электронных денег в количестве, соответствующем информации о платеже, второму денежному модулю, относящемуся к доверенному агенту продавца, а также с возможностью информирования доверенного агента покупателя об успешной передаче электронных денег.

18. Доверенный агент покупателя по п.17, **отличающийся** тем, что информация о платеже содержит сумму платежа.

19. Доверенный агент покупателя по п.17, **отличающийся** тем, что информация о платеже содержит данные проверки суммы платежа.

20. Доверенный агент покупателя по п.17, **отличающийся** тем, что электронный товар содержит электронный билет.

21. Доверенный агент покупателя по п.17, **отличающийся** тем, что электронный товар содержит зашифрованный электронный объект и электронный билет расшифровки, способный расшифровать зашифрованный электронный объект.

22. Доверенный агент покупателя по п.17, **отличающийся** тем, что он и первый денежный модуль содержат прикладные программы, выполняемые разными процессорами, защищенными от несанкционированного доступа.

23. Доверенный агент покупателя по п.17, **отличающийся** тем, что он и первый денежный модуль содержат прикладные программы, выполняемые одним и тем же защищенным от несанкционированного доступа процессором.

24. Доверенный агент продавца для использования при безопасной продаже электронного товара с помощью доверенного агента покупателя и первого и второго денежных модулей, способных устанавливать второй криптографически безопасный сеанс связи, **отличающийся** тем, что он содержит процессор, выполненный с возможностью установления первого криптографически безопасного сеанса связи с доверенным агентом покупателя, с возможностью осуществления безопасной связи со вторым денежным модулем, относящимся к доверенному агенту продавца, с возможно-

стью передачи электронного товара при первом криптографически безопасном сеансе связи доверенному агенту покупателя и с возможностью предоставления информации о платеже второму денежному модулю, который выполнен с возможностью приема при втором криптографически безопасном сеансе связи электронных денег в количестве, соответствующем информации о платеже, от первого денежного модуля, а также с возможностью информирования доверенного агента продавца об успешном получении электронных денег.

25. Доверенный агент продавца по п.24, **отличающийся** тем, что информация о платеже содержит сумму платежа.

26. Доверенный агент продавца по п.24, **отличающийся** тем, что информация о платеже содержит данные проверки суммы платежа.

27. Доверенный агент продавца по п.24, **отличающийся** тем, что электронный товар содержит электронный билет.

28. Доверенный агент продавца по п.27, **отличающийся** тем, что электронный товар содержит зашифрованный электронный объект и электронный билет расшифровки, способный расшифровать зашифрованный электронный объект.

29. Доверенный агент продавца по п.24, **отличающийся** тем, что он и второй денежный модуль содержат прикладные программы, выполняемые разными процессорами, защищенными от несанкционированного доступа.

30. Доверенный агент продавца по п.24, **отличающийся** тем, что он и второй денежный модуль содержат прикладные программы, выполняемые одним и тем же защищенным от несанкционированного доступа процессором.

31. Способ безопасного обмена электронного билета и электронных денег с использованием доверенного агента покупателя, первого денежного модуля, доверенного агента продавца и второго денежного модуля, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают первый криптографически безопасный сеанс связи, при первом криптографически безопасном сеансе связи передают электронный билет от доверенного агента продавца доверенному агенту покупателя, который условно сохраняет электронный билет, между первым денежным модулем и вторым денежным модулем устанавливают второй криптографически безопасный сеанс связи, осуществляют безопасное предоставление доверенным агентом покупателя первому денежному модулю первой информации о платеже, осуществляют безопасное предоставление доверенным агентом продавца второму денежному модулю второй информации о платеже, при втором криптографически безопасном сеансе связи передают электронные деньги в количестве, соответствующем первой и второй информации о платеже, от первого денежного модуля ко второму денежному модулю, который условно сохраняет электронные деньги, с помощью первого денежного модуля осуществляют фиксацию транзакции и безопасное информирование доверенного агента покупателя об успешной передаче электронных денег, с помощью второго денежного модуля осуществляют фиксацию

транзакции, после чего сохранение электронных денег более не является условным, и безопасное информирование доверенного агента продавца об успешном получении электронных денег, осуществляют фиксацию транзакции с помощью доверенного агента покупателя, после чего сохранение электронного товара более не является условным, и осуществляют фиксацию транзакции с помощью доверенного агента продавца.

32. Способ по п.31, **отличающийся** тем, что после безопасного предоставления доверенным агентом покупателя первому денежному модулю первой информации о платеже, которая содержит сумму платежа, и перед безопасным предоставлением доверенным агентом продавца второму денежному модулю второй информации о платеже, которая содержит данные проверки суммы платежа, дополнительно передают от первого денежного модуля при втором криптографически безопасном сеансе связи сумму платежа ко второму денежному модулю и осуществляют безопасное информирование с помощью второго денежного модуля доверенного агента продавца о сумме платежа.

33. Способ по п.31, **отличающийся** тем, что после безопасного предоставления доверенным агентом покупателя первому денежному модулю первой информации о платеже, которая содержит данные проверки суммы платежа, и перед безопасным предоставлением доверенным агентом продавца второму денежному модулю второй информации о платеже, которая содержит сумму платежа, дополнительно передают от второго денежного модуля при втором криптографически безопасном сеансе связи сумму платежа к первому денежному модулю и осуществляют безопасное информирование с помощью первого денежного модуля доверенного агента покупателя о сумме платежа.

34. Способ по п.31, **отличающийся** тем, что после передачи электронного билета доверенному агенту покупателя электронный билет для проверки его правильности обрабатывают в доверенном агенте покупателя.

35. Способ по п.31, **отличающийся** тем, что для расшифровки зашифрованного электронного объекта используют электронный билет, представляющий собой электронный билет расшифровки.

36. Способ по п.31, **отличающийся** тем, что фиксация транзакции с помощью первого и второго денежных модулей и безопасное информирование доверенного агента продавца или доверенного агента покупателя заключаются в том, что от второго денежного модуля передают сообщение "Готовность к фиксации транзакции" к первому денежному модулю при втором криптографически безопасном сеансе связи, с помощью первого денежного модуля обновляют первый журнал транзакций и информируют доверенного агента покупателя об успешной передаче электронных денег и с помощью второго денежного модуля обновляют второй журнал транзакций и осуществляют безопасное информирование доверенного агента продавца об успешном получении электронных денег.

37. Способ по п.31, **отличающийся** тем, что фиксация транзакции с помощью доверенного агента покупателя, доверенного агента продавца, первого денежного модуля и второго денежного мо-

дуля заключается в том, что транзакцию записывают в журнал транзакций, после чего доверенные агенты покупателя и продавца или первый и второй денежные модули не могут более прекратить транзакцию путем возврата в первоначальное состояние.

38. Способ безопасного обмена электронного билета и электронных денег при помощи доверенного агента покупателя, первого денежного модуля, доверенного агента продавца и второго денежного модуля, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают первый криптографически безопасный сеанс связи, между первым денежным модулем и вторым денежным модулем устанавливают второй криптографически безопасный сеанс связи, с помощью доверенного агента покупателя осуществляют безопасное предоставление первой информации о платеже первому денежному модулю, с помощью доверенного агента продавца осуществляют безопасное предоставление второй информации о платеже второму денежному модулю, при втором криптографически безопасном сеансе связи передают от первого денежного модуля электронные деньги в количестве, соответствующем первой и второй информации о платеже, ко второму денежному модулю, который условно сохраняет эти электронные деньги, от доверенного агента продавца передают электронный билет при первом криптографически безопасном сеансе связи к доверенному агенту покупателя, который условно сохраняет этот электронный билет, осуществляют безопасную передачу команды от доверенного агента покупателя к первому денежному модулю на фиксацию транзакции, с помощью первого денежного модуля осуществляют фиксацию транзакции и информирование доверенного агента покупателя об успешной передаче электронных денег, с помощью второго денежного модуля осуществляют фиксацию транзакции, после чего сохранение электронных денег более не является условным, и безопасное информирование доверенного агента продавца об успешном получении электронных денег, осуществляют фиксацию транзакции с помощью доверенного агента покупателя, после чего сохранение электронного билета более не является условным, и осуществляют фиксацию транзакции с помощью доверенного агента продавца.

39. Способ осуществления транзакции платежа на основе проверки полномочий с использованием защищенного от несанкционированного доступа доверенного агента покупателя и защищенного от несанкционированного доступа доверенного агента продавца, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают криптографически безопасный сеанс связи, при этом доверенный агент покупателя и доверенный агент продавца обмениваются подписанными в цифровом виде сертификатами доверенных агентов, каждый из которых содержит идентификатор доверенного агента, от доверенного агента продавца передают электронный товар доверенному агенту покупателя при криптографически безопасном сеансе связи, при этом доверенный агент покупателя услов-

но сохраняет электронный товар, с помощью доверенного агента покупателя проверяют электронный товар, с помощью доверенного агента покупателя передают платежное удостоверение к доверенному агенту продавца при криптографически безопасном сеансе связи, причем платежное удостоверение включает идентификатор принимающего доверенного агента, с помощью доверенного агента продавца проверяют платежное удостоверение, при этом идентификатор доверенного агента из сертификата доверенного агента покупателя сравнивается с идентификатором принимающего доверенного агента, от доверенного агента продавца посылают платежное удостоверение и цену, соответствующую электронному товару, в сеть проверки полномочий для проверки полномочий на осуществление платежа, с помощью доверенного агента продавца получают проверку полномочий на осуществление платежа, от доверенного агента продавца посылают сообщение о проверке полномочий на осуществление платежа к доверенному агенту покупателя при криптографически безопасном сеансе связи с последующей фиксацией транзакции платежа с помощью доверенного агента продавца на основе проверки полномочий и осуществляют фиксацию транзакции платежа с помощью доверенного агента покупателя на основе проверки полномочий, после чего наличие электронного товара более не является условным.

40. Способ по п.39, **отличающийся** тем, что доверенные агенты покупателя и продавца записывают в журнал транзакций информацию, которая безусловно сохраняется при осуществлении фиксаций транзакции.

41. Способ по п.39, **отличающийся** тем, что после установления криптографически безопасного сеанса связи от доверенного агента продавца посылают удостоверение продавца доверенному агенту покупателя и обрабатывают с помощью доверенного агента покупателя это удостоверение продавца для подтверждения его действительности.

42. Способ по п.39, **отличающийся** тем, что при осуществлении фиксаций транзакции доверенным агентом покупателя и доверенным агентом продавца записывают транзакции в журнал транзакций, после чего доверенные агенты продавца и покупателя не могут прекратить транзакцию путем возврата в первоначальное состояние.

43. Способ предъявления электронного билета на услуги с использованием доверенного агента покупателя, первого центрального процессора, доверенного агента продавца и второго центрального процессора, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают криптографически безопасный сеанс связи, с помощью первого центрального процессора осуществляют информирование доверенного агента покупателя об электронном билете, выбранном для предъявления, от доверенного агента покупателя посылают копию электронного билета доверенному агенту продавца при криптографически безопасном сеансе связи, с помощью доверенного агента продавца проверяют действительность электронного билета, от доверенного агента продавца переда-

ют указание ко второму центральному процессору на предоставление услуг, определяемых электронным билетом, с помощью доверенного агента продавца уведомляют доверенного агента покупателя при криптографически безопасном сеансе связи об использовании электронного билета, с помощью второго центрального процессора осуществляют информирование доверенного агента продавца о том, что услуги были предоставлены, от доверенного агента продавца посылают новое значение билета доверенному агенту покупателя, с помощью доверенного агента покупателя осуществляют маркирование билета как неиспользуемого и обновляют значение билета, осуществляют фиксацию транзакции доверенным агентом покупателя и осуществляют фиксацию транзакции доверенным агентом продавца.

44. Способ передачи электронного билета от первого доверенного агента второму доверенному агенту, **отличающийся** тем, что между первым доверенным агентом и вторым доверенным агентом устанавливают криптографически безопасный сеанс связи, с помощью первого доверенного агента переподписывают электронный билет путем добавления информации о передаче к разделу предыстории передачи электронного билета и добавления цифровой подписи к разделу подписей отправителей электронного билета, от первого доверенного агента посылают переподписанный электронный билет ко второму доверенному агенту при криптографически безопасном сеансе связи, с помощью второго доверенного агента проверяют действительность переподписанного электронного билета, от второго доверенного агента посылают подтверждающее сообщение к первому доверенному агенту при криптографически безопасном сеансе связи, от первого доверенного агента посылают сообщение второму доверенному агенту, и после получения подтверждающего сообщения осуществляют фиксацию транзакции с помощью первого доверенного агента и после приема сообщения осуществляют фиксацию транзакции с помощью второго доверенного агента, причем в случае, если транзакция передачи является неудачной, то первый и второй доверенные агенты возвращаются в исходное состояние посредством устройств прекращения транзакции.

45. Способ по п.44, **отличающийся** тем, что после получения подтверждающего сообщения уничтожают электронный билет с помощью первого доверенного агента.

46. Способ приобретения электронного удостоверения с использованием доверенного агента покупателя, доверенного агента уполномоченного лица и центрального процессора, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом уполномоченного лица устанавливают первый криптографически безопасный сеанс связи, от центрального процессора посылают информацию об удостоверении к доверенному агенту уполномоченного лица, с помощью доверенного агента уполномоченного лица создают электронное удостоверение, содержащее информацию об удостоверении, цифровую подпись и сертификат, электронное удостоверение посылают доверенному агенту покупателя при



первом криптографически безопасном сеансе связи, с помощью доверенного агента покупателя проверяют действительность электронного удостоверения, осуществляют фиксацию транзакции с помощью доверенного агента покупателя и осуществляют фиксацию транзакции с помощью доверенного агента уполномоченного лица.

47. Способ по п.46, **отличающийся** тем, что доверенному агенту покупателя при первом криптографически безопасном сеансе связи посылают сумму платежа, между первым денежным модулем, относящимся к доверенному агенту покупателя, и вторым денежным модулем, относящимся к доверенному агенту уполномоченного лица, устанавливают второй криптографически безопасный сеанс связи и от первого денежного модуля передают ко второму денежному модулю электронные деньги в сумме, соответствующей сумме платежа.

48. Способ по п.46, **отличающийся** тем, что при первом криптографически безопасном сеансе связи доверенному агенту покупателя посылают сумму платежа, от доверенного агента покупателя посылают платежное удостоверение к доверенному агенту уполномоченного лица при первом криптографически безопасном сеансе связи, с помощью доверенного агента уполномоченного лица проверяют действительность платежного удостоверения, посылают в сеть проверки полномочий карт сумму платежа и платежное удостоверение, с помощью доверенного агента уполномоченного лица получают сообщение о том, что платеж разрешен, и от доверенного агента уполномоченного лица посылают сообщение о проверке полномочий на осуществление платежа к доверенному агенту покупателя.

49. Способ по п.46, **отличающийся** тем, что доверенный агент покупателя и доверенный агент уполномоченного лица записывают в журналы транзакций информацию, которая после фиксации транзакции безусловно сохраняется этими доверенными агентами.

50. Способ дистанционного продления электронного удостоверения с использованием доверенного агента покупателя и доверенного агента уполномоченного лица, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом уполномоченного лица устанавливают первый криптографически безопасный сеанс связи, от доверенного агента покупателя посылают электронное удостоверение к доверенному агенту уполномоченного лица при первом криптографически безопасном сеансе связи для дистанционного продления, с помощью доверенного агента уполномоченного лица проверяют действительность электронного удостоверения, с помощью доверенного агента уполномоченного лица создают обновленное электронное удостоверение, содержащее обновленную информацию удостоверения, цифровую подпись и сертификат, обновленное электронное удостоверение посылают к доверенному агенту покупателя при первом криптографически безопасном сеансе связи, с помощью доверенного агента покупателя проверяют действительность обновленного электронного удостоверения, осуществляют фиксацию транзакции с помощью доверенного агента

покупателя и осуществляют фиксацию транзакции с помощью доверенного агента уполномоченного лица.

51. Способ по п.50, **отличающийся** тем, что при первом криптографически безопасном сеансе связи к доверенному агенту покупателя посылают сумму платежа, между первым денежным модулем, относящимся к доверенному агенту покупателя, и вторым денежным модулем, относящимся к доверенному агенту уполномоченного лица, устанавливают второй криптографически безопасный сеанс связи и от первого денежного модуля передают ко второму денежному модулю электронные деньги в сумме, соответствующей сумме платежа.

52. Способ по п.50, **отличающийся** тем, что при первом криптографически безопасном сеансе связи к доверенному агенту покупателя посылают сумму платежа, от доверенного агента покупателя посылают платежное удостоверение к доверенному агенту уполномоченного лица при первом криптографически безопасном сеансе связи, с помощью доверенного агента уполномоченного лица проверяют действительность платежного удостоверения, посылают сумму платежа и платежное удостоверение в сеть проверки полномочий карт, с помощью доверенного агента уполномоченного лица получают сообщение о том, что платеж разрешен, и от доверенного агента уполномоченного лица посылают сообщение о проверке полномочий на осуществление платежа к доверенному агенту покупателя.

53. Способ по п.50, **отличающийся** тем, что доверенный агент покупателя и доверенный агент уполномоченного лица записывают в журнал транзакций информацию, которая после осуществления фиксации транзакции безусловно сохраняется этими доверенными агентами.

54. Способ по п.50, **отличающийся** тем, что с помощью доверенного агента уполномоченного лица также проверяют необходимость продления электронного удостоверения.

55. Способ по п.50, **отличающийся** тем, что после установления первого криптографически безопасного сеанса связи от доверенного агента уполномоченного лица посылают удостоверение уполномоченного лица к доверенному агенту покупателя и с помощью доверенного агента покупателя проверяют действительность этого удостоверения уполномоченного лица.

56. Способ платежа через денежный модуль на основе идентификации с использованием защищенного от несанкционированного доступа первого доверенного агента, первого денежного модуля, второго доверенного агента и второго денежного модуля, **отличающийся** тем, что между первым доверенным агентом и вторым доверенным агентом устанавливают первый криптографически безопасный сеанс связи, от второго доверенного агента посылают удостоверение этого второго доверенного агента к первому доверенному агенту при первом криптографически безопасном сеансе связи, с помощью первого доверенного агента проверяют действительность удостоверения второго доверенного агента и условно сохраняют это удостоверение, от первого доверенного агента посылают информацию о пла-

теже ко второму доверенному агенту при первом криптографически безопасном сеансе связи, с помощью первого доверенного агента инициализируют платеж электронных денег от первого денежного модуля ко второму денежному модулю в сумме, соответствующей информации о платеже, при втором криптографически безопасном сеансе связи между первым и вторым денежными модулями, осуществляют фиксацию транзакции с помощью первого доверенного агента после получения информации об успешном платеже от первого денежного модуля, после чего в первом доверенном агенте безусловно сохраняют информацию в журнале транзакций, содержащую удостоверение второго доверенного агента и данные, соответствующие информации о платеже, и осуществляют фиксацию транзакции с помощью второго доверенного агента после приема информации об успешном платеже от второго денежного модуля.

57. Способ по п.56, **отличающийся** тем, что от первого доверенного агента второму доверенному агенту посылают сообщение с запросом о необходимости посылки удостоверения первого доверенного агента, от первого доверенного агента посылают удостоверение этого первого доверенного агента ко второму доверенному агенту при первом криптографически безопасном сеансе связи и с помощью второго доверенного агента проверяют действительность удостоверения первого доверенного агента.

58. Способ разрешения спора по электронному товару с использованием доверенного агента покупателя, первого центрального процессора, доверенного агента продавца и второго центрального процессора, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают криптографически безопасный сеанс связи, от доверенного агента покупателя посылают данные журнала транзакций к первому центральному процессору для выбора предмета спора, соответствующего электронному билету, хранящемуся в доверенном агенте покупателя, от первого центрального процессора посылают информацию о предмете спора к доверенному агенту покупателя, от доверенного агента покупателя посылают копию электронного билета и информацию о предмете спора доверенному агенту продавца при первом криптографически безопасном сеансе связи, с помощью доверенного агента продавца проверяют действительность электронного билета, от доверенного агента продавца посылают электронный билет и информацию о предмете спора ко второму центральному процессору, принимают решение об отклонении спора, касающегося электронного билета и информации о предмете спора, от второго центрального процессора посылают сообщение об отклонении спора доверенному агенту продавца, от доверенного агента продавца отправляют сообщение об отклонении спора доверенному агенту покупателя, осуществляют фиксацию транзакции с помощью доверенного агента покупателя и осуществляют фиксацию транзакции с помощью доверенного агента продавца.

59. Способ по п.58, **отличающийся** тем, что записывают в журнал транзакций сообщение об отклонении спора.

60. Способ по п.58, **отличающийся** тем, что от доверенного агента покупателя посылают доверенному агенту продавца электронный объект, соответствующий электронному билету, проверяют подлинность электронного объекта, расшифровывают электронный объект при помощи электронного билета и расшифрованный электронный объект посылают на второй центральный процессор для выявления дефектов.

61. Способ разрешения спора по электронному товару с использованием доверенного агента покупателя, первого центрального процессора, доверенного агента продавца и второго центрального процессора, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают первый криптографически безопасный сеанс связи, от доверенного агента покупателя посылают данные журнала транзакций к первому центральному процессору для выбора предмета спора, соответствующего электронному билету, хранящемуся в доверенном агенте покупателя, от первого центрального процессора посылают информацию о предмете спора к доверенному агенту покупателя, от доверенного агента покупателя посылают копию электронного билета и информацию о предмете спора к доверенному агенту продавца при первом криптографически безопасном сеансе связи, с помощью доверенного агента продавца проверяют действительность электронного билета, от доверенного агента продавца посылают электронный билет и информацию о предмете спора ко второму центральному процессору, принимают решение не отклонять спор, касающийся электронного билета и информации о предмете спора, и инициализируют возмещение расходов покупателю.

62. Способ по п.61, **отличающийся** тем, что от второго центрального процессора посылают сообщение на первый центральный процессор с запросом о решении покупателя, с помощью первого центрального процессора осуществляют информирование доверенного агента покупателя, что решением покупателя является денежное возмещение, и от доверенного агента покупателя посылают запрос о возмещении доверенному агенту продавца при первом криптографически безопасном сеансе связи.

63. Способ по п.62, **отличающийся** тем, что между первым денежным модулем, относящимся к доверенному агенту покупателя, и вторым денежным модулем, относящимся к доверенному агенту продавца, устанавливают второй криптографически безопасный сеанс связи, с помощью доверенного агента покупателя предоставляют первому денежному модулю первую информацию о возмещении, а с помощью доверенного агента продавца предоставляют второму денежному модулю вторую информацию о возмещении и от второго денежного модуля передают электронные деньги в сумме, соответствующей информации о возмещении, к первому денежному модулю при втором криптографически безопасном сеансе связи.

64. Способ по п.62, **отличающийся** тем, что от доверенного агента продавца посылают возмещаемую сумму доверенному агенту покупателя при первом криптографически безопасном сеансе

связи, от доверенного агента покупателя посылают платежное удостоверение доверенному агенту продавца при первом криптографически безопасном сеансе связи, с помощью доверенного агента продавца проверяют действительность платежного удостоверения, от доверенного агента продавца посылают платежное удостоверение и сумму возмещения в сеть проверки полномочий для проверки полномочий возмещения, с помощью доверенного агента продавца получают проверку полномочий возмещения и от доверенного агента продавца посылают сообщение о проверке полномочий возмещения доверенному агенту покупателя при первом криптографически безопасном сеансе связи.

65. Способ по п.62, **отличающийся** тем, что от доверенного агента покупателя посылают электронный объект, соответствующий электронному билету, к доверенному агенту продавца, подтверждают действительность электронного объекта, расшифровывают электронный объект при помощи электронного билета и расшифрованный электронный объект посылают на второй центральный процессор для проверки на наличие дефектов.

66. Способ по п.61, **отличающийся** тем, что дополнительно осуществляют фиксацию транзакции с помощью доверенных агентов покупателя и продавца.

67. Способ по п.66, **отличающийся** тем, что после фиксации транзакции в доверенных агентах продавца и покупателя безусловно сохраняют данные журнала транзакций.

68. Способ разрешения спора по электронному товару с использованием доверенного агента покупателя, первого центрального процессора, доверенного агента продавца и второго центрального процессора, **отличающийся** тем, что между доверенным агентом покупателя и доверенным агентом продавца устанавливают криптографически безопасный сеанс связи, от доверенного агента покупателя посылают данные журнала транзакций на первый центральный процессор для выбора предмета спора, соответствующего электронному билету, хранящемуся в доверенном агенте покупателя, от первого центрального процессора посылают информацию о предмете спора доверенному агенту покупателя, от доверенного агента покупателя посылают копию электронного билета и информацию о предмете спора доверенному агенту продавца при криптографически безопасном сеансе связи, с помощью доверенного агента продавца проверяют действительность электронного билета, от доверенного агента продавца посылают электронный билет и информацию о предмете спора на второй центральный процессор, принимают решение не отклонять спор, касающийся электронного билета и информации о предмете спора, с помощью доверенного агента продавца запрашивают новый электронный товар у сервера товаров, от сервера товаров посылают новый товар доверенному агенту продавца и от доверенного агента продавца посылают новый товар доверенному агенту покупателя при криптографически безопасном сеансе связи.

69. Способ по п.68, **отличающийся** тем, что от доверенного агента покупателя посылают доверенному агенту продавца электронный объект,

соответствующий электронному билету, проверяют действительность электронного объекта, расшифровывают электронный объект при помощи электронного билета и расшифрованный электронный объект посылают на второй центральный процессор для проверки на наличие дефектов.

70. Способ по п.68, **отличающийся** тем, что дополнительно осуществляют фиксацию транзакции доверенными агентами покупателя и продавца.

71. Способ по п.70, **отличающийся** тем, что после фиксации транзакции в доверенных агентах продавца и покупателя безусловно сохраняют данные журнала транзакций.

72. Система для разрешения спора по электронному товару, **отличающаяся** тем, что содержит защищенный от несанкционированного доступа доверенный агент покупателя, выполненный с возможностью получения электронного товара от доверенного агента продавца при первом криптографическом безопасном сеансе связи, с возможностью проверки действительности электронного товара и записи транзакции покупки в свой журнал транзакций, а также с возможностью связи с доверенным агентом продавца для выполнения первого протокола спора и, если спор отклонен, записи отказа от спора в свой журнал транзакций, защищенный от несанкционированного доступа доверенный агент продавца, выполненный с возможностью связи с доверенным агентом покупателя посредством криптографически безопасного сеанса связи, с возможностью передачи электронного товара доверенному агенту покупателя при криптографически безопасном сеансе связи и с возможностью записи транзакции покупки в свой журнал транзакций, и доверенный сервер, выполненный с возможностью связи с доверенным агентом покупателя для выполнения второго протокола спора в случае, если доверенный агент покупателя не удовлетворен результатом первого протокола спора.

73. Система для обеспечения безопасности одновременно производимых платежей электронных денег и доставки электронного товара в коммуникационной сети, **отличающаяся** тем, что содержит защищенный от несанкционированного доступа первый электронный агент, содержащий первый процессор, защищенный от несанкционированного доступа первый денежный модуль, выполненный с возможностью осуществления безопасной связи с первым электронным агентом и содержащий второй процессор, защищенный от несанкционированного доступа второй электронный агент, выполненный с возможностью установления первого криптографически безопасного сеанса связи с первым электронным агентом по коммуникационной сети и содержащий третий процессор, защищенный от несанкционированного доступа второй денежный модуль, выполненный с возможностью осуществления безопасной связи со вторым электронным агентом, а также с возможностью установления второго криптографически безопасного сеанса связи с первым денежным модулем и содержащий четвертый процессор, при этом первый электронный агент и первый денежный модуль удалены от второго электронного агента и второго денежного модуля, а третий процессор выполнен с возмож-

ностью передачи электронного товара первому электронному агенту при первом криптографически безопасном сеансе связи, первый процессор выполнен с возможностью приема электронного товара и отказа в открытом внешнем доступе к электронному товару до приема сообщения, указывающего на успешный платеж, произведенный первым денежным модулем, второй процессор выполнен с возможностью передачи электронных денег второму денежному модулю при втором криптографически безопасном сеансе связи и последующей отсылки первому процессору сообщения, указывающего на успешный платеж, а четвертый процессор выполнен с возможностью приема электронных денег.

74. Система по п.73, **отличающаяся** тем, что первый электронный агент выполнен с возможностью непредоставления информации, идентифицирующей своего владельца, второму электронному агенту в течение транзакции дистанционной покупки по коммуникационной сети.

75. Способ осуществления безопасной связи между электронными устройствами обработки, **отличающийся** тем, что между первым и вторым электронными устройствами обработки устанавливают первый криптографически безопасный сеанс связи, причем первое электронное устройство обработки удалено от второго электронного устройства обработки, между третьим и четвертым электронными устройствами обработки устанавливают второй криптографически безопасный сеанс связи, причем третье электронное устройство обработки удалено от четвертого электронного устройства обработки и связь между первым и третьим электронными устройствами обработки осуществляют по первой линии связи, а связь между вторым и четвертым электронными устройствами обработки осуществляют по второй линии связи, формируют ключ сеанса связи, этот ключ сеанса связи сохраняют в первом электронном устройстве обработки, на третье электронное устройство обработки по второй линии связи при втором криптографически безопасном сеансе связи посылают информацию о ключе сеанса связи, хранящуюся во втором электронном устройстве обработки, в третьем электронном устройстве обработки формируют ключ сеанса связи по меньшей мере частично на основе информации о ключе сеанса связи, сохраняют ключ сеанса связи в третьем электронном устройстве обработки и при помощи ключа сеанса связи устанавливают третий криптографически безопасный сеанс связи между первым электронным устройством обработки и третьим электронным устройством обработки.

76. Способ по п.75, **отличающийся** тем, что информация о ключе сеанса связи содержит второе случайное число, а стадия формирования ключа сеанса связи заключается в том, что с помощью первого электронного устройства обработки генерируют первое случайное число, с помощью второго электронного устройства обработки генерируют второе случайное число, которое посылают на первое электронное устройство обработки при первом криптографически безопасном сеансе связи, и с помощью первого электронного устройства обработки формируют ключ сеанса связи, выпол-

няя операцию ИСКЛЮЧАЮЩЕЕ ИЛИ над первым и вторым случайными числами.

77. Способ по п.76, **отличающийся** тем, что от первого электронного устройства обработки дополнительно посылают первое случайное число на третье электронное устройство обработки по первой линии связи и определяют наличие ключа сеанса связи в третьем электронном устройстве обработки, выполняя операцию ИСКЛЮЧАЮЩЕЕ ИЛИ над первым и вторым случайными числами.

78. Способ по п.77, **отличающийся** тем, что от первого электронного устройства обработки дополнительно посылают первое случайное число на второе электронное устройство обработки при первом криптографически безопасном сеансе связи, с помощью второго электронного устройства обработки формируют ключ сеанса связи, выполняя операцию ИСКЛЮЧАЮЩЕЕ ИЛИ над первым и вторым случайными числами, и сохраняют этот ключ сеанса связи во втором электронном устройстве обработки, от второго электронного устройства обработки посылают второе случайное число на четвертое электронное устройство обработки по второй линии связи, от первого электронного устройства обработки на четвертое электронное устройство обработки по первой линии связи при втором криптографически безопасном сеансе связи посылают первое случайное число, с помощью четвертого электронного устройства обработки формируют ключ сеанса связи, выполняя операцию ИСКЛЮЧАЮЩЕЕ ИЛИ над первым и вторым случайными числами, этот ключ сеанса связи сохраняют в четвертом электронном устройстве обработки и при помощи ключа сеанса связи устанавливают четвертый криптографически безопасный сеанс связи между вторым и четвертым электронными устройствами обработки.

79. Способ по п.75, **отличающийся** тем, что информацию, проходящую при втором криптографически безопасном сеансе связи, дополнительно шифруют при первом криптографически безопасном сеансе связи.

80. Способ по п.75, **отличающийся** тем, что в качестве электронных устройств обработки используют защищенные от несанкционированного доступа электронные устройства.

81. Способ по п.80, **отличающийся** тем, что в качестве первого и второго электронных устройств обработки используют доверенные агенты, а в качестве третьего и четвертого электронных устройств обработки используют денежные модули.

82. Способ осуществления безопасной связи между электронными устройствами обработки, **отличающийся** тем, что между первым и вторым электронными устройствами обработки устанавливают первый криптографически безопасный сеанс связи, причем первое электронное устройство обработки удалено от второго электронного устройства обработки, между третьим и четвертым электронными устройствами обработки устанавливают второй криптографически безопасный сеанс связи, при этом третье электронное устройство обработки удалено от четвертого электронного устройства обработки и связь между первым и третьим электронными устройствами обработки осуществляют по первой линии связи, а связь между вторым и четвертым электронными устройствами

обработки осуществляют по второй линии связи, с помощью первого электронного устройства обработки генерируют первое случайное число, это первое случайное число посылают на второе электронное устройство обработки при первом криптографически безопасном сеансе связи и на четвертое электронное устройство обработки по второй линии связи, сохраняя указанное первое случайное число в первом, втором и четвертом электронных устройствах обработки, с помощью второго электронного устройства обработки генерируют второе случайное число, это второе случайное число посылают на первое устройство обработки при первом криптографически безопасном сеансе связи и на третье устройство обработки по первой линии связи, сохраняя указанное второе случайное число в первом, втором и третьем электронных устройствах обработки, первое случайное число посылают от четвертого электронного устройства обработки на третье устройство обработки при втором криптографически безопасном сеансе связи, второе случайное число посылают от третьего электронного устройства обработки на четвертое электронное устройство обработки при втором криптографически безопасном сеансе связи, из первого и второго случайных чисел формируют случайный ключ сеанса связи с помощью первого электронного устройства обра-

ботки, из первого и второго случайных чисел формируют случайный ключ сеанса связи с помощью второго электронного устройства обработки, из первого и второго случайных чисел формируют случайный ключ сеанса связи с помощью третьего электронного устройства обработки и из первого и второго случайных чисел формируют случайный ключ сеанса связи с помощью четвертого электронного устройства обработки, при этом связь между первым и третьим электронными устройствами обработки и между вторым и четвертым электронными устройствами обработки осуществляют криптографически при помощи ключа сеанса связи.

83. Способ по п.82, **отличающийся** тем, что информацию, проходящую при втором криптографически безопасном сеансе связи, дополнительно шифруют при первом криптографически безопасном сеансе связи.

84. Способ по п.82, **отличающийся** тем, что в качестве электронных устройств обработки используют защищенные от несанкционированного доступа электронные устройства.

85. Способ по п.84, **отличающийся** тем, что в качестве первого и второго электронных устройств обработки используют доверенные агенты, а в качестве третьего и четвертого электронных устройств обработки используют денежные модули.

Изобретение относится к системе для упрощения открытого электронного бизнеса. В частности, в этой системе используются защищенные от несанкционированного доступа электронные устройства, обозначаемые как "доверенные агенты", совместно с денежными модулями для создания защищенной среды для осуществления транзакций (сделок) как для покупателя, так и для продавца электронных товаров или услуг.

На сегодняшний день электронный бизнес состоит из набора закрытых организаций. Примерами подобных организаций являются местные и междугородные телефонные компании, компании кабельной связи, компании сотовой телефонной связи, службы электронной почты (E-mail), а также такие поставщики электронных услуг, как Prodigy и CompuServe. Пользователи должны становиться членами каждой такой организации, соответственно подписываться на предоставляемые этими организациями услуги, чтобы пользоваться предлагаемыми услугами и товарами. Таким образом, перед электронной поставкой товаров и услуг требуется предварительная идентификация покупателя. Оператор службы может затем либо выставить пользователю счет, либо записать сумму в кредит или дебет его счета.

С появлением высокоскоростных сетей, предоставляющих информацию развлекательного характера и информацию по требованию, существующие вексельные и платежные системы будут переполнены транзакциями. Следовательно, пользователь будет "завален" счетами со множеством пунктов по каждому платежному периоду. Более того, образ жизни пользователя будет ви-

ден каждому системному оператору из-за неанонимной природы транзакций.

Один из способов анонимных платежей описан в международной заявке WO 93/10503, озаглавленной "Electronic-Monetary System", опубликованной 27 мая 1993 г. В этой заявке рассматривается электронная денежная система для осуществления электронных денежных платежей в качестве альтернативного средства обмена по отношению к наличным деньгам, чекам, кредитным картам, дебетовым картам и электронным переводам. В частности, описанная система использует денежные модули, помещенные в защищенные от несанкционированного доступа "гнезда" для хранения и передачи электронных банкнот. Платежи денежного модуля могут быть либо автономными платежами в реальном времени между денежными модулями (например, между денежным модулем, содержащимся в "электронном бумажнике" покупателя, и денежным модулем, содержащимся в находящемся в месте продажи терминале продавца и называемом также кассовым терминалом), либо интерактивными платежами за такие сетевые услуги, как поиск информации и телефонные вызовы, соответственно переговоры, или за покупку авиабилетов, театральных билетов и т.п.

Однако серьезной проблемой дистанционных анонимных покупок является безопасность платежа и доставки. Если кто-либо хочет купить фильм по телефону анонимно, то неизвестно, насколько покупатель может быть уверен в том, что именно он получит фильм, если он заплатил первым, и насколько может быть уверен продавец, что именно ему заплатят, если он первым доста-

вит фильм. Таким образом, при покупке чего-либо с удаленного местоположения обычной на сегодняшний день для покупателя и продавца является идентификация самих себя, приводящая в результате к утрате секретности.

Таким образом, задачей настоящего изобретения является разработка системы, которая позволила бы покупателям приобретать электронные товары или услуги по требованию без вступления в члены организации, предоставляющей электронные услуги.

Другой задачей настоящего изобретения является обеспечение дистанционной доставки электронной покупки или услуг при помощи анонимного платежа в реальном времени или платежа на основе проверки (установления) полномочий в реальном времени, когда ни покупатель, ни продавец не могут вмешиваться в процесс платежа или доставки, как только они заключили сделку.

Еще одной задачей настоящего изобретения является использование доверенных агентов и денежных модулей для создания системы для открытого электронного бизнеса, в которой как покупатели, так и продавцы могут безопасно заключать сделки на расстоянии посредством электронных сетей без предварительного ознакомления друг с другом.

Еще одной задачей настоящего изобретения является обеспечение безопасной электронной транзакции покупки в реальном времени между покупателем и продавцом без посредничества третьей стороны.

В соответствии с изобретением предлагается, таким образом, система для открытого электронного бизнеса, содержащая первый и второй денежные модули и в ней предусмотрены доверенный агент покупателя и доверенный агент продавца. В этой системе доверенный агент покупателя устанавливает криптографически безопасный сеанс связи с доверенным агентом продавца. Доверенный агент покупателя затем безопасно связывается с первым денежным модулем, а доверенный агент продавца безопасно связывается со вторым денежным модулем. Доверенный агент продавца поставяет электронный товар, который временно хранится доверенным агентом покупателя. Доверенные агенты участвуют в безопасном диалоге и взаимно соглашаются с условиями платежа. Первый денежный модуль передает электронные деньги второму денежному модулю. После успешного выполнения платежа с помощью денежных модулей первый денежный модуль информирует доверенного агента покупателя, а второй денежный модуль - доверенного агента продавца. Затем продавец регистрирует продажу, а покупатель может использовать купленный электронный товар.

В соответствии с одним из вариантов выполнения изобретения покупатель может платить за электронную покупку путем предъявления удостоверения в виде кредитной или дебетовой карты.

В соответствии с другим вариантом выполнения изобретения электронные билеты или мандаты могут быть предъявлены другим доверенным агентам для получения услуг.

В соответствии с еще одним вариантом выполнения изобретения доверенные агенты могут использоваться для осуществления безопасного платежа, основанного на идентификации.

Кроме того, в другом варианте выполнения изобретения доверенные агенты могут использоваться для разрешения спора по электронной покупке.

Ниже изобретение более подробно описано со ссылками на прилагаемые чертежи, на которых показано:

на фиг. 1 - схема, иллюстрирующая взаимодействие доверенного агента/денежного модуля,

на фиг. 2 - разделы и поля различных билетов,

на фиг. 3 - компоненты устройства транзакций,

на фиг. 4А-4Г - функциональные компоненты доверенных агентов,

на фиг. 6А - схема, иллюстрирующая структуру сети системы для открытого электронного бизнеса,

на фиг. 6Б - функциональные компоненты (основного) доверенного сервера,

на фиг. 7А - протокол фиксации транзакции,

на фиг. 7Б - протокол прекращения транзакции,

на фиг. 8А-8В - протокол пересертификации доверенного агента,

на фиг. 9А-9Д - протокол установления сеанса связи,

на фиг. 10 - протокол отправки сообщения,

на фиг. 11 - протокол прекращения транзакции,

на фиг. 12А-12Б - протокол покупки электронного товара,

на фиг. 13 - различные уровни кодирования сообщения, установленные между доверенными агентами и денежными модулями,

на фиг. 14 - протокол проверки удостоверения,

на фиг. 15А-15Б - протокол доставки товара,

на фиг. 16А-16Д - протокол платежа с помощью денежного модуля,

на фиг. 17 - протокол отправки маршрутизированного сообщения,

на фиг. 18 - протокол отправки сообщения от денежного модуля к доверенному агенту,

на фиг. 19 - протокол отправки сообщения от доверенного агента к денежному модулю,

на фиг. 20 - протокол отправки маршрутизированного сообщения по электронной почте,

на фиг. 21А-21Б - протокол платежа-возврата на основе проверки полномочий,

на фиг. 22 - протокол открывания покупки,

на фиг. 23А-23Г - протокол предъявления электронного билета на услуги,

на фиг. 24 - протокол выдачи билета,

на фиг. 25А-25В - протокол передачи билета,

на фиг. 26 - протокол приобретения удостоверения,

на фиг. 27А-27Б - протокол доставки удостоверения,

на фиг. 28А-28Б - протокол дистанционного переподтверждения удостоверения,

на фиг. 29А-29Б - протокол платежа с помощью денежных модулей на основе идентификации,

на фиг. 30А-30Д - протокол разрешения спора по электронной покупке,

на фиг. 31 - протокол совершения спора,

на фиг. 32 - протокол выплаты по спору,

на фиг. 33А - схема, иллюстрирующая иерархию безопасности в электронной денежной системе,

на фиг. 33Б - схема, иллюстрирующая обмен сообщениями по сети безопасности между основным сервером обеспечения безопасности и обычным сервером,

на фиг. 34 - схема, иллюстрирующая структуру сети безопасности для системы электронной купли-продажи,

на фиг. 35А - функциональные компоненты сервера обеспечения безопасности,

на фиг. 35Б - функциональные компоненты сетевого сервера,

на фиг. 36 - процедура входа в сеть,

на фиг. 37А-37Л - протокол входа в сеть,

на фиг. 38А-38Д - протокол установления сеанса связи в электронной денежной системе,

на фиг. 39А-39Б - протокол передачи банкнот,

на фиг. 40А-40Г - протокол обмена иностранной валюты,

на фиг. 41 - протокол фиксации транзакции для модулей в электронной денежной системе,

на фиг. 42А-42Б - протокол прекращения транзакции для модулей в электронной денежной системе,

на фиг. 43А-43В - протокол платежа "на месте продажи" (через кассовый терминал),

на фиг. 44А-44Б - протокол связывания счетов.

В настоящем изобретении предлагается система для обеспечения безопасной доставки электронной покупки с анонимной оплатой в реальном времени или оплатой, основанной на проверке полномочий. Система обеспечивает соблюдение интересов как покупателя, так и продавца.

На фиг. 1 показано основное взаимодействие между компонентами системы во время анонимной платежной транзакции. Для достижения безопасного обмена платежами за электронную покупку, когда покупатель и продавец совершают транзакцию посредством электронной системы, в описание настоящего изобретения введено понятие доверенных агентов 2, 4 как для покупателя, так и для продавца. Доверенный агент представляет собой электронное устройство обработки, являющееся сочетанием аппаратных и программных компонентов. Это устройство защищено от несанкционированного доступа и содержит обеспечивающие безопасность протоколы, которые взаимодействуют с денежным модулем 6 для синхронизации безопасных платежа и доставки.

Денежные модули, рассматриваемые в настоящем описании, представляют собой защищенные от несанкционированного доступа электронные устройства обработки, способные хранить и передавать электронные деньги. Электронные деньги предпочтительно являются электронными

банкнотами, представляющими собой валюту или кредит. Денежные модули также способны устанавливать криптографически безопасные сеансы связи с другими устройствами. В предпочтительном варианте выполнения настоящего изобретения используются денежные модули транзакций, представленные в заявке WO 93/10503, с учетом модификаций и усовершенствований, описываемых ниже.

Теоретически доверенный агент является заменой объекта, желающего дистанционно (в электронном виде) совершить транзакцию безопасным образом. Доверенные агенты управляются протоколами транзакций и действуют в соответствии с таким расчетом, который обеспечивает совершение транзакции с соблюдением интересов обеих сторон. С целью обеспечить правильное функционирование доверенного агента протоколы защищаются физически. Таким образом, ни одна из сторон не может модифицировать протоколы в целях нанесения ущерба другой стороне.

Доверенные агенты обмениваются электронными товарами и платежами. Как показано на фиг. 1, доверенный агент 4 продавца (ДАПрод) посылает электронный товар доверенному агенту 2 покупателя (ДАПок). В свою очередь денежный модуль 6 покупателя посылает электронные деньги денежному модулю 6 продавца через ДАПок 2 и ДАПрод 4.

Билеты.

Электронными покупками являются любые товары, которые могут быть представлены в электронной форме, и в предпочтительном варианте выполнения, описанном в данном разделе, состоит из билета или зашифрованного электронного объекта (ЭО) и связанного с ним билета расшифровки. Как показано на фиг. 1 и 2, билет 8 является электронным объектом, создаваемым ДАПрод 4 и передаваемым к ДАПок 2 во время транзакции покупки. Билеты можно представить как собственность доверенных агентов. Покупатель, ДАПок 2 которого только что получил билет 8, может использовать этот билет только после успешного завершения транзакции.

Согласно настоящему изобретению оперируют билетами следующих различных типов, используемыми в различных целях.

1. Билет дешифровки соответственно расшифровки всегда связан с отдельным зашифрованным электронным объектом. Примерами электронных объектов являются компьютерные программы, игры, фильмы или информационные продукты типа электронных газет или книг. В этом случае товары продавца являются электронными объектами, которые шифруются ДАПрод перед тем, как они посылаются покупателю. Зашифрованный электронный объект может быть расшифрован при помощи уникальной информации, содержащейся в связанном с ним билете расшифровки. Зашифрованный электронный объект и связанный с ним билет расшифровки вместе составляют электронную покупку, передаваемую продавцом.

Передаваемый электронный объект криптографически защищен от проверки и использования принимающим покупателем или какой-либо



третьей стороной до тех пор, пока у них нет доступа к билету расшифровки. Билет расшифровки, в свою очередь, является "собственностью" ДАПок и может быть использован только после успешного завершения транзакции покупки.

2. Удостоверяющий билет идентифицирует "владельца" и дает особые привилегии. Примерами удостоверяющих билетов или удостоверений являются водительские права, паспорт, кредитная карта, дебетовая карта, полис социального страхования и корпоративная печать.

3. Транспортный билет может служить билетом в электронном виде на самолет, поезд или автобус.

4. Билет на мероприятие может служить входным билетом на различные мероприятия, например, на театральные, концертные, игровые представления или спортивные соревнования.

5. Билет на услуги связи обеспечивает доступ к различным службам связи, в том числе спутниковой связи, кабельной связи, радиосвязи, сотовой телефонной связи и общественной телефонной службе. Например, билет на услуги связи может использоваться для декодирования теле- или радиопередачи.

6. Билет физического объекта может служить в качестве заказа на покупку, накладной, платежного уведомления, квитанции или названия для физических объектов.

Очевидно, что возможны и другие типы билетов, которые могут оказаться приемлемыми для открытого электронного бизнеса по настоящему изобретению.

Доверенный агент может не только покупать билеты, но и предъявлять их другим доверенным агентам в различных целях. Например, билеты на мероприятия могут быть предъявлены электронным путем для входа в зал или на стадион. После этого билет может быть снова электронно предъявлен для автоматического поиска места зрителя. Водительские права в виде билета могут быть предъявлены как удостоверение личности. Билет может быть предъявлен как удостоверение покупки неэлектронных товаров и обременен на физический объект либо доставляемый покупателю, либо выбранный покупателем в магазине или на складе. Билет в виде кредитной или дебетовой карты может быть предъявлен для платежа на основе проверки полномочий. В случае спора по покупке билет может быть предъявлен как доказательство покупки дефектного товара.

На фиг. 2 показан предпочтительный вариант билета 8, при этом билет состоит из шести следующих главных разделов: раздела 10 "Идентификатор", раздела 12 "Компоненты", раздела 14 "Подпись эмитента", раздела 16 "Сертификат эмитента", раздела 18 "Предыстория передачи" и раздела 20 "Подписи отправителей". Эти части, в свою очередь, состоят из содержащих различную информацию полей.

Раздел 10 "Идентификатор" имеет поле 22, содержащее информацию, идентифицирующую продавца или уполномоченного, создавшего билет. Такая информация, например, имя продавца или уполномоченного, копируется из удостоверения продавца или уполномоченного, хранящегося у эмитента билета. Поле 22 содержит также срок

действия удостоверения продавца или уполномоченного. Поле 24 содержит идентификационный номер принимающего доверенного агента. Поле 24 содержит также срок действия удостоверения доверенного агента лица, принимающего билет. Поле 26 устанавливает тип билета (например, билет расшифровки, билет на мероприятие и т.д.).

Раздел 12 "Компоненты" составляет основное содержание билета, которое изменяется в зависимости от типа билета и его конкретных целей. На фиг. 2 приведены примеры компонентов, содержащихся в билетах различных типов.

Раздел 12 "Компоненты" билета расшифровки имеет поле 36 "Идентификатор объекта", которое уникальным образом идентифицирует конкретный электронный объект и может также содержать краткое описание электронного объекта (например, название и автора). Сами электронные объекты (например, фильмы) состоят из заголовка и основной части. Заголовок содержит идентификатор объекта, который связан с разделом 36 "Идентификатор объекта" в билете расшифровки. Заголовок также содержит описательную информацию, которая может быть предоставлена покупателю для ознакомления с содержанием объекта. В основной части представлено основное содержание объекта, иными словами, с этой частью покупатель может работать, т.е. читать или просматривать.

Поле 38 "Ключ расшифровки" содержит информацию, используемую для расшифровки относящегося к билету электронного объекта. Поле 40 "Цена покупки" содержит информацию о цене электронного объекта. Поле 42 "Дата покупки" содержит дату покупки электронного объекта. Поле 44 "Подпись объекта" содержит цифровую подпись электронного объекта. Цифровые подписи хорошо известны из уровня техники и используются для определения того, не был ли объект как-либо изменен с тех пор, как он был подписан. Таким образом, может проверяться целостность электронного объекта. Поле 46 "Использование" определяет ограничения на использование данного электронного объекта.

Удостоверяющий билет, такой, как водительские права, может содержать поле 48 "Имя", поле 50 "Адрес", поле 52 "Изображение и физическое описание", поле 54 "Подпись водителя", содержащее электронное изображение подписи водителя, поле 56 "Срок действия", поле 58 "Статус", показывающее, являются ли права действующими, приостановлено ли их действие либо являются ли они аннулированными, и поле 60 "Использование", показывающее, что копия билета предъявлена ДАПрод 4 для использования, чтобы оригинал билета, удерживаемый ДАПок 2, не мог быть использован еще раз в течение периода предъявления. Удостоверяющий билет типа корпоративной печати может иметь поле 62 "Название корпорации", поле 64 "Адрес", поле 66 "Идентификатор налогоплательщика", поле 68 "Срок действия" и поле 70 "Использование".

Транспортный билет может содержать поле 72 "Наименование транспорта", поле 74 "Номер рейса", определяющее, например, номер рейса самолета, номер поезда или автобуса, поля 76, 78

"Отправление и прибытие", каждое из которых определяет время и место отправления и прибытия, поле 80 "Цена покупки", поле 82 "Дата покупки", поле 84 "Статус", показывающее, является ли билет неиспользованным или уже использовался, и поле 86 "Использование".

Билет на мероприятие может содержать поле 88 "Идентификация мероприятия", поле 90 "Местонахождение", поле 92 "Дата", поле 94 "Номер места", поле 96 "Цена покупки", поле 98 "Дата покупки", поле 100 "Статус" и поле 102 "Использование".

Билет на услуги связи может содержать поле 104 "Идентификатор компании-поставщика коммуникационных услуг", поле 106 "Купленное время", поле 108 "Канал/частота", поле 110 "Цена покупки", поле 112 "Дата покупки", поле 114 "Ключи расшифровки" для декодирования или расшифровки, если связь зашифрована, поле 116 "Доступное время", показывающее оставшееся значение в билете, и поле 118 "Использование".

Билет физического объекта (не показан) может служить заказом на покупку и содержать следующую информацию: регистрационный номер, дату, идентификатор покупателя, список покупаемых предметов, инструкции (команды) и статус (сделан заказ, выписан счет и т.д.). Билет физического объекта может также служить счетом и содержать номер счета, дату, почтовый индекс, идентификатор поставщика и сумму. Подобным же образом уведомление о переводе будет содержать регистрационные номера счета, идентификатор получателя, дату и уплаченную сумму. Квитанция будет содержать дату, идентификатор поставщика, список предметов или регистрационных номеров счетов и уплаченную сумму.

Доверенные агенты могут использоваться для розничной покупки физических объектов как лично, так и дистанционно. При покупке лично с помощью доверенного агента вся сделка целиком может выполняться со скоростью действия электроники и без бумаги как для анонимных, так и для основанных на проверке полномочий сделок. Для продавца это означает, что он может уменьшить расходы на обслуживание покупателя. Покупателю же предоставляются большие удобства и обеспечивается более легкое управление, т.к. время сделки уменьшается, а агент имеет электронный список покупок, который может быть легко проанализирован позже.

При дистанционной покупке физических объектов по телефону или интерактивному телевидению негативным для продавца и покупателя ограничением является то, что покупка должна быть доставлена на адрес покупателя. Это делается для защиты продавца от мошенничества. Платеж обычно выполняется при помощи кредитной карты либо покупателю выставляется счет, что раскрывает личность покупателя.

Если покупка делается с использованием доверенного агента, то товар не должен обязательно доставляться на адрес покупателя, а покупатель не должен раскрывать информацию о себе. Анонимность может достигаться, если покупатель платит электронными деньгами в момент заказа или получения покупки. Ограничение на место доставки может быть в любом случае снято.

Продавец защищен от мошенничества, поскольку ему платят до или во время доставки товара. Более того, проверка правильности получателя осуществляется во время доставки покупки. Покупатель может чувствовать себя защищенным, поскольку третьей стороне будет сложно обмануть его, т.к. имеется защищенная квитанция. Кроме того, транзакция может быть оспорена при помощи защищенной квитанции в случае, если доставленная покупка дефектна. В конце транзакции как доверенный агент 2 покупателя, так и доверенный агент 4 продавца делают соответствующую запись о том, что заказанная покупка оплачена и доставлена именно заказавшей стороне.

Для коммерческих транзакций доверенные агенты обеспечивают надежные, аутентификационные, автоматические транзакции и записи от момента заказа до оплаты. Эффективные платежи поставщикам могут производиться при доставке товаров, а покупатели могут получать аутентификационные квитанции без какой-либо "бумажной волокиты". Все вспомогательные функции, такие, как оплата счета, получение счета, заказ на покупку, выписывание счета, могут быть интегрированы в доверенный агент для обеспечения невидимой безопасной системы приобретения и доставки.

После разделов 10 "Идентификатор" и 12 "Компоненты" билет 8 содержит в разделе 14 "Подпись эмитента" цифровую подпись, поставленную эмитентом билета. Такая подпись делается при помощи личного, или частного, ключа, принадлежащего доверенному агенту эмитента. Раздел 16 "Сертификат эмитента" содержит подтверждение третьей доверенной стороны (ниже обозначаемой как "доверенное агентство"), используемое вместе с подписью эмитента для проверки подлинности выпущенного билета 8. Такое подтверждение имеет вид сертификата, принадлежащего доверенному агенту эмитента. Общее использование сертификатов и цифровых подписей известно и описано, например, у D.W. Davies и W.L. Price, "Security For Computer Networks" (издательство John Wiley & Sons, 1984).

Раздел 18 "Предыстория передачи" содержит информацию, создаваемую при передаче билета между доверенными агентами после начального выпуска билета 8 продавцом или уполномоченным. Поле 28 "Идентификатор получателя" содержит идентификационный номер принимающего доверенного агента. Поле 30 "Идентификатор отправителя" содержит идентификационный номер отправляющего доверенного агента. Поле 32 "Сертификат отправителя" содержит сертификат отправляющего доверенного агента. Поле 34 "Дата/время" содержит дату и время передачи билета 8. При выполнении последующих передач к соответствующим полям добавляются дополнительные идентификаторы получателя и отправителя, сертификаты отправителя, даты и время, за счет чего создается список информации о предыстории передачи. Необходимо отметить, что идентификатор доверенного агента, находящийся в поле "Получатель" раздела "Идентификатор", должен быть тем же, что и первый идентификатор в поле "Идентификатор отправителя".

Кроме того, когда бы билет 8 ни передавался между доверенными агентами, отправитель подписывает в цифровом виде билет после пяти предыдущих билетных разделов, используя личный ключ, принадлежащий доверенному агенту отправителя. Раздел 20 "Подпись отправителя" затем обновляется путем добавления заново созданной цифровой подписи, за счет чего создается список подписей отправителей.

Устройства транзакций.

На фиг. 3 доверенный агент 120 встроен в устройство 122 транзакций. Устройство 122 транзакций состоит из трех главных компонентов как для продавца, так и для покупателя. Этими компонентами являются центральный процессор 124, доверенный агент 120 и денежный модуль 6. Эти компоненты соединены, например, шиной 126. Когда доверенный агент 120 представляет собой ДАПрод 2, то устройство 122 называется устройством транзакций продавца (УТПрод). Когда доверенный агент 120 представляет собой ДАПок 4, то устройство 122 называется устройством транзакций покупателя (УТПок).

На фиг. 3 показаны функциональные компоненты центрального процессора 124. Центральные функции обеспечивают выполнение следующих функций: функции 128 "Коммуникации", функции 130 "Приложение транзакций", функции 132 "Интерфейс человек-машина", функции 136 "Дата/время" и функции 134 "Менеджер сообщений" (называемой также "Диспетчер сообщений").

Функция 128 "Коммуникации" поддерживает связь между устройством 122 транзакций и внешним миром. Такая связь может быть проводной или беспроводной, широкополосной или узкополосной, при условии, что средства связи УТПок 2 и УТПрод 4 совместимы. Функция 128 "Коммуникации" устанавливает соединение между двумя устройствами 122 транзакций или соединяет устройство транзакций с сетью для не прямой связи с другим устройством транзакций или доверенным сервером.

Функция 130 "Приложение транзакций" может выполнять различные задачи. Например, "Приложение транзакций" может выполнять задачу покупки путем взаимодействия с каталожными услугами сервера продавца по программам просмотра, задачу выбора продуктов и задачу инициализации платежа и доставки. В другом варианте функция "Приложение транзакций" может предусматривать временное хранение электронных объектов и возможное выполнение связанных с конкретным объектом функций. Для выполнения таких связанных с конкретным объектом функций могут быть предусмотрены дополнительные процессоры объектов в зависимости от типа электронного объекта (например, кино, книга, игра и т.д.). В целом устройство 122 транзакций содержит все протоколы процессов, необходимых для выбора, покупки и возможного использования электронных объектов, удостоверений и других билетов 8, или процессов для их продажи.

Функция 132 "Интерфейс человек-машина" для устройства 122 транзакций обеспечивает ввод, просмотр и восприятие информации. Этот интерфейс может представлять собой клавиатуру, мышь, электронное перо, речевой ввод, сенсор-

ный экран, пиктограммы, меню и т.д. Функция 132 "Интерфейс человек-машина" связывается с остальными функциями доверенного агента 120 и денежного модуля 6 через функцию 134 "Менеджер сообщений". В некоторых приложении функция 132 "Интерфейс человек-машина" может не быть необходимой, например, в полностью автоматизированном устройстве транзакций продавца.

Функция 136 "Дата/время" устанавливается владельцем устройства 122 транзакций и содержит дату, время и часовой пояс. Информация о дате/времени передается соответствующему доверенному агенту 120 всегда, когда этот доверенный агент готов к работе.

Функция 134 "Менеджер сообщений" передает межпроцессорные сообщения (т.е. сообщения между устройствами транзакций) и сообщения между центральным процессором 124, доверенным агентом 120 и денежным модулем 6.

Доверенные агенты.

На фиг. 4А показаны функциональные компоненты доверенного агента 120. Описываемая система для открытого электронного бизнеса использует три типа доверенных агентов 120, различающиеся некоторыми уникальными функциями 146 "Транзактор", которые они обеспечивают. На фиг. 4Б показаны функции "Транзактор", находящиеся в ДАПок 2. На фиг. 4В изображены функции "Транзактор", находящиеся в ДАПрод 4. На фиг. 4Г показаны функции "Транзактор", находящиеся в доверенном агенте уполномоченного лица (ДАУ), который, в свою очередь, входит в состав устройства транзакций уполномоченного лица (УТУ). УТУ связано с различными учреждениями, выдающими удостоверения, такими, как Департамент моторного транспорта.

Функция 138 "Внешний интерфейс" обеспечивает физическую связь с центральным процессором 124 и денежным модулем 6 устройства 122 транзакций, в состав которого входит доверенный агент 120. Функция 140 "Интерфейс сообщений" обрабатывает и маршрутизирует межагентские и внутриагентские сообщения. Функция 142 "Менеджер сеанса связи" устанавливает и прерывает сеансы связи между агентами и сеансы связи агента с доверенным сервером. Функция 144 "Менеджер безопасности" обеспечивает поддержку информации о безопасности (например, ведет сертификат доверенного агента и список ненадежных доверенных агентов) и устанавливает защищенную связь с доверенным агентом партнера (через центральный процессор 124) и с местным денежным модулем 6 внутри того же самого устройства 122 транзакций. Функция 146 "Транзактор" содержит протоколы для совершения транзакции. Функции "Транзактор" для покупателя, продавца и уполномоченного лица используются соответственно в ДАПок, ДАПрод и ДАУ.

На фиг. 4Б приведены функции транзактора для покупателя. Функция 158 "Покупка" осуществляет платеж, обменивая платежную сумму на билеты 8 и электронные объекты. Функция 160 "Связь с центральным процессором" обеспечивает взаимодействие с центральным процессором 124 устройства транзакций. Функция 164 "Предъявление билета" предъявляет билеты 8 для получения информации или услуг. Функция 166

"Приобретение удостоверения" служит для получения удостоверяющего билета. Функция 162 "Журнал транзакций" ведет журнал транзакций доверенного агента. ДАПок 2, равно как и ДАПрод 4 обеспечивают поддержку журнала транзакций, в котором хранится следующая информация: тип транзакции (например, тип билета), вид билета до транзакции, вид билета после транзакции, информация о предмете спора, в том числе дата спора (как она записана каждым доверенным агентом в диалоге разрешения спора), статус и резолюция продавца (например, заменить, возместить, отклонить), а также информация о пересертификации (например, дата пересертификации). Функция 168 "Инициализация спора" предъявляет электронную покупку в случае, если покупатель недоволен этой покупкой.

На фиг. 4В показаны функции транзактора для продавца. Функция 170 "Покупка" обменивает билеты 8 и электронные объекты на платеж. Функция 172 "Связь с центральным процессором" обеспечивает взаимодействие с центральным процессором 124 устройства транзакций. Функция 176 "Получение билета" обрабатывает полученный билет 8 для предоставления услуг или информации. Функция 177 "Приобретение удостоверения" получает удостоверение продавца. Функция 174 "Журнал транзакций" осуществляет поддержку журнала транзакций доверенного агента. Функция 178 "Разрешение спора" получает билеты 8 и электронные объекты с целью разрешения жалобы покупателя.

На фиг. 4Г показаны функции транзактора для уполномоченного лица. Функция 180 "Создание удостоверения" формирует и доставляет удостоверяющие билеты запрашивающей стороне. Функция 182 "Связь с центральным процессором" обеспечивает взаимодействие с центральным процессором 124 устройства транзакций. Функция 184 "Получение билета" обрабатывает полученный билет 8 для предоставления услуг или информации, функция 186 "Продление удостоверения" забирает имеющееся удостоверение и заново выпускает удостоверение с новым сроком действия. Функция 183 "Журнал транзакций" ведет журнал транзакций. Функция 185 "Приобретение удостоверения" получает удостоверение уполномоченного лица.

Согласно фиг. 4А функция 150 "Обращение к денежному модулю" связывается с денежным модулем 6 того же устройства 122 транзакции для обеспечения платежа. Функция 152 "Криптография" выполняет криптографические функции по созданию ключа общего пользования (открытого ключа) и симметричного ключа. Для создания ключа общего пользования и симметричного ключа могут использоваться любые хорошо известные методы криптографии, например, RSA-алгоритм (алгоритм цифровой подписи Райвеста-Шамира-Адлемана) и стандарт шифрования данных DES. Функция 148 "Держатель билетов" создает билеты 8 в ДАПрод 4 или же хранит билеты 8 в ДАПок 2 и забирает их оттуда. Функция 156 "Генератор случайных чисел" вырабатывает случайные числа для формирования криптографических ключей. Функция 154 "Дата/время" управляет датой и временем, полученными от центрального процессора 124 для датирования билетов 8 и установления

годности сертификатов и предъявленных билетов. Информация о текущем времени передается на доверенный агент 120 каждый раз, когда доверенный агент готов к работе (т.е. к нему имеется доступ для использования), и поддерживается до тех пор, пока доверенный агент не завершит работу.

Общая структура системы.

На фиг. 5 показана общая архитектура сети рассматриваемой системы для открытого электронного бизнеса. Устройство 188 транзакций покупателя может связываться с продавцом через любую шлюзовую сеть 190, не раскрывая при этом данных о владельце. Таким образом, покупатели могут "двигаться" по сети анонимно, каждый оплачивая доступ в реальном времени. Они могут исследовать электронное пространство продавцов и анонимно входить в него, выбирать предметы для покупки и производить оплату в реальном времени. Система обеспечивает также безопасный платеж на основе проверки полномочий при помощи кредитной или дебетовой карт. Это может быть реализовано путем предъявления покупателем информации, находящейся в кредитной или дебетовой карте и хранящейся в доверенном агенте 120 в качестве удостоверения.

В предпочтительном варианте выполнения шлюзы 190 обеспечивают доступ УТПок 188 к локальным сетям 134 продавца для осуществления сделок и к локальным сетям 192 идентифицирующего уполномоченного лица для приобретения и продления удостоверений (например, водительских прав, кредитных карт и т.д.). Сети 192 продавца могут состоять из серверов 194 продавца, которые предоставляют каталог товаров, устройств 198 транзакций продавца для доставки товаров в обмен на платеж и серверов 196 товаров, которые составляют электронный склад. Сети 192 продавца также предпочтительно имеют доверенные серверы 200 для распределения информации о безопасности.

Сети 202 идентифицирующего уполномоченного лица могут иметь серверы 204 уполномоченного лица, которые ведут базу данных по удостоверениям, и устройство 206 транзакций уполномоченного лица, которое выпускает и продлевает удостоверения. Примерами идентифицирующих уполномоченных лиц, подсоединенных к сетям 202, являются Министерства иностранных дел, Департаменты автотранспорта, банки и Управление социальной безопасности. Сети 202 идентифицирующих уполномоченных также имеют доверенные серверы 200 для распределения информации о защите или безопасности.

Защита системы.

Согласно фиг. 5 защита системы открытого электронного бизнеса обеспечивается при помощи сети доверенных серверов 200, расположенных в сети 208 доверенного агентства, в сетях 192 продавца и в сетях 202 идентифицирующих уполномоченных. Доверенные серверы 200 защищены от несанкционированного доступа процессорами, которые выполняют четыре основные функции: сертификацию доверенных агентов 120, распределение списков недоверия, распределение списков ключей общего пользования основного доверенного сервера и разрешение споров покупателя с продавцом.

На фиг. 6А показана иерархия защиты или безопасности системы. Во главе этой иерархии находятся основные доверенные серверы 210, которые расположены в сети 208 доверенного агентства и которые предоставляют сертификаты доверенных серверов (серт.ДС) всем доверенным серверам 200 в системе.

Каждый основной доверенный сервер 210 имеет свой собственный ключ общего пользования и соответствующий личный ключ. Ключи общего пользования основного доверенного сервера обычно используются совместно всеми доверенными серверами 200 и доверенными агентами 120 в системе. Эти ключи общего пользования хранятся в списке ключей общего пользования основного доверенного сервера ((КОП) ОДС). Используемый здесь и далее в описании термин "ключ общего пользования" не означает, что этот ключ является общедоступным. В данном случае, например, ключ общего пользования известен лишь всем доверенным серверам 200 и доверенным агентам 120 и "запечатан" в их защищенных от несанкционированного доступа корпусах. Такое ограниченное понимание термина "общее пользование" обеспечивает дополнительную безопасность всей системы.

Вслед за основным доверенным сервером 210 в иерархии безопасности следуют доверенные серверы 200, которые могут быть расположены по всей системе электронного бизнеса. Доверенные серверы 200 предоставляют сертификаты доверенных агентов (серт.ДА) доверенным агентам 120 (т.е. ДАПок 2, ДАПрод 4 и ДАУ 212).

Доверенное агентство гарантирует предоставление протоколов и физическую защиту для каждого доверенного агента 120 в системе. Доверенные агенты 120 изготавливаются в физически защищенных условиях под контролем доверенного агентства. Компоненты изготавливают, собирают и загружают в них соответствующие программы в этих условиях. В результате доверенные агенты 120 защищены от несанкционированного доступа, а связь с ними может быть установлена только через их внешний интерфейс.

При инициализации каждый доверенный агент 120 связывается с доверенным сервером

200. Доверенный сервер 200 присваивает каждому доверенному агенту 120 уникальный идентификационный номер (ид) ДА. Затем доверенный сервер 200 посылает запрос доверенному агенту 120 на создание пары ключей, состоящей из ключа общего пользования и личного ключа. Доверенный агент 120 создает эту пару ключей и передает свой ключ общего пользования (КОП)ДА доверенному серверу 200, пославшему запрос. Доверенный сервер 200 вносит эту информацию и (ид) ДА в сертификат доверенного агента серт.(ДА) и возвращает сертификат доверенному агенту 120 вместе со списком (КОП) ОДС и списком ненадежных доверенных агентов. В завершение доверенный агент 120 проверяет свой вновь полученный сертификат и удостоверяется, что этот сертификат действителен.

Такая инициализация выполняется только один раз перед выдачей доверенного агента 120 пользователю. При покупке владелец вводит в доверенный агент 120 персональные данные с помощью биометрии или скрытой информации (например, выбирает персональный идентификационный номер (ПИН)).

Аналогичным образом доверенный сервер 200 инициализируется основным доверенным сервером 210. После решения об инициализации доверенного сервера каждый доверенный сервер 200 содержит сертификат серт.(ДС), хранящий уникальный идентификационный номер доверенного сервера (ид)ДС и ключ общего пользования доверенного сервера (КОП)ДС. Доверенный сервер 200 также содержит личный ключ, соответствующий его ключу общего пользования (КОП)ДС, список (КОП)ОДС и список ненадежных доверенных агентов.

Сертификат серт.(ДС) шифруется основным доверенным сервером 210 и содержит уникальный идентификационный номер основного доверенного сервера 210 (ид)ОДС в открытом виде. Сертификат серт.(ДА) шифруется доверенным сервером 200 и содержит сертификат серт.(ДС) этого доверенного сервера для проверки действительности.

Серт.(ДС) и серт.(ДА) имеют следующие структуры:

$$\begin{aligned} \text{Серт. (ДС)} &= \frac{E_{\text{ОДС}}[(\text{ид}) \text{ ДС} \| (\text{КОП ДС}) \| \text{срок действия} \| \sigma_{\text{ОДС}}(X)] \| (\text{ид}) \text{ ОДС}}{X} \\ \text{Серт. (ДА)} &= \frac{E_{\text{ДС}}[(\text{ид}) \text{ ДА} \| (\text{КОП ДА}) \| \text{срок действия} \| \sigma_{\text{ДС}}(Y)] \| \text{серт. (ДС)}}{Y} \end{aligned}$$

где ОДС - основной доверенный сервер,

ДС - доверенный сервер,

ДА - доверенный агент,

II ~ символ конкатенации,

ид - идентификационный номер,

КОП - ключ общего пользования,

$\sigma$  - цифровая подпись,

серт. - сертификат,

Е - означает алгоритм, в котором личный ключ используется для шифрования и создания цифровой подписи.

Протоколами подтверждения сертификата являются следующие:

1) Подтверждение действительности серт. (ДС)

а)  $D_{\text{ОДС}}(E_{\text{ОДС}}(X \| \sigma_{\text{ОДС}}(X))) = X \| \sigma_{\text{ОДС}}(X)$ ;

б) проверить, действительна ли дата;

в) проверить, соблюдается ли

$D_{\text{ОДС}}(\sigma_{\text{ОДС}}(X)) = h(X)$ .

2) Подтверждение действительности серт. (ДА)

а) подтвердить действительность серт.(ДС);

б)  $D_{\text{ДС}}(E_{\text{ДС}}(\sigma_{\text{ДС}}(Y))) = Y \| \sigma_{\text{ДС}}(Y)$ ;

в) проверить, действительна ли дата;

г) проверить, соблюдается ли

$D_{\text{ДС}}(\sigma_{\text{ДС}}(Y)) = h(Y)$ .

где  $h$  является хэш-функцией, используемой при создании цифровой подписи (т.е. односторонняя функция),

Д - алгоритм с использованием ключа общего пользования для расшифровывания и для проверки цифровой подписи,  $\sigma = E \cdot h$ .

Следует заметить, что Е и D могут также использоваться соответственно для расшифровывания и шифрования в случае применения в других приложениях.

В дополнение к своим функциям, выполняемым при изготовлении и инициализации компонентов системы, доверенное агентство обеспечивает также текущую защиту системы путем пересертификации доверенных агентов 120 и доверенных серверов 200 и предоставления общесистемной информации по обновленным спискам ненадежных доверенных агентов и обновленным спискам (КОП) ОДС.

Доверенные агенты 120 и доверенные серверы 200 должны периодически пересертифицироваться, поскольку их сертификаты содержат дату окончания срока действия. Доверенные серверы 200 периодически пересертифицируются для защиты общесистемной безопасности путем изменения их криптографических ключей. Временное ограничение на возможность совершать транзакции доверенными агентами налагается таким образом, чтобы кто-либо, внезапно начавший работать в системе, мог использовать своего доверенного агента 120 только в течение заданного максимального периода времени (например, три месяца) до момента, когда необходима пересертификация. В процессе пересертификации доверенные агенты 120 связываются с доверенным агентством для получения информации о безопасности (например, обновленных списков ненадежных доверенных агентов) и для получения обновленного списка (КОП) ОДС.

Ключ общего пользования, связанный с каждым основным доверенным сервером 210, никогда не меняется. Если вводятся новые или списываются старые основные доверенные серверы 210, то корректировки списка (КОП) ОДС транслируются доверенным серверам 200 по сети 208 доверенного агентства. Эти изменения списка затем распределяются среди доверенных серверов 200 в сетях 202 идентифицирующих уполномоченных лиц и сетях 192 продавцов и могут в любое время запрашиваться доверенным агентом 120 и передаваться ему. Изменения списка также всегда передаются доверенным агентам 120, когда заканчивается срок действия их сертификатов, и они пересертифицируются. Новые значения (КОП) ОДС распределяются до их введения в действие, чтобы исключить возможность их отсутствия у доверенного агента 120 на момент необходимости подтверждения действительности сертификатов.

Идентификационные номера доверенных агентов 120 или доверенных серверов 200, идентифицированных как ненадежные, помещаются основным доверенным сервером 210 в список ненадежных доверенных агентов и сообщаются доверенным серверам 200, а затем доверенным агентам 120 таким же образом, как и список (КОП) ОДС. Доверенные серверы 200 продавцов, считающихся не вызывающими доверия или ненадежными, будут списаны доверенным агентством, а информация об этих продавцах станет известна доверенным агентам 120.

На фиг. 6Б представлены функциональные компоненты доверенного сервера 200 или основного доверенного сервера 210. Функция 214 "Ком-

муникации" обеспечивает взаимодействие с локальной сетью. Функция 216 "Менеджер сеанса связи" управляет сеансами связи внутри сервера и сервера с агентом, функция 218 "Менеджер безопасности" служит для установления безопасной связи, функция 220 "Менеджер списка недоверия" обеспечивает обновление списка ненадежных агентов, серверов и организаций. Функция 222 "Сертификация" управляет пересертификацией доверенных агентов 120 для доверенного сервера 200. В случае основного доверенного сервера 210 этот процесс пересертифицирует доверенные серверы 200. Функция 224 "Разрешение спора" принимает билеты 8 и электронные объекты (покупки) для разрешения претензий покупателя, функция 228 "Криптография" обеспечивает шифрование при помощи симметричного ключа и ключа общего пользования для засекречивания связи и аутентификации сторон-участников. Функция 226 "Дата/время" предоставляет текущую информацию о дате, времени и часовом поясе для подтверждения действительности сертификата.

Вопрос о неисправной работе или потере доверенного агента 120 аналогичен вопросу о потере квитанции, авиабилета и т.д. В случаях, когда потеря или неисправность должна быть устранена, может потребоваться идентификация транзактора. Это может быть реализовано путем использования удостоверений, которые идентифицируют покупателя и доверенного агента 120. Удостоверение и билет 8 могут сохраняться отдельно в виде вторичных записей. В случае неисправности агента покупатель может возбудить спор, как он сделал бы это на сегодняшний день, путем предъявления этих вторичных записей.

Блок-схемы алгоритмов.

В изображенных на последующих чертежах блок-схемах алгоритмов используются обозначения "А" и "В" для указания двух взаимодействующих доверенных агентов 120 или взаимодействия доверенного агента 120 с доверенным сервером 200. Те же самые обозначения А и В применимы и к центральному процессору 124 или денежному модулю 6, связанным с отдельным доверенным агентом 120 (т.е. находящиеся внутри того же устройства 122 транзакций). На блок-схемах алгоритмов показан функциональный компонент, в первую очередь отвечающий за выполнение данной задачи. Например, МЕНЕДЖЕР БЕЗОПАСНОСТИ А означает, что соответствующая задача выполняется функцией 144 "Менеджер безопасности" (см. фиг. 4А) в доверенном агенте А.

Блок-схемы алгоритмов также вызывают подпрограммы, в некоторых из которых для обозначения параметров используются буквы X и Y. Например, УСТАНОВИТЬ СЕАНС СВЯЗИ А -> В является вызовом подпрограммы "Установить сеанс связи". При дальнейшем продвижении по блок-схеме алгоритма "Установление сеанса связи" подразумевается, что X = А, а Y = В.

Прекращение и фиксация транзакций.

В рассматриваемом типе обработки транзакций между двумя сторонами необходимо передавать электронные объекты, например, билеты 8, и электронные банкноты, поддерживая "игру с нулевой суммой". Иными словами, нежелательно дублировать электронные объекты, чтобы

по окончании электронной транзакции имелось в два раза больше объектов, чем до транзакции. Подобным же образом нежелательно терять электронные объекты, чтобы после транзакции их было меньше, чем до транзакции. Например, если в начале транзакции А имеет один электронный билет 8 и желает передать его В, то необходимо гарантировать, что в конце транзакции у В будет один электронный билет 8, а у А не будет электронных билетов 8. На практике, однако, возможны два других исхода, а именно: А и В имеют один и тот же электронный билет 8 (дублирование), либо ни А, ни В не имеют электронного билета 8 (потеря).

С целью свести вероятность дублирования или потери к пренебрежимо малым значениям протокол транзакции должен учитывать возможность того, что естественные или преднамеренные события могут прервать типичный ход транзакции. Примером естественного прерывания является прерывание связи между А и В во время транзакции. Для минимизации вероятности дублирования или потери из-за таких случайных событий возможные пределы дублирования или потери должны быть сведены к минимуму. Для минимизации преднамеренных прерываний (т.е. откровенных вторжений) целесообразно устранить экономические стимулы таких вторжений. Например, если вторгающийся может лишь потерять билеты и/или деньги, пытаясь прервать транзакцию, то у него не будет никаких стимулов для начала такого вторжения.

Эти концепции реализованы в эффективных протоколах транзакций описываемой системы. В частности, целесообразно обеспечить согласованные состояния прерывания и фиксации между двумя совершающими транзакцию доверенными агентами 120 (или денежными модулями 6). Например, если А фиксирует транзакцию, то и В должен фиксировать эту транзакцию, или если А прекращает транзакцию, то и В тоже должен ее прекратить. Для достижения согласованности и минимизации возможности дублирования или потери (в случае наличия несогласованности) протоколы транзакций учитывают порядок и время, когда А и В фиксируют данную транзакцию.

На фиг. 7 показаны две подпрограммы: "Прекращение" и "Фиксация". Подпрограмма прекращения выполняется внутри данного доверенного агента 120, когда транзакция, в которую он вовлечен, дает сбой. Подпрограмма прекращения возвращает доверенный агент 120 в точно такое же состояние, в котором он был до начала неудачной транзакции. В отличие от этого подпрограмма фиксации транзакции выполняется внутри доверенного агента 120, когда транзакция, в которую он вовлечен, успешно завершена. Доверенный агент 120 записывает завершенную транзакцию в свой журнал транзакций и готов к новой транзакции. Например, во время транзакции передачи билета электронный билет 8 передается от доверенного агента А доверенному агенту В. Поскольку в этот момент времени ни А, ни В не фиксировали и не прекращали транзакцию, А условно сохраняет билет 8, тогда как В также условно имеет билет 8. Если и А и В зафиксировали транзакцию, то А уничтожит свой билет 8, а на-

личие у В билета 8 перестанет быть условным. Если же А и В прекратили транзакцию, то А сохранит свой билет 8, а билет 8, который условно имел В, будет уничтожен путем возврата к началу транзакции. Следует отметить, что операция уничтожения может быть реализована различными способами, хорошо известными из уровня техники. Как отмечалось ранее, целесообразно свести к минимуму возможность фиксации одним доверенным агентом 120 транзакции в то время, когда другой доверенный агент 120 прекратил ее, поскольку при некоторых ограниченных условиях это может привести к дублированию или потере электронных объектов.

Подобная ситуация имеет место и по отношению к денежным модулям 6, обменивающимся электронными банкнотами. В течение транзакции покупки электронные банкноты передаются от денежного модуля А денежному модулю В, так что А условно уменьшает свои электронные банкноты (на переданное количество), в то время как В условно имеет электронные банкноты (в количестве, равном переданному). Если и А, и В фиксируют транзакцию, то у А остается уменьшенное количество банкнот, а наличие электронных банкнот у В более не является условным.

На фиг. 7А приведена подпрограмма фиксации транзакции. Функция "Журнал транзакций Х" обновляет журнал транзакций. Функция "Связь с центральным процессором Х" оповещает центральный процессор, что транзакция завершена. Функция "Менеджер сеанса связи Х" записывает конец сеанса связи (шаги 230-234).

На фиг. 7Б представлена подпрограмма прекращения транзакции. Функция "Менеджер сеанса связи Х" отменяет изменения и записывает, что агент прекратил транзакцию. Функция "Менеджер сеанса связи" отслеживает действия, совершенные с начала транзакции, и отменяет эти шаги. Функция "Связь с центральным процессором Х" посылает сообщение центральному процессору, что транзакция прекращена (шаги 236-238).

Подпрограмма прекращения может быть вызвана непосредственно из блок-схемы алгоритма, например, когда доверенный агент 120 определяет, что сертификат недействителен. Подпрограмма прекращения может быть вызвана также в том случае, когда ожидаемое действие не происходит. В частности, когда два доверенных агента 120 связываются друг с другом, они будут отслеживать протокол истечения времени ожидания события. Например, после того, как первый доверенный агент 120 послал сообщение второму доверенному агенту 120, менеджер сеанса связи первого доверенного агента (А) установит таймер ожидания ответа, если требуется ответ. Функция "Менеджер сеанса связи" может также пронумеровать посланное сообщение. Этот номер появится в ответном сообщении от функции "Менеджер сеанса связи" второго доверенного агента (В).

Если таймер закончит отсчет до того, как сообщение принято, то функция "Менеджер сеанса связи А" направит запрос функции "Менеджер сеанса связи В" определить, продолжает ли происходить выполнение транзакции в В. Если В не отвечает, то функция "Менеджер сеанса связи А" прекратит транзакцию. Если принят ответ, что



транзакция продолжает выполняться, то таймер будет переустановлен на новое время. Если А запрашивает В определенное число раз, не получая ответа на исходное сообщение, то А прекращает транзакцию. Подобные же функции истечения времени ожидания события существуют в денежных модулях 6.

Пересертификация доверенного агента.

На фиг.8 показана блок-схема пересертификации доверенного агента. Когда владелец доверенного агента А решает пересертифицировать своего агента, обычно после или незадолго до даты истечения срока действия текущего сертификата (серт.(ДА)), приложение транзакций центрального процессора связывается с доверенным сервером В через этот центральный процессор, который входит в состав его устройства транзакций (шаги 240-242).

Далее для установления криптографически безопасного канала связи между доверенным агентом А и доверенным сервером В вызывается подпрограмма "Установление сеанса связи" (шаг 244). Согласно фиг.9 функция "Менеджер сеанса связи" доверенного агента А запрашивает, а затем получает сертификат А (т.е. (серт.(ДА)) от функции "Менеджер безопасности" (шаги 296-298). Затем функция "Менеджер сеанса связи А" посылает этот сертификат функции "Менеджер сеанса связи" доверенного сервера В, который, в свою очередь, посылает его своей функции "Менеджер безопасности" (шаги 300-304).

Функция "Ключ общего пользования" доверенного сервера В проверяет серт.(ДА) при помощи протоколов проверки действительности, представленных выше при описании безопасности системы (шаги 306-308). Однако существует предупреждение, что когда функция "Установление сеанса связи" вызывается во время процедуры продления срока действия, описанный ранее протокол подтверждения действительности сертификата не прерывается, если он определяет, что сертификат просрочен, что является причиной пересертификации доверенного агента.

Если серт.(ДА) недействителен, то функция "Менеджер сеанса связи В" записывает, что сеанс связи прекращен, и информирует функцию "Менеджер сеанса связи А", что транзакция отменена. Функция "Менеджер сеанса связи А" также записывает, что сеанс связи прекращен (шаги 310-312). Если серт.(ДА) действителен, то функция "Менеджер безопасности В" проверяет, не состоит ли доверенный агент А в списке ненадежных агентов (шаги 314-316). Если доверенный агент А является ненадежным, то сеанс связи прекращается (шаги 310-312).

Если А нет в списке ненадежных агентов, то функция "Генератор случайных чисел В" создает случайное число R(B), а также проверочное сообщение В (шаг 318). Случайное число R(B) будет в итоге использовано для формирования ключа сеанса связи. Проверочное сообщение В является случайным числом, используемым В для защиты от повторного запуска сообщения. Далее функция "Менеджер безопасности В" объединяет R(B), проверочное сообщение В и серт.(ДС) в сообщение для доверенного агента А (шаг 320). Функция "Ключ общего пользования В" зашифровывает

сообщение при помощи ключа общего пользования доверенного агента А (КОП)ДА, который доверенный сервер В принимает вместе с сертификатом доверенного агента А (серт.(ДА)) (шаг 322). После этого функция "Менеджер сеанса связи В" посылает зашифрованное сообщение функции "Менеджер сеанса связи А" (шаги 324-326).

Функция "Ключ общего пользования А" расшифровывает сообщение при помощи своего личного, или частного, ключа (соответствующего ее ключу общего пользования) и проверяет действительность сертификата серт.(ДС) (шаги 328-330). Если серт.(ДС) недействителен, то функция "Менеджер сеанса связи А" записывает, что сеанс связи прекращен, и посылает сообщение об отмене транзакции к В, функция "Менеджер сеанса связи" которого также записывает, что сеанс связи прекращен (шаги 332-334). Если же серт.(ДС) действителен, то функция "Менеджер безопасности А" проверяет, не состоит ли доверенный сервер В в списке ненадежных агентов (шаги 336-338). Если доверенный сервер В есть в этом списке, сеанс связи прекращается (шаги 332-334).

Если же В не состоит в указанном списке ненадежных агентов, то функция "Генератор случайных чисел А" создает случайное число R(A) и проверочное сообщение А (например, другое случайное число) (шаг 340). Функция "Дата/время" передает текущие дату и время функции "Менеджер безопасности" (шаг 342). А и В обмениваются датой и временем для окончательной записи в их журналы транзакций во время фиксации, функция "Менеджер безопасности А" затем формирует и сохраняет ключ сеанса связи доверенного агента с доверенным агентом (ДА/ДА) при помощи операции "ИСКЛЮЧАЮЩЕЕ ИЛИ" над числами R(A) и R(B) (шаг 344). Функция "Ключ сеанса связи" (ДА/ДА) используется для шифрования связи между двумя доверенными агентами 120 или между доверенным агентом 120 и доверенным сервером 200 (как в приведенном случае, когда функция "Установление сеанса связи" вызывается во время пересертификации).

Функция "Менеджер сеанса связи А" компонует сообщение, содержащее проверочные сообщения А и В, информацию о дате/времени, а также R(A) (шаг 344). Функция "Ключ общего пользования А" шифрует это сообщение при помощи ключа общего пользования доверенного сервера В (который А получил с сертификатом серт.(ДС) и посылает зашифрованное сообщение функции "Менеджер сеанса связи" доверенного сервера В (шаги 346-350).

Функция "Ключ общего пользования В" расшифровывает полученное сообщение при помощи своего частного, или личного, ключа (соответствующего ее ключу общего пользования) (шаг 352). Функция "Менеджер безопасности В" проверяет, является ли проверочное сообщение В, полученное от А, тем же самым проверочным сообщением В, которое было до этого послано А (шаги 354-356). Если они не совпадают, то сеанс связи прекращается (шаги 310-312). Если же они одинаковы, то функция "Менеджер сеанса связи В" записывает начало сеанса связи (шаг 358).

Функция "Менеджер безопасности В" формирует ключ сеанса связи (ДА/ДА) при помощи

операции "ИСКЛЮЧАЮЩЕЕ ИЛИ" над R(A) и R(B), а затем сохраняет этот ключ сеанса связи (шаг 360). В этот момент и A, и B создали и сохранили один и тот же ключ сеанса связи (т.е. ключ сеанса связи (ДА/ДА)) для использования в их текущем взаимодействии при пересертификации A. Далее функция "Дата/время B" посылает свою текущую информацию о дате и времени функции "Менеджер безопасности B" (шаг 362). Функция "Менеджер безопасности B" компонует сообщение, содержащее подтверждение о приеме A, проверочное сообщение A и информацию B о дате/времени (шаг 364). Затем вызывается подпрограмма "Посылка сообщения" (шаг 366) для посылки сообщения от B к A.

Согласно фиг. 10 функция "Симметричный ключ" доверенного сервера B зашифровывает сообщение при помощи ключа сеанса связи (ДА/ДА) (шаг 376). Затем функция "Интерфейс сообщений B" форматирует сообщение и посылает его функции "Менеджер сообщений" центрального процессора (шаг 378). Функция "Менеджер сообщений центрального процессора B" затем направляет сообщение через функцию "Коммуникации" функции "Менеджер сообщений центрального процессора A" в центральном процессоре доверенного агента A (шаг 380).

После этого функция "Менеджер сообщений центрального процессора A" посылает это сообщение функции "Интерфейс сообщений" доверенного агента A, который разбирает это сообщение (шаги 382-384). Функция "Симметричный ключ A" расшифровывает сообщение при помощи ключа сеанса связи (ДА/ДА), завершая таким образом безопасную передачу сообщения между доверенным сервером и доверенным агентом с использованием ключа сеанса связи (ДА/ДА) (шаг 386).

На фиг. 9 функция "Менеджер безопасности A" принимает подтверждение о приеме, проверочное сообщение A и информацию B о дате/времени (шаг 368). Функция "Менеджер безопасности A" проверяет, является ли проверочное сообщение A тем же самым проверочным сообщением A, которое A ранее посылал к B (шаги 370-372). Если эти сообщения не совпадают, то функция "Менеджер сеанса связи A" прекращает сеанс связи (шаги 332 - 334). Если же они одинаковы, то функция "Менеджер сеанса связи A" записывает начало сеанса связи (шаг 374).

Далее процесс пересертификации продолжается в соответствии с фиг.8. Функция "Менеджер безопасности A" посылает запрос функции "Ключ общего пользования A" на создание новой пары ключей, состоящей из ключа общего пользования и частного ключа, и затем на подпись в цифровом виде нового ключа общего пользования при помощи старого частного ключа (соответствующего старому (КОП) ДА) (шаги 246-248). Как описано выше, пара из ключа общего пользования и частного ключа доверенного агента используется при установлении сеанса связи между доверенными агентами 120 или между доверенным агентом 120 и доверенным сервером 200.

Функция "Менеджер безопасности A" компонует сообщение, содержащее новый подписанный ключ общего пользования и номер текущей версии списка ненадежных агентов (шаг 250). Каждое

изменение списка ненадежных агентов имеет номер новой версии, и поэтому доверенный сервер должен только вносить изменения в список. Затем сообщение посылается доверенному серверу B при помощи подпрограммы "Посылка сообщения" (шаг 252). Доверенный сервер B принимает сообщение и проверяет, действительна ли цифровая подпись на новом ключе общего пользования (при помощи старого ключа общего пользования доверенного агента A) (шаги 254-258). Если подпись недействительна, то вызывается подпрограмма "Прекращение транзакции" (шаг 260).

На фиг. 11 доверенный сервер B прекращает транзакцию (шаг 388), а его функция "Менеджер сеанса связи" посылает функции "Менеджер сеанса связи" доверенного агента A сообщение, информирующее A, что B прекратил транзакцию (шаги 390-394). После этого доверенный агент A прекращает транзакцию (шаг 396).

Как показано далее на фиг. 8, если подпись на новом ключе общего пользования действительна, то доверенный сервер B создает новый сертификат (серт.(ДА)), содержащий новый ключ общего пользования и новую дату окончания срока действия. Затем новый сертификат посылается обратно A вместе с последней версией списка недоверия и последней версией списка (КОП) ОДС (шаги 262-264). Функция "Менеджер безопасности A" принимает это сообщение, а функция "Ключ общего пользования A" проверяет, действителен ли новый сертификат (шаги 268-270).

Если сертификат недействителен, то функция "Менеджер безопасности A" проверяет, пытался ли доверенный сервер B создать новый сертификат менее трех раз (шаг 274). Если это так, то функция "Менеджер безопасности A" посылает доверенному серверу B сообщение, чтобы тот снова попытался создать сертификат (шаги 280-284). Если доверенный сервер не способен создать действительный сертификат серт.(ДА), то функция "Журнал транзакций A" записывает попытку как неудачную и прекращает транзакцию (шаги 276-278).

Если доверенный сервер посылает действительный новый сертификат серт.(ДА), то функция "Менеджер безопасности A" обновляет серт.(ДА), список недоверия и список (КОП) ОДС (шаг 286). После этого доверенный агент A фиксирует транзакцию (шаг 288). Функция "Менеджер безопасности A" посылает доверенному серверу сообщение о том, что доверенный агент обновил свой сертификат. Затем доверенный сервер B записывает, что A пересертифицирован (шаги 290-294).

Покупка электронных товаров.

Покупка электронных товаров описана со ссылками на фиг. 12. Объекты, покупаемые в соответствии с блок-схемой по фиг. 12, включают электронные объекты и связанные с ними билеты расшифровки, транспортные билеты, билеты на мероприятия и билеты на услуги связи. Удостоверения, с другой стороны, приобретаются при помощи блок-схемы алгоритма "Приобретение удостоверения" (фиг. 26). Приложение транзакций покупателя (ПТПок) в центральном процессоре 124 устройства 188 транзакций покупателя соединяется с сервером 194 продавца в сети 192 продавца. ПТПок позволяет покупателю просматривать то-

вары продавца и делать выбор (шаги 398-400). ПТПок посылает идентификатор выбранного товара серверу 194 продавца (шаг 402). Затем ПТПок посылает доверенному агенту А (находящемуся в том же самом устройстве транзакций покупателя) сообщение, дающее команду доверенному агенту А купить выбранный товар и идентифицирующее его. Сервер продавца также посылает доверенному агенту В устройства 198 транзакций продавца сообщение, дающее доверенному агенту В команду продать выбранный товар и идентифицирующее его (шаги 404-406).

Затем между доверенным агентом А и доверенным агентом В устанавливается сеанс связи, когда и А, и В могут связываться друг с другом при помощи заново созданного ключа сеанса связи (ДА/ДА) (шаг 408). На фиг. 13 изображены четыре канала шифрования, устанавливаемые в процессе транзакции покупки. Канал 436 шифрования между двумя доверенными агентами 120 передает сообщения, зашифрованные ключом сеанса связи доверенного агента с доверенным агентом (ДА/ДА). Каналы 438 и 440 между доверенным агентом 120 и его денежным модулем 6 совместно используют ключ сеанса связи доверенного агента с денежным модулем (ДА/ДМ). Канал 442 между денежными модулями 6 в различных устройствах 122 транзакций использует ключ сеанса связи денежного модуля с денежным модулем (ДМ/ДМ).

Далее согласно фиг. 12 вызывается подпрограмма "Проверка действительности удостоверения" (шаг 410). Все устройства 198 транзакций продавца содержат удостоверение, идентифицирующее владельца/продавца (например, NYNEX, Ticketron и т.д.). Такое удостоверение продавца может быть выдано, например, службой идентификации продавцов, контролируемой доверенным агентством. С другой стороны, удостоверение покупателя, содержащиеся в устройстве 188 транзакций покупателя, могут представлять собой водительские права или кредитные карты, эмитированные различными идентифицирующими уполномоченными лицами. Согласно фиг. 14 функция "Покупка А" посылает сообщение к функции "Покупка В" доверенного агента В, запрашивающее его удостоверение продавца (шаги 444-448). Функция "Держатель билетов В" затребует удостоверение продавца и посылает это удостоверение к А для подтверждения действительности (шаги 450-456).

Удостоверения или любой другой тип билета 8 проверяются на действительность следующим образом.

- 1) Проверяется действительность сертификата эмитента и подпись эмитента.
- 2) Проверяется каждая передача - на совпадение идентификаторов получателя и отправителя (т.е. если  $S_0$  = эмитент,  $R_0$  = первый получатель, то  $R_i = S_{i+1}$ , где  $i \geq 0$ ).
- 3) Проверяется действительность сертификата каждого отправителя и подпись каждого отправителя.
- 4) Проверяется совпадение идентификатора последнего получателя с идентификатором (ид (ДА)) сертификата доверенного агента (серт.(ДА)) в текущем сеансе связи.

Если удостоверение продавца недействительно, то транзакция прекращается (шаг 458). Если удостоверение продавца действительно, то функция "Связь с центральным процессором А" посылает информацию об удостоверении приложению центрального процессора, осуществляющему контроль за передачей, для подтверждения (например, визуального подтверждения имени продавца владельцем доверенного агента покупателя) (шаги 460-462).

На фиг. 12 функция "Покупка В" запрашивает выбранный товар у сервера товаров, который затребует товар и посылает его функции "Покупка В" для подтверждения идентичности (шаги 412-418). Если этот товар не совпадает с выбранным, то товар затребуется еще дважды, после чего транзакция прекращается (шаги 420-422). Если доверенным агентом В получен товар, соответствующий выбранному, то вызывается подпрограмма "Доставка покупки" (шаг 424).

На фиг. 15 функция "Покупка В" проверяет, является ли покупка только билетом (в отличие от билета расшифровки и электронного объекта) (шаги 464-466). Если покупка представляет собой только билет, то функция "Держатель билетов В" создает билет (шаг 468). Затем функция "Покупка В" посылает билет доверенному агенту А (шаги 470-472). Функция "Покупка А" принимает билет и проверяет его правильность путем сравнения с идентификатором ожидаемой покупки (ранее полученным от ПТПок) с информацией в билете (шаги 474-476). Если билет неправильный, то функция "Покупка А" идентифицирует транзакцию как покупку и, следовательно, прекращает транзакцию (шаги 478-482). Если доверенный агент А считает билет правильным, то он затем посылает информацию билета приложению транзакций центрального процессора для проверки покупателем (шаги 486-488). Такая информация позволяет владельцу доверенного агента покупателя убедиться в том, что он получает именно тот товар и по той цене, которые он предварительно выбрал. Если информация билета неправильна, то транзакция прекращается (шаги 478-482). Если билет правильный, то функция "Покупка А" посылает билет к функции "Держатель билетов А" для хранения (шаги 490-492). Теперь доверенный агент А условно имеет билет 8. Если доверенный агент А затем прекращает транзакцию, то билет 8 уничтожается. Если же доверенный агент А затем фиксирует транзакцию, то владелец А сможет предъявлять билет 8.

С другой стороны, если покупаемый товар состоит как из электронного объекта, так и из соответствующего ему билета расшифровки, то функция "Генератор случайных чисел В" в доверенном агенте В продавца создает случайный ключ (шаг 494). Затем функция "Симметричный ключ В" шифрует электронный объект при помощи этого случайного ключа, а функция "Ключ общего пользования В" подписывает в цифровом виде зашифрованный электронный объект при помощи частного ключа доверенного агента продавца (шаги 496-498). Затем функция "Держатель билетов В" создает билет расшифровки, содержащий случайный ключ, цену и другую информацию (шаг 500). Владелец доверенного агента А может теперь получить зашифрованный электронный

объект от продавца, но он не сможет использовать его, пока не будет иметь доступа к случайному ключу, содержащемуся в соответствующем билете расшифровки.

Функция "Покупка В" посылает зашифрованный электронный объект и билет расшифровки доверенному агенту А (шаги 502-504). Функция "Покупка А" принимает сообщение и передает зашифрованный электронный объект центральному процессору, сохраняя копию зашифрованной информации заголовка (шаг 506). Одновременно функция "Ключ общего пользования А" проверяет подпись на зашифрованном электронном объекте при помощи функции "Ключ общего пользования В" (шаги 508-510). Если подпись неправильная, то транзакция прекращается (шаги 478-482). Если проверяется целостность электронного объекта, то функция "Симметричный ключ А" расшифровывает заголовок при помощи случайного ключа, взятого из билета расшифровки (шаг 512). Функция "Покупка А" проверяет идентичность электронного объекта и билета расшифровки (шаги 514-516). Такая проверка может выполняться путем сравнения идентификатора ожидаемого товара с идентификатором электронного объекта и с информацией, содержащейся в билете расшифровки. Таким образом, подтверждается, что выбранный товар, электронный объект и билет расшифровки соответствуют друг другу. Если проверка идентичности дает отрицательный результат, транзакция прекращается (шаги 478-482).

Если электронный объект и билет расшифровки правильные, то функция "Покупка А" посылает расшифрованные заголовки и цену приложению транзакций центрального процессора для подтверждения покупателем (шаги 518, 488). Если покупатель не принимает товар, то транзакция прекращается (шаги 478-482). Если же покупатель принимает товар, то функция "Покупка А" посылает билет расшифровки на хранение функции "Держатель билетов А" (шаги 490-492).

Согласно фиг. 12, когда доставка покупки от продавца покупателю закончена (и покупка недоступна для покупателя вследствие того, что она зашифрована или хранится в доверенном агенте 2), функция "Покупка А" в данном случае посылает приложению транзакций центрального процессора сообщение, запрашивающее предпочтительный для покупателя способ оплаты (шаги 426-428). Оплата может производиться одним из двух альтернативных способов: анонимным платежом при помощи денежного модуля 6 или платежом на основе проверки полномочий (для чего необходима идентификация покупателя) при помощи удостоверения в виде кредитной или дебетовой карты.

Если используется анонимная оплата, то вызывается подпрограмма "Платеж денежным модулем" (шаг 430). Согласно фиг. 16 функция "Генератор случайных чисел А" создает случайное число R(1) (шаг 520). Функция "Покупка А" затем посылает доверенному агенту В сообщение, указывающее на то, что будет произведен "платеж через денежный модуль", соответственно "платеж денежным модулем", а также содержащее R(1) (шаги 522-524). Функция "Покупка В" принимает это сообщение и посылает R(1) функции "Менеджер безопасности В" (шаги 526-528). Функция "Ге-

нератор случайных чисел В" создает случайное число R(2) и посылает его доверенному агенту А (шаги 530-532). Функции "Менеджеры безопасности А и В" совместно формируют ключ сеанса связи (ДА/ДМ) при помощи операции ИСКЛЮЧАЮЩЕЕ ИЛИ над R(1) и R(2) (шаги 534-536).

Согласно фиг. 13 ключ сеанса связи (ДА/ДМ) используется для шифрования сообщений, передаваемых между доверенным агентом 120 и относящимся к нему денежным модулем 6 по каналам 438 и 440 шифрования. В этой точке блок-схемы алгоритма только два доверенных агента 120 имеют ключ сеанса связи (ДА/ДМ). Оба денежных модуля 6 по блок-схеме формируют копии ключа сеанса связи (ДА/ДМ) в более позднее время, чтобы инициализировать обмен зашифрованными сообщениями между доверенными агентами 120 и их денежными модулями 6.

Следует отметить, что вместо реализации доверенного агента 120 и денежного модуля 6 в виде дискретных, защищенных от несанкционированного доступа компонентов, их можно выполнить в виде одного защищенного от несанкционированного доступа модуля. В этом случае необязательно устанавливать безопасный сеанс связи между доверенным агентом 120 и денежным модулем 6 в одном и том же устройстве 122 транзакций. Однако дискретные денежные модули 6 и доверенные агенты 120 предпочтительны в том отношении, что такая конфигурация обеспечивает большую гибкость приложений.

На фиг. 16 функция "Связь с денежным модулем А" посылает сообщение "Сделать платеж" и R(1) своему денежному модулю А. Функция "Связь с денежным модулем В" также посылает сообщение "Принять платеж" и R(2) своему денежному модулю В (шаги 538-544).

На этой стадии денежный модуль А (в доверенном агенте 2 покупателя) и денежный модуль В (в доверенном агенте 4 продавца) устанавливают между собой сеанс связи таким образом, что каждый денежный модуль 6 завершает его, имея новый ключ сеанса связи (ДМ/ДМ) (шаг 546). При установлении такого сеанса связи денежного модуля с денежным модулем эти денежные модули обмениваются сообщениями посредством уже существующего сеанса связи между доверенными агентами. На фиг. 13 ключ сеанса связи для канала 442 шифрования формируется путем обмена сообщениями, зашифрованными при помощи канала 436. После установления между денежными модулями сеанса связи сообщения, передаваемые между денежными модулями, будут зашифрованы дважды обоими ключами сеанса связи (ДМ/ДМ) и (ДА/ДА) на протяжении части тракта связи между доверенными агентами 120.

В предпочтительном варианте выполнения сеанс связи между денежными модулями устанавливается аналогично установлению сеанса связи между доверенными агентами. Денежные модули 6, таким образом, будут иметь свои собственные сертификаты, содержащие их ключи общего пользования. Обмен сертификатами и случайными числами (для применения операции ИСКЛЮЧАЮЩЕЕ ИЛИ) инициализирует создание ключей сеанса связи (ДМ/ДМ). Протокол "Установление сеанса связи", используемый денежными модулями, по-

казан на фиг. 38 и описан ниже. Общая безопасность или защита системы в отношении денежных модулей может быть совмещена с безопасностью в отношении доверенных агентов 120, но предпочтительно отделена от нее в целях повышения безопасности и увеличения гибкости системы.

Согласно фиг. 16 денежный модуль А посылает R(1) денежному модулю В. Эта функция может инициализироваться приложением "Поддержание безопасности денежного модуля А", резидентно находящимся в денежном модуле А (шаг 548). Это и другие приложения денежного модуля имеют префикс "ДМ" и описаны в международной заявке WO 93/10503, включая любые модификации и/или дополнения.

Случайное число R(1) посылается от денежного модуля А денежному модулю В подпрограммой "Посылка маршрутизированного сообщения" (шаг 550). На фиг. 17 функция "Симметричный ключ денежного модуля А" шифрует сообщение (в том числе R(D) при помощи ключа сеанса связи (ДМ/ДМ) (шаг 640). Функция "Менеджер сеанса связи денежного модуля А" посылает сообщение функции "Менеджер сообщений центрального процессора А", который, в свою очередь, посылает сообщения функции "Интерфейс сообщений А" доверенного агента А (шаги 642-646). Доверенный агент А затем посылает сообщение функции "Интерфейс сообщений В" доверенного агента В при помощи подпрограммы "Посылка сообщения" (шаг 648), которая шифрует и расшифровывает сообщение при помощи ключа сеанса связи (ДА/ДА) между доверенными агентами. Функция "Интерфейс сообщений В" затем посылает сообщение функции "Менеджер сеанса связи денежного модуля В" в денежном модуле В через функцию "Менеджер сообщений центрального процессора В" (шаги 650-654). В завершение функция "Симметричный ключ денежного модуля В" расшифровывает сообщение при помощи ключа сеанса связи (ДМ/ДМ) (шаг 656).

Согласно фиг. 16 функция "Поддержание безопасности денежного модуля В" (в денежном модуле В) формирует ключ сеанса связи (ДА/ДМ) путем операции "ИСКЛЮЧАЮЩЕЕ ИЛИ над R(1) и R(2)". Затем денежный модуль В посылает R(2) денежному модулю А, который также формирует ключ сеанса связи (ДА/ДМ) путем операции "ИСКЛЮЧАЮЩЕЕ ИЛИ над R(1) и R(2)" (шаги 552-556). Как показано на фиг. 13, на этой стадии существуют три ключа сеанса связи: (ДМ/ДМ), (ДМ/ДА) и (ДА/ДА). Таким образом, в наличии имеется четыре показанных канала шифрования.

Как показано далее на фиг. 16, функция "Связь денежного модуля с абонентом А" приглашает доверенного агента А ввести сумму платежа в одной из валют (например, в долларах, йенах, фунтах и т.п.) (шаг 558). Денежный модуль, описанный в международной заявке WO 93/10503, будет обычно использовать приложение "Связь с абонентом" для связи с владельцем/держателем денежного модуля. Однако, как в рассматриваемом примере, приложение "Связь с абонентом" связывается с доверенным агентом 120 для получения различных команд. В данном случае доверенный агент 120 предоставляет информацию о размере платежа и типе банкнот (доверенный

агент А ранее связался с владельцем/держателем доверенного агента 2 покупателя для подтверждения цены выбранного товара).

Приглашение на ввод, поступающее от денежного модуля 6 доверенному агенту 120, посылается при помощи подпрограммы "Посылка сообщения от денежного модуля доверенному агенту" (шаг 560). Как показано на фиг. 18, функция "Симметричный ключ денежного модуля А" шифрует сообщение при помощи ключа сеанса связи (ДА/ДМ) (шаг 658). Функция "Менеджер сеанса связи денежного модуля А" посылает сообщение функции "Менеджер интерфейса доверенного агента А" через функцию "Менеджер сообщений центрального процессора А" (шаги 660-664). Функция "Симметричный ключ А" расшифровывает сообщение при помощи ключа сеанса связи (ДА/ДМ) (шаг 666). Согласно фиг. 16 функция "Покупка А" доверенного агента А посылает сумму (цену выбранного товара), выраженную типом банкнот, функции "Платеж/обмена денежным модулем А" (шаги 562-566). Это сообщение посылается при помощи подпрограммы "Посылка сообщения от доверенного агента денежному модулю" (шаг 564). Как показано на фиг. 19, функция "Симметричный ключ А" шифрует сообщение при помощи ключа сеанса связи (ДА/ДМ) (шаг 668). Функция "Интерфейс сообщений А" посылает сообщение функции "Менеджер сеанса связи денежного модуля А" через функцию "Менеджер сообщений центрального процессора А" (шаги 670-674). В завершение функция "Симметричный ключ денежного модуля А" расшифровывает сообщение при помощи ключа сеанса связи (ДА/ДМ) (шаг 676).

Как показано далее на фиг. 16, функция "Управление банкнотами денежного модуля А" проверяет, имеет ли денежный модуль 6 достаточно средств, чтобы произвести оплату (шаги 568-570). Если нет, то денежные модули А и В прекращают транзакцию (шаги 572-582).

Функция "Протокол прекращения транзакции денежным модулем" (шаг 582) для предпочтительного варианта выполнения электронной денежной системы описана ниже и показана на фиг. 42. Сообщения между денежным модулем А и денежным модулем В посылаются при помощи подпрограммы "Посылка маршрутизированного сообщения по электронной почте", которая использует все три ключа сеанса связи (ДМ/ДМ), (ДА/ДМ) и (ДА/ДА). Согласно фиг. 20 функция "Симметричный ключ денежного модуля А" шифрует сообщения при помощи ключа сеанса связи (ДМ/ДМ) (шаг 678). Это сообщение затем дважды зашифровывается ключом сеанса связи (ДМ/ДА), после чего оно посылается доверенному агенту А. По получении доверенным агентом А сообщение расшифровывается при помощи ключа сеанса связи (ДМ/ДА) (шаг 680). Функция "Интерфейс сообщений А" затем посылает сообщение функции "Интерфейс сообщений В" (шаги 682-684). На пути между доверенными агентами 120 сообщение дважды шифруется при помощи ключа сеанса связи (ДА/ДА). Подобным же образом функция "Интерфейс сообщений В" посылает сообщение функции "Симметричный ключ денежного модуля В" для окончательного расшифровывания (шаги

686-690). На фиг. 13 проиллюстрированы различные уровни шифрования.

Как показано на фиг. 16, во время операций прекращения работы денежных модулей А и В (шаг 582) они создают сообщения, посылаемые соответственно их доверенным агентам А и В (шаги 584-586), информируя этих доверенных агентов, что они прекратили транзакцию и что тем самым платеж был неудачным. Функции "Менеджеры сеанса связи А и В" отмечают, что платеж был неудачным, после чего доверенные агенты А и В прекращают транзакцию (шаги 588-598).

Если же, с другой стороны, денежный модуль 6 покупателя имеет достаточное количество средств, то функция "Платеж/обмен денежным модулем А" посылает денежному модулю продавца сообщение, содержащее сумму, которая должна быть передана во время платежа, и тип банкнот (шаг 600). Это сообщение посылается при помощи подпрограммы "Посылка маршрутизированного сообщения по электронной почте" (шаг 602).

Денежный модуль В принимает сообщение, содержащее сумму платежа в соответствии с определением денежного модуля А. Функция "Связь денежного модуля с абонентом В" затем посылает доверенному агенту напоминание проверить эту сумму платежа (шаги 604-606). Соответственно, функция "Покупка В" в доверенном агенте В проверяет, является ли сумма правильной (шаги 608-610). Если сумма правильная, то доверенный агент В посылает сообщение "Правильная сумма" денежному модулю В. Если же сумма неправильная, то посылается сообщение "Неправильная сумма" (шаги 612-616). В случае сообщения "Неправильная сумма" денежный модуль В информирует денежный модуль А, который, в свою очередь, передает запрос своему доверенному агенту на пересылку новой суммы или в противном случае прекращает транзакцию (шаги 618-622, 572-582). При платежах через денежный модуль, совершаемых во время покупки электронного товара, доверенный агент не посылает новую сумму, и, следовательно, оба денежных модуля 6 и оба доверенных агента 120 прекращают транзакцию.

Если же, с другой стороны, денежный модуль В принимает сообщение "Правильная сумма" от своего доверенного агента, то денежный модуль В посылает обратно денежному модулю покупателя подтверждающее сообщение (шаги 624-626). Когда функция "Платеж/обмен денежным модулем А" принимает подтверждающее сообщение, она передает сумму функции "Держатель денег А" (приложению, которое содержит и распределяется электронными эквивалентами денег) (шаг 628).

Следует отметить, что описанный выше инициализируемый платательщиком протокол иначе может быть реализован в виде инициализируемого ремитентом платежа, как в случае протокола "Платеж на месте продажи", показанного на фиг. 43 и описанного ниже. В таком протоколе доверенный агент продавца информирует свой денежный модуль о сумме платежа, которая ожидается к получению, и эта информация посылается денежному модулю покупателя, который запрашивает своего доверенного агента для проверки, и, если сум-

ма правильная, то доверенный агент покупателя информирует свой денежный модуль.

Согласно фиг. 16 денежный модуль покупателя А затем передает электронные банкноты в определенном количестве денежному модулю 4 продавца через тракт "Маршрутизированное сообщение по электронной почте" (шаг 630). На этой стадии транзакции А условно имеет правильный билет 8 (и зашифрованный электронный объект), а В условно имеет электронные банкноты на правильную сумму. На фиг. 39 представлен описываемый ниже протокол "Передача банкнот".

Далее вызывается подпрограмма "Фиксация транзакции денежным модулем" (шаг 632). На фиг. 41 показан протокол "Фиксация", используемый в предпочтительном варианте выполнения электронной денежной системы. Эта блок-схема используется и в том случае, когда денежные модули 6 взаимодействуют с доверенными агентами 120, с учетом того, что функция "Посылка сообщения" приравнена к функции "Посылка маршрутизированного сообщения по электронной почте" и что сообщения функции "Связь с абонентом" фактически посылаются в зашифрованном виде доверенному агенту 120. С учетом вышесказанного функция "Менеджер сеанса связи ДМ" денежного модуля В посылает сообщение "Готовность к фиксации" функции "Менеджер сеанса связи ДМ" денежного модуля А при помощи подпрограммы "Посылка маршрутизированного сообщения по электронной почте" (шаги 1702-1704). Функция "Менеджер сеанса связи денежного модуля А" затем посылает подтверждающее сообщение денежному модулю В, и денежный модуль А фиксирует транзакцию (шаги 1706-1716). Когда денежный модуль В принимает подтверждающее сообщение, он также фиксирует транзакцию (шаги 1718-1724).

Во время операций по фиксации, выполняемых денежными модулями А и В, последние выработывают сообщения, посылаемые соответственно их доверенным агентам А и В (шаги 1714, 1722), информируя последних о том, что они зафиксировали транзакцию и что, следовательно, платеж был успешным.

Как показано на фиг. 16, оба денежных модуля затем посылают вышеуказанные сообщения "Платеж успешен" своим доверенным агентам (шаги 584-586). Эти сообщения шифруются ключом сеанса связи (ДА/ДМ). Функция "Менеджер сеанса связи А" фиксирует, что был совершен успешный платеж, а функция "Держатель билетов А" обновляет билет, снабжая его информацией о платеже, например, датой покупки (шаги 588, 592, 634). Доверенный агент А затем фиксирует транзакцию (шаг 636), так что наличие у него билета не является более "условным". Аналогичным образом функция "Менеджер сеанса связи В" фиксирует успешный платеж (шаги 590, 594), а доверенный агент В фиксирует транзакцию (шаг 638). После этого транзакция завершена.

Таким образом, безопасная или защищенная транзакция купли-продажи в соответствии с предпочтительным вариантом выполнения настоящего изобретения происходит следующим образом:

1. между денежными модулями покупателя и продавца, между доверенными агентами покупа-

теля и продавца и между денежным модулем и доверенным агентом каждого устройства транзакций устанавливается безопасный транзакционный сеанс связи;

2) выбранный электронный товар передается от доверенного агента продавца доверенному агенту покупателя (где он условно остается); в случае, если электронный товар содержит электронный объект, то электронный объект шифруется таким образом, что он может храниться вне доверенного агента;

3) после проверки правильности передаваемого электронного товара доверенный агент покупателя дает команду своему денежному модулю выплатить определенную сумму электронных денег денежному модулю продавца;

4) денежный модуль покупателя информирует денежный модуль продавца о сумме электронных денег, которая будет выплачена, а денежный модуль продавца проверяет с помощью своего доверенного агента, является ли эта сумма правильной ценой товара;

5) если сумма правильная, то денежный модуль продавца посылает подтверждение о приеме денежному модулю покупателя;

6) денежный модуль покупателя передает электронные деньги денежному модулю продавца (денежный модуль продавца условно имеет банкноты, а денежный модуль покупателя условно уменьшает количество банкнот на переданное количество);

7) денежные модули покупателя и продавца фиксируют транзакцию (наличие банкнот у денежного модуля продавца более не является условным, а в денежном модуле покупателя остается новое количество банкнот), и в то же время они посылают сообщения об успешном платеже соответственно своим доверенным агентам;

8) в заключение доверенные агенты покупателя и продавца фиксируют транзакцию (доверенный агент продавца записывает продажу, а наличие товара у доверенного агента покупателя более не является условным), так что покупатель может после этого использовать свою электронную покупку, а продавец получает свои электронные деньги.

Следует отметить, что в альтернативном варианте выполнения порядок обмена электронного товара и денег может быть обратным. В этом случае электронные деньги могут передаваться (условно) первыми, а затем (условно) передается электронный товар. Доверенный агент покупателя в этом случае дает команду своему денежному модулю на фиксацию транзакции, и транзакция будет происходить аналогично описанной выше схеме. Для такого альтернативного варианта выполнения потребуется соответствующая модификация протоколов платежей через денежный модуль.

Выше было описано, каким образом обезопасить одновременно оплату и доставку электронной покупки в сети связи, где продавец не знает покупателя. Этот случай является прямой аналогией покупки товаров в магазине за наличные деньги. Продавец в магазине не знает лично покупателя, но продаст ему товар за наличные. Покупатель уверен, что он получит покупку, так как

он находится в физической близости к продавцу за прилавком. При помощи вышеописанного протокола был создан электронный "прилавок", у которого доверенный агент 2 покупателя и доверенный агент 4 продавца могут совершать сделку так же надежно, как и в физическом аналоге.

В дополнение к анонимным платежам денежными модулями доверенный агент 120 обеспечивает также надежную базу для ведения транзакций, основанных на проверке полномочий, т.е. транзакций, требующих раскрытия личности покупателя. Примерами таких транзакций являются платежи по кредитным или дебетовым картам, открытие чекового счета, покупка товара, например автомобиля, при которой требуется регистрация покупателя, или оплата счета или накладной. На сегодняшний день удаленное получение продавцом номера кредитной или дебетовой карты для оплаты и доставки товара по адресу, отличному от адреса покупателя, связаны с определенным риском. Если такая сделка является мошенничеством, то ответственность несет продавец. Однако продавец может взять номер карты в виде части удостоверения доверенного агента, которое будет являться для эмитента карты достаточной гарантией, чтобы исключить возможность мошенничества.

Как показано на фиг. 12, если вместо анонимного платежа денежным модулем покупатель решает платить при помощи удостоверения в виде кредитной или дебетовой карты, то вызывается подпрограмма "Платеж/возврат на основе проверки полномочий" (шаг 432). Согласно фиг. 21 функция "Держатель билетов А" затребует удостоверение в виде кредитной или дебетовой карты (шаг 692). Функция "Покупка А" посылает сообщение, указывающее на то, что платеж является платежом по удостоверению, и содержащее удостоверение для подтверждения его действительности функцией "Покупка В" (шаги 694-700). Если удостоверение недействительно, то транзакция прекращается (шаг 702). Если же удостоверение действительно, то функция "Покупка В" проверяет, запрашивает ли покупатель возврат (шаги 704-706). Если предположить, что в данном случае транзакция не является транзакцией возврата, то функция "Связь с центральным процессором В" посылает цену и удостоверение в сеть проверки полномочий карт для проверки полномочий платежа (шаг 708). Устройство транзакций продавца инициализирует процесс проверки полномочий карты (шаг 710). Проверка полномочий карты хорошо известна из уровня техники и для нее обычно требуется эмитент карты или его агент, уполномоченный на осуществление отдельного платежа в случае, когда на карте имеются достаточная сумма или сумма в пределах лимита кредитования держателя карты. По завершении процесса проверки полномочий карты функция "Покупка В" проверяет, был ли санкционирован платеж (шаги 712-714).

Если платеж не санкционирован, то транзакция прекращается (шаг 702). Если же платеж санкционирован, то функция "Покупка В" посылает сообщение "Платеж санкционирован" функции "Держатель билетов А", а доверенный агент В фиксирует транзакцию (шаги 716-720). Когда



функция "Держатель билетов А" принимает сообщение "Платеж санкционирован", он обновляет билет с помощью информации о платеже (например, даты покупки) (шаг 722). Затем доверенный агент А фиксирует транзакцию (шаг 724), завершая платеж на основе проверки полномочий.

Как показано на фиг. 12, после платежа вызывается подпрограмма "Открытие покупки" (шаг 434). Согласно фиг. 22 функция "Покупка А" проверяет, является ли покупка электронным объектом (шаги 736-738). Если это так, то функция "Держатель билетов А" посылает ключ расшифровки и идентификатор электронного объекта из билета расшифровки в приложение транзакций центрального процессора для использования при расшифровывании электронного объекта (шаги 740-742). Если же, однако, покупка является билетом на услуги связи с ключом расшифровки, то функция "Держатель билетов А" посылает ключ расшифровки приложению транзакций центрального процессора (шаг 746). Приложение транзакций центрального процессора использует этот ключ для декодирования связи (шаг 748). Если покупка не является ни электронным объектом, ни билетом на услуги связи с ключом расшифровки, то процедура просто заканчивается. Для получения услуг должны предъявляться другие типы билетов 8.

Предъявление билета.

Как показано на фиг. 23, когда покупатель-владелец доверенного агента А намерен использовать билет для получения услуг от продавца через его доверенный агент В, то приложение транзакций центрального процессора А (ПТЦПА) связывается с приложением транзакций центрального процессора В (ПТЦПВ) (шаги 750-752). ПТЦПА посылает сообщение "Предъявить билет" своему доверенному агенту, а ПТЦПВ посылает своему доверенному агенту сообщение "Принять билет" (шаги 754-756).

Доверенные агенты устанавливают сеанс связи (шаг 758), а А проверяет удостоверение продавца В (шаг 760). Функция "Держатель билетов А" запрашивает идентификатор билета у центрального процессора и предъявляет список билетов, которые он имеет (шаг 762). Функция "Связь с центральным процессором А" посылает это сообщение ПТЦПА, чтобы покупатель мог выбрать, какой билет предъявить (шаг 764). После выбора покупателем соответствующего билета ПТЦПА посылает идентификатор билета доверенному агенту А (шаги 766-768). Функция "Держатель билетов А" затребует выбранный билет и проверяет, является ли он действующим или "активным" (шаги 770-772). Билет 8 "активен", если он еще имеет ценность. Например, в случае билета на мероприятие поле 100 "Статус" показывает, был ли билет 8 уже использован и, следовательно, не представляет никакой ценности. В случае билета на услуги связи оставшаяся ценность билета 8 показывает поле 116 "Доступное время". Если билет 8 недействующий или "неактивен", то функция "Связь с центральным процессором А" посылает сообщение ПТЦПА, что билет неактивен, и транзакция прекращается (шаги 774-776).

Если билет 8 является действующим, то функция "Предъявление билета А" посылает ко-

пию билета к В (шаги 778-780). Функция "Получение билета В" принимает билет и проверяет как его действительность, так и его активность (шаги 782-784). Если билет недействителен или неактивен, транзакция прекращается (шаг 786). Если же билет действителен и активен, то функция "Связь с центральным процессором В" дает указание ПТЦПВ предоставить услуги ПТЦПА (шаг 788). Оставшаяся ценность билета А также передается обратно, т.к. билет может представлять собой билет, ценность которого уменьшается постепенно по мере получения услуг (например, как в случае с оплатой телефонной картой), функция "Получение билета В" затем посылает сообщение к А, что билет 8 используется (шаги 790-792). Функция "Держатель билетов А" маркирует билет 8 как используемый (шаг 794).

Взаимодействие ПТЦПА с ПТЦПВ осуществляется соответствующим образом в зависимости от типа билета и предоставляемых услуг (шаг 796). ПТЦПВ постоянно отслеживает оставшуюся ценность билета, пока эта ценность не уменьшится до нуля (шаги 798-800). В этот момент ПТЦПВ сообщает ПТЦПА о недостаточной ценности и посылает В сообщение, что билет обесценился (шаг 802). Затем вызывается подпрограмма "Фиксация билетной транзакции" (шаг 804).

На фиг. 24 функция "Получение билетов В" посылает новую остаточную ценность билета, в данном случае нуль, функции "Предъявление билетов А" (шаги 822-826). Функция "Держатель билетов А" затем маркирует билет 8 как неиспользуемый и обновляет ценность билета (шаг 828). В завершение доверенный агент А фиксирует транзакцию, функция "Менеджер сеанса связи А" информирует В, что билет 8 обновлен, и доверенный агент В фиксирует транзакцию (шаги 830-834). Согласно фиг. 23 ПТЦПА после этого посылает запрос, намеревается ли покупатель продолжить транзакцию (шаги 806-808). Если да, то доверенный агент А пытается увеличить (путем покупки) ценность билета (шаг 810).

Во время взаимодействия ПТЦПА и ПТЦПВ (шаг 796) ПТЦПА проверяет, завершил ли владелец ПТЦПА транзакцию (шаги 812-814). Если транзакция завершена, то ПТЦПА информирует об этом ПТЦПВ, который, в свою очередь, информирует своего доверенного агента (шаги 816-818). ПТЦПВ посылает также остаточную ценность билета своему доверенному агенту. В заключение вызывается подпрограмма "Фиксация билетной транзакции" (шаг 820).

Передача билетов.

Билеты 8 могут передаваться между доверенными агентами 120 (кроме начальной выдачи билета). Существует несколько причин, по которым владельцу может потребоваться осуществить передачу. Например, если билет 8 был куплен через настольное устройство 122 транзакций (например, доверенный агент 188 покупателя, встроженный в персональный компьютер), то владельцу может потребоваться переместить билет в переносное устройство (например, в электронный бумажник). Или же, если владелец купил билет 8 для третьего лица (например, друга или родственника), он может передать ему билет, чтобы тот мог его использовать. Еще одной возможной си-

туацией является таковая, когда владелец покупает новое устройство 122 транзакций и ему требуется переместить свои удостоверения в это новое устройство.

На фиг. 25 показана процедура, выполняемая в том случае, когда владельцу доверенного агента А требуется передать один или более билетов 8 доверенному агенту В (шаг 836). Сначала ПТЦПА соединяется с ПТЦПВ (шаг 838). Затем ПТЦПА дает команду своему доверенному агенту "Передать билет (ы)", а ПТЦПВ дает команду своему доверенному агенту "Принять билет(ы)" (шаги 840-842). Затем доверенные агенты устанавливают безопасный сеанс связи (шаг 844). После этого функция "Связь с центральным процессором А" посылает через ПТЦПА владельцу устройства транзакций запрос, проверять ли идентификационное удостоверение принимающей билет (ы) стороны (шаги 846-848). Если проверка удостоверения не требуется либо завершается успешно (шаги 850 - 854), то функция "Держатель билетов А" запрашивает идентификаторы билетов, которые передаются (шаг 856). Билеты выбираются из списка билетов, которые имеются у доверенного агента А. Функция "Связь с центральным процессором А" посылает ПТЦПА сообщение, содержащее список билетов, которые выбрал владелец, а также принимает ответную идентификацию выбранного(ых) билета(ов) (шаги 858-862).

Функция "Держатель билетов А" затребует выбранный билет (выбранные билеты) (шаг 864). Затем функция "Ключ общего пользования А" подписывается на билетах для В путем добавления соответствующей информации о передаче к разделу "Предыстория передачи" и внесения цифровой подписи в раздел "Подписи отправителя" (шаг 866). После этого функция "Держатель билетов А" посылает билет(ы) функции "Получатель билетов В" для подтверждения действительности с помощью функции "Ключ общего пользования В" (шаги 868-876). Если билет(ы) недействителен (недействительны), то транзакция прекращается (шаг 878). Если билет(ы) действителен (действительны), то функция "Держатель билетов В" сохраняет билет(ы) и посылает А подтверждение о приеме (шаги 880-882). Функция "Держатель билетов А" принимает подтверждение о приеме и уничтожает билет(ы) (шаг 884). Доверенный агент А информирует функцию "Держатель билетов В", что билеты уничтожены (шаги 884-886) и фиксирует транзакцию (шаг 888). Функция "Держатель билетов В" принимает сообщение (шаг 890), после чего доверенный агент В фиксирует транзакцию (шаг 892).

#### Удостоверения.

Покупатель может приобретать удостоверения лично у идентифицирующего уполномоченного лица. Удостоверение может быть водительскими правами, выданными управлением автотранспорта, паспортом, выданным Государственным Департаментом или Министерством иностранных дел, кредитной или дебетовой картой, выданной банком, или корпоративной печатью (идентификатором), выданной коммерческим бюро. Удостоверения могут быть дистанционно продлены или даже дистанционно приобретены, если, в первую очередь, доверенный агент 120 уже имеет удостове-

рения для подтверждения своей подлинности. При помощи удостоверений было бы возможно открывать чековый счет дистанционно, даже если покупатель неизвестен банку.

На фиг. 26 представлена процедура, выполняемая в том случае, когда владелец доверенного агента А решает лично приобрести удостоверение у идентифицирующего уполномоченного лица (шаг 894). Прежде всего владелец А предъявляет представителю идентифицирующего уполномоченного лица удостоверение своей личности. Затем представитель вводит различную информацию (например, имя, адрес и т.д.) через ПТЦПВ доверенного агента В уполномоченного лица (шаги 896-898). Далее владелец А дает команду своему ПТЦПА приобрести удостоверение. В ответ ПТЦПА посылает доверенному агенту А сообщение "Приобрести удостоверение" (шаги 900-902). В то же время ПТЦПВ посылает доверенному агенту В сообщение "Создать удостоверение" (шаг 904). После этого доверенный агент В устанавливает сеанс связи с доверенным агентом А (шаг 906). Функция "Связь с центральным процессором В" сообщает В, что сеанс связи установлен. ПТЦПВ посылает доверенному агенту В различную информацию об удостоверении (шаги 908-910). Затем функция "Создание удостоверения" создает информацию об удостоверении (т.е. разделы 10, 12 "Идентификатор" и "Компоненты" удостоверяющего билета) (шаг 912).

На следующем этапе вызывается подпрограмма "Доставка удостоверения" для передачи вновь созданного удостоверения доверенному агенту А (шаг 914). Как показано на фиг. 27, функция "Ключ общего пользования В" подписывает информацию об удостоверении (при помощи ключа общего пользования доверенного агента уполномоченного лица) и посылает ее функции "Создание удостоверения В" (шаг 916). Функция "Создание удостоверения В" создает удостоверение, содержащее информацию об удостоверении, подпись и сертификат доверенного агента уполномоченного лица (серт.(ДА)) (шаг 918). Затем функция "Создание удостоверения В" посылает заново созданное удостоверение доверенному агенту А (шаг 920). При необходимости функция "Создание удостоверения" также посылает А цену удостоверения.

Функция "Ключ общего пользования А" проверяет удостоверение (шаги 922-924). Если удостоверение недействительно, то транзакция прекращается (шаг 926). Если же удостоверение действительно, то функция "Связь с центральным процессором А" посылает информацию об удостоверении и сумму оплаты (при необходимости) ПТЦПА для подтверждения (шаги 928-930). Если владелец доверенного агента А не дает подтверждения, то транзакция прекращается (шаг 926).

Если удостоверение подтверждено, то функция "Держатель билетов А" принимает удостоверение и проверяет, требуется ли оплата (шаги 932-934). Если оплата не требуется, то доверенный агент А фиксирует транзакцию (шаг 936) и посылает доверенному агенту В сообщение, что удостоверение было принято (шаги 938-940). После получения этого сообщения доверенный агент В фиксирует транзакцию (шаг 942). Функция "Соз-

дание удостоверения В" затем сообщает ПТЦПВ, что удостоверение принято, а ПТЦПВ посылает информацию об удостоверении в базу данных по удостоверениям, хранимую в сервере уполномоченного лица (шаги 944-946).

Если же, с другой стороны, требуется оплата удостоверения, то функция "Связь с центральным процессором А" посылает запрос владельцу доверенного агента А на выбор способа оплаты (шаги 948-950). Если выбран платеж денежным модулем, то вызывается подпрограмма "Платеж через денежный модуль" (шаг 952). В той точке, где В выходит из подпрограммы, функция "Создание удостоверения В" сообщает ПТЦПВ, что удостоверение принято, а ПТЦПВ посылает информацию об удостоверении серверу уполномоченного лица (шаги 944-946). Если же владелец доверенного агента А решает платить при помощи кредитной или дебетовой карты, то вызывается подпрограмма "Платеж/возврат на основе проверки полномочий" (шаг 954).

Для идентифицирующих уполномоченных может быть необходимо обновлять свою информацию об удостоверении с некоторой периодичностью. Таким образом, требуется продление путем задания сроков окончания действия удостоверений. На фиг. 28 показано, каким образом владелец доверенного агента А может дистанционно продлить свое удостоверение (шаг 956). Сначала ПТЦПА связывается с ПТЦПВ (шаг 958). ПТЦПА посылает доверенному агенту А сообщение "Продлить удостоверение" (шаг 960). ПТЦПВ посылает доверенному агенту В сообщение "Принять удостоверение для продления" (шаг 962). Затем доверенный агент А устанавливает безопасный сеанс связи с доверенным агентом В (шаг 964).

Доверенный агент А сначала проверяет удостоверение уполномоченного лица (шаг 966). Удостоверения уполномоченных лиц могут выпускаться под контролем доверенного агентства. Функция "Приобретение удостоверения А" запрашивает удостоверение, которое необходимо продлить, у функции "Держатель билетов А", который посылает удостоверение доверенному агенту В уполномоченного лица (шаги 968-972). Функция "Создание удостоверения В" проверяет, действительно ли удостоверение, (шаги 974-976). Если удостоверение недействительно, то транзакция прекращается (шаг 978). Если же удостоверение действительно, то функция "Создание удостоверения В" проверяет, должно ли удостоверение продлеваться лично (шаги 980-982). Если удостоверение может быть продлено дистанционно, то функция "Создание удостоверения В" обновляет информацию удостоверения, в том числе задает новый срок окончания его действия (шаг 984). Затем вызывается подпрограмма "Доставка удостоверения" (шаг 986).

Если удостоверение должно продлеваться лично, то функция "Создание удостоверения В" посылает доверенному агенту А сообщение "Продлить лично" (шаги 988-990). Функция "Приобретение удостоверения А" принимает это сообщение (шаг 992). Затем доверенный агент А фиксирует транзакцию (шаг 994), а функция "Менеджер сеанса связи А" посылает подтверждение о прие-

ме доверенному агенту В (шаги 996-998). После этого доверенный агент В фиксирует транзакцию (шаг 1000).

Оплата через денежный модуль на основе идентификации.

Покупка электронного товара без платежей электронными наличными может быть осуществлена согласно блок-схеме алгоритма, представленного на фиг. 29. Ниже рассмотрен случай, когда владелец доверенного агента А решает произвести платеж через денежный модуль владельцу доверенного агента В, причем владелец А хочет проверить личность В, поскольку транзакция дистанционная (шаг 1002). ПТЦПА связывается с ПТЦПВ (шаг 1004). ПТЦПА посылает своему доверенному агенту сообщение "Платить" (шаг 1006). ПТЦПВ посылает своему доверенному агенту сообщение "Принять платеж" (шаг 1008). Затем А устанавливает безопасный сеанс связи с В (шаг 1010).

Доверенный агент А проверяет удостоверение В (шаг 1012). Это удостоверение может быть водительскими правами, кредитной картой или другим соответствующим удостоверением. Если удостоверение действительно и приемлемо для А, то функция "Покупка А" посылает доверенному агенту В сообщение "Требуется ли В удостоверение А" (шаги 1014-1016). Функция "Связь с центральным процессором В" затем посылает ПТЦПВ сообщение "Требуется удостоверение А?" для проверки, требуется ли В удостоверение А (шаги 1018-1020). Если да, то В проверяет удостоверение А (шаг 1022). В этом случае также могут использоваться различные типы удостоверений. Если В не требуется удостоверение А, то функция "Покупка В" соответственно информирует доверенного агента А (шаги 1024-1026).

Затем функция "Покупка А" посылает доверенному агенту В извещение о переводе, определяющее сумму, которая должна быть уплачена (в случае оплаты счета), либо сразу посылает сумму к оплате (шаги 1028-1030). Функция "Связь с центральным процессором В" посылает эту информацию ПТЦПВ для подтверждения (шаги 1032-1034). Если подтверждения не происходит, то транзакция прекращается (шаг 1036). Если подтверждение имеет место, то функция "Покупка В" соответственно информирует А (шаги 1038-1040). Затем инициализируется платеж через денежный модуль (шаг 1042).

Споры.

В случае, когда покупатель неудовлетворен покупкой, доверенные агенты 120 могут выступать в качестве заместителей покупателя и продавца для дистанционного разрешения спора. Например, если электронный объект кажется дефектным, то покупатель может связаться с продавцом и войти в диалог разрешения спора. Продавец не может не признать товар, если он был подтвержден его доверенным агентом 4 (т.к. это будет записано в журнал транзакций доверенного агента 2 покупателя).

Если покупатель неудовлетворен результатом спора с продавцом, он может направить свою жалобу в доверенное агентство. Журнал транзакций покупателя показывает, что от спора первым отказался продавец. Спор и сопутствующая до-

кументация могут быть представлены доверенному серверу 200 в сети 208 доверенного агентства. Дальнейшее взаимодействие аналогично взаимодействию с доверенным агентом 4 продавца. Для большинства продавцов будет желательно разрешить спор непосредственно с покупателем, не допуская обращения покупателя к процедуре разрешения с помощью доверенного агентства. Слишком большое количество споров может поставить под сомнение статус продавца в доверенном агентстве.

В процессе разрешения спора покупатель должен воспроизвести электронный товар и доказать, что этот товар является товаром, купленным у продавца. Процесс разрешения спора также защищает продавца от мошеннических требований. Продавец может доверять доверенному агенту 2 покупателя путем проверки, что доверенный агент 2 покупателя получил покупку. Затем жалоба покупателя может быть разрешена путем исследования товара на наличие дефектов.

На фиг. 30 показана процедура, которая выполняется в том случае, когда владелец доверенного агента А решает вернуть электронную покупку владельцу доверенного агента В продавца (шаг 1044). Сначала ПТЦПА связывается с ПТЦПВ. ПТЦПА посылает своему доверенному агенту сообщение "Послать спор". ПТЦПВ посылает своему доверенному агенту сообщение "Принять спор". Доверенный агент А затем устанавливает безопасный сеанс связи с доверенным агентом В (шаги 1046-1052).

Доверенный агент А проверяет удостоверение продавца В (шаг 1054). Функция "Журнал транзакций А" посылает свой журнал ПТЦПА через функцию "Связь с центральным процессором А", чтобы владелец мог выбрать, какую транзакцию оспорить и описать проблему (шаги 1056-1060). Функция "Связь с центральным процессором А" принимает информацию о предмете спора от ПТЦПА (шаг 1062). Функция "Держатель билетов А" затем посылает выбранный билет функции "Инициализация спора А" (шаг 1064).

Функция "Инициализация спора А" проверяет, затрагивает ли спор электронный объект (шаги 1066-1068). Если спор не затрагивает электронный объект (затрагивается только билет), то функция "Инициализация спора А" посылает копию билета вместе с информацией о предмете спора доверенному агенту В (шаги 1070-1072). Функция "Разрешение спора В" принимает сообщение, а функция "Покупка В" проверяет билет (шаги 1074-1078). Если билет недействителен, то функция "Разрешение спора В" посылает функции "Инициализация спора А" сообщение "Билет недействителен" (шаги 1080-1084). После этого вызывается подпрограмма "Совершение спора" (шаг 1086).

Как показано на фиг. 31, доверенный агент А фиксирует транзакцию (шаг 1156). Функция "Менеджер сеанса связи А" посылает подтверждение о приеме функции "Менеджер сеанса связи В" (шаги 1158-1162). Затем доверенный агент В фиксирует транзакцию (шаг 1164).

Согласно фиг. 30, если билет действителен (шаг 1078), то функция "Разрешение спора В" посылает билет и информацию о предмете спора ПТЦПВ. Продавец затем изучает предмет спора и

решает, отклонить или нет претензии покупателя (шаги 1088-1092). Если спор отклонен, то функция "Разрешение спора В" посылает сообщение "Спор отклонен" доверенному агенту А, который инициализирует подпрограмму "Фиксация транзакции спора" (шаги 1094, 1082-1086).

Если продавец не отклоняет спор, то ПТЦПВ посылает ПТЦПА сообщение, запрашивающее резолюцию покупателя (шаг 1096). Затем покупатель выбирает, хочет ли он вернуть деньги или получить новый товар (предполагается, что продавец предоставляет такой выбор) (шаги 1098-1100).

Если покупатель требует денежного возмещения, то вызывается подпрограмма "Выплата по спору" (шаг 1102). Как показано на фиг. 32, функция "Инициализация спора А" посылает доверенному агенту В сообщение "Запросить возврат денег" (шаги 1166-1170). Функция "Разрешение спора В" принимает это сообщение и проверяет способ платежа А (шаг 1172). Если необходим платеж через денежный модуль, то вызывается подпрограмма "Платеж через денежный модуль" (шаг 1174).

Если же необходимо возмещение по кредитной или дебетовой карте, то функция "Покупка В" посылает А сообщение, содержащее размер возмещения (шаги 1176-1178). Затем вызывается подпрограмма "Платеж/возврат на основе проверки полномочий" (шаг 1180). На фиг. 21 изображена блок-схема процесса, выполняемого в случае возврата. Если выполняется транзакция возврата (шаги 704-706), то функция "Связь с центральным процессором В" посылает ПТЦПА сообщение, содержащее удостоверение в виде кредитной или дебетовой карты и сумму к возврату (шаг 726). После этого выполняется процесс проверки полномочий карты (шаг 728). Затем функция "Покупка В" проверяет, был ли санкционирован возврат (шаги 730-732). Если возврат не санкционирован, то транзакция прекращается (шаг 702). Если же возврат санкционирован, то функция "Покупка В" посылает доверенному агенту А сообщение "Возврат санкционирован" (шаги 734, 718). Затем доверенный агент В фиксирует транзакцию (шаг 720). После получения сообщения от В функция "Держатель билетов А" обновляет билет при помощи информации о возврате (шаг 722). После этого доверенный агент А фиксирует транзакцию (шаг 724).

Как показано на фиг. 30, если вместо возврата денег владелец доверенного агента А выбирает получение нового товара, то функция "Покупка В" запрашивает товар у сервера товаров (шаг 1104). Сервер товаров затребует товар и посылает его доверенному агенту В. Функция "Покупка В" принимает товар и проверяет его идентификатор (шаги 1106-1110). Если товар соответствует выбранному, то вызываются подпрограммы "Доставка покупки", "Открытие покупки" и "Совершение спора" (шаги 1120-1124). Если товар не соответствует выбранному или же товар невозможно получить от сервера товаров, то функция "Разрешение спора В" посылает доверенному агенту А сообщение "Товар недоступен" (шаги 1114-1116). В этом случае инициализируется возврат денег (шаг 1118).

Если спор о товаре затрагивает электронный объект (шаги 1066-1068), то функция "Инициализация спора А" затребуется идентификатор электронного объекта у связанного с ним билета расшифровки. Затем функция "Связь с центральным процессором А" дает команду ПТЦПА послать электронный объект доверенному агенту А (шаги 1126-1130). После этого функция "Инициализация спора А" посылает копию билета и электронный объект вместе с информацией о предмете спора В (шаги 1132-1134). Функция "Разрешение спора В" принимает это сообщение (шаг 1136). Затем функция "Покупка В" проверяет билет (шаги 1138-1140). Если билет недействителен, то доверенный агент А информируется об этом, а спор завершается (шаги 1080-1086). Если билет действителен, то функция "Покупка В" проверяет электронный объект (шаги 1142-1144). Если объект недействителен, то функция "Разрешение спора В" информирует об этом доверенного агента А (шаг 1146), а спор завершается (шаги 1082-1086). Если электронный объект действителен, то функция "Симметричный ключ В" расшифровывает, соответственно декодирует электронный объект и посылает его ПТЦПВ для тестирования. Информация о предмете спора также посылается ПТЦПВ (шаги 1148-1152).

ПТЦПВ, основываясь на жалобе покупателя, определяет, содержит ли электронный объект дефекты. Если продавец определяет, что товар не содержит дефектов, то функция "Разрешение спора В" информирует об этом доверенного агента А (шаг 1154), и спор завершается (шаги 1082-1086). Если же, однако, продавец определяет, что товар содержит дефекты, то покупатель может выбрать либо денежное возмещение, либо новый товар (шаги 1096-1098).

Электронная денежная система.

Электронная денежная система, которая может использоваться с описанной системой для открытого электронного бизнеса, описана в международной заявке WO 93/10503. Ниже приведено описание различных усовершенствований и приложений к электронной денежной системе по настоящему изобретению.

Общий обзор.

Термин "денежный модуль", используемый в заявке WO 93/10503, обычно относится к денежным модулям транзакций, денежным модулям банковских кассиров и модулям генератора денег. Описанные выше денежные модули 6, взаимодействующие с доверенными агентами 120, обычно соответствуют в предпочтительном варианте выполнения денежным модулям транзакций. При дальнейшем описании электронной денежной системы термин "денежные модули" также используется в общем смысле по отношению к денежным модулям транзакций, денежным модулям банковских кассиров и модулям генератора денег.

Эффективная безопасность для денежной системы характеризуется тремя функциями:

воспрепятствование мошенничеству, отслеживание мошенничества и подавление мошенничества. Описываемая электронная денежная система сконструирована таким образом, что она содержит компоненты, которые выполняют все три функции.

Для воспрепятствования мошенничеству денежные модули взаимодействуют друг с другом при помощи шифров с симметричным и асимметричным ключами. Ни одно сообщение не передается в явном виде. Протоколы модуля также физически защищены при помощи аппаратуры, не допускающей несанкционированного доступа.

Мошенничество выявляется при помощи процессов согласования банкнот. Общесистемные временные протоколы (например, срок окончания действия банкноты) вызывают регулярную проверку соответствия банкнот. Электронные банкноты также обновляются (т.е. заменяются новыми банкнотами с новым сроком действия) при выполнении банковских транзакций.

Денежные модули блокируются (например, помещаются в список неверных идентификаторов), если с ними связаны дублированные или поддельные банкноты. Кроме того, банкноты, прошедшие через эти модули, не будут разрешены к передаче. Передача дублированных или поддельных банкнот будет подавлена, т.к. у банкнот истекает срок действия или они будут в итоге отложены в банке. Более того, в случае возникновения серьезных проблем с безопасностью или защитой системы электронная денежная система может вызвать глобальную пересертификацию, требующую пересертификации всех модулей, в том числе денежных модулей транзакций, как только они в следующий раз подключатся к сети электронной денежной системы.

Иерархия безопасности.

Как показано на фиг. 33А, электронная денежная система имеет два типа серверов безопасности: основной 1182 и обыкновенный 1184. Основные серверы 1182 безопасности сертифицируют (обыкновенные) серверы 1184 безопасности. Серверы 1184 безопасности сертифицируют все остальные модули в системе (денежные модули 1186 транзакций, денежные модули 1188 банковских кассиров, модуль 1190 генератора денег и модуль 1192 обслуживания клиентов).

Основные серверы 1182 взаимодействуют только с другими основными серверами 1182 или серверами 1184 безопасности. Как показано на фиг. 34, основные серверы 1182 безопасности помещены в защищенные от несанкционированного доступа условия и соединены друг с другом при помощи локальной вычислительной сети (ЛВС) 1194 безопасности. ЛВС 1194 связана через безопасный шлюз с сетью безопасности 1196. По этой сети связываются только серверы безопасности. Все серверы безопасности являются физически защищенными устройствами.

Серверы 1184 безопасности также связаны с сетью 1198 электронной денежной системы (ЭДС) и локальными банковскими сетями 1200. Предполагается, что серверы безопасности могут подвергаться определенному риску, и они проверяются после каждого взаимодействия с другим модулем.

Сертификаты имеют только серверы 1184 безопасности и модули. Эти устройства содержат ключи общего пользования основного сервера безопасности. Существует два типа сертификатов: сертификат сервера безопасности и сертификат модуля.

Структура и проверка достоверности сертификата

Сертификат имеет следующую структуру:

$$\begin{array}{l} \text{Серт. (СБ)} = \frac{E_{\text{ОСБ}}[(\text{ид}) \text{СБ} \| \text{КОП} \text{СБ} \| \text{срок действия} \| \sigma_{\text{ОСБ}}(X)] \| (\text{ид}) \text{ОСБ}}{\text{ИСКЛЮЧАЮЩЕЕ ИЛИ С}} \\ \text{Серт. (М)} = \frac{E_{\text{СБ}}[(\text{ид}) \text{М} \| \text{КОП} \text{М} \| \text{срок действия} \| \sigma_{\text{СБ}}(Y)] \| \text{серт. (СБ)}}{Y} \end{array}$$

Протоколами подтверждения сертификата являются следующие:

- 1) Проверка достоверности серт.(СБ)
  - а)  $(\text{ид}) \text{ОСБ} = [(\text{ид}) \text{ОСБ} \text{ ИСКЛЮЧАЮЩЕЕ ИЛИ С} \text{ ИСКЛЮЧАЮЩЕЕ ИЛИ С,}$
  - б)  $D_{\text{ОСБ}}(E_{\text{ОСБ}}(X) \| \sigma_{\text{ОСБ}}(X))) = X \| \sigma_{\text{ОСБ}}(X),$
  - в) проверить, аутентичен ли  $(\text{ид}) \text{СБ}$  (см. схему нумерации модулей),
  - г) проверить, действительна ли дата,
  - д) проверить, выполняется ли  $D_{\text{ОСБ}}(\sigma_{\text{ОСБ}}(X)) = h(X).$
- 2) Проверка достоверности серт.(М)
  - а) проверить достоверность серт.(СБ),
  - б)  $D_{\text{СБ}}(E_{\text{СБ}}(Y) \| \sigma_{\text{СБ}}(Y))) = Y \| \sigma_{\text{СБ}}(Y)$
  - в) проверить, аутентичен ли  $(\text{ид}) \text{М}$  (см. схему нумерации модулей),
  - г) проверить, действительна ли дата,
  - д) проверить, выполняется ли

$$D_{\text{СБ}}(\sigma_{\text{СБ}}(Y)) = h(Y),$$

где ОСБ - основной сервер безопасности,

СБ - сервер безопасности,

М - модуль,

|| - знак конкатенации,

ид - идентификационный номер,

h - хэш-функция,

С - постоянное случайное число, используемое всеми модулями совместно,

D - алгоритм с использованием ключа общего пользования для расшифровывания и проверки цифровой подписи,

КОП - ключ общего пользования (включая длину ключа),

$$\sigma = E \cdot h,$$

серт. - сертификат,

E - алгоритм с использованием частного ключа для шифрования и создания цифровой подписи.

Следует отметить, что E и D могут также использоваться для расшифровывания и шифрования соответственно при использовании с другими приложениями.

Схема нумерации модулей.

Основные серверы 1182 безопасности, серверы 1184 безопасности, денежные модули 1188 банковских кассиров, модули 1190 генератора денег, модули 1192 обслуживания клиентов и денежные модули 1186 транзакций получают идентификационные номера (ид), чтобы с помощью этого номера можно было осуществлять аутентификацию. Генерируется 48-разрядное простое число "p", и в процессе обеспечения безопасности находится первообразный корень "a" по модулю p (где  $a^n \not\equiv 1(p)$  для всех  $1 \leq n < p-1$ ). Обе величины a и p секретно загружаются во все модули в системе

в процессе их изготовления при помощи основных серверов безопасности.

Схема работает следующим образом:

если  $a^n \equiv m(p)$  и

(1)  $1 \leq m \leq 99999$ , то n назначается в качестве (ид) основного сервера безопасности,

(2)  $100000 \leq m \leq 999999$ , то n назначается в качестве (ид) сервера безопасности,

(3)  $1000000 \leq m \leq 6999999$ , то n назначается в качестве (ид) модуля банковского кассира,

(4)  $7000000 \leq m \leq 9999999$ , то n назначается в качестве (ид) модуля генератора денег,

(5)  $10000000 \leq m \leq 11999999$ , то n назначается в качестве (ид) модуля обслуживания клиентов,

(6)  $m \geq 12000000$ , то n назначается в качестве (ид) денежного модуля транзакций. Если модуль или сервер подтверждает достоверность сертификата, то этот модуль или сервер аутентифицирует идентификационный номер n (например, (ид)М, (ид)СБ или (ид)ОСБ) путем вычисления  $a^n \equiv m(p)$ , а затем проверяет, находится ли m в требуемом интервале.

Сеть безопасности.

Как показано на фиг. 34, сеть 1196 безопасности и ЛВС 1194 безопасности связывают серверы 1184 безопасности с основными серверами 1182 безопасности. Серверы 1184 безопасности первоначально сертифицируют денежные модули и модули 1192 обслуживания клиентов при их изготовлении. Такие серверы безопасности могут быть связаны посредством ЛВС 1202 производства модулей. Они передают модулям информацию о безопасности, такую, как список неверных идентификаторов и список основных серверов безопасности и их ключей общего пользования. Список неверных идентификаторов содержит идентификаторы денежных модулей, модулей обслуживания клиентов и серверов безопасности, транзакции которых заблокированы. Пересертификация этих модулей описана ниже со ссылкой на блок-схему, поясняющую процесс входа в сеть.

Серверы 1184 безопасности первоначально сертифицируются основными серверами 1182 безопасности в процессе изготовления, соответственно производства. Такие основные серверы 1182 безопасности могут быть связаны посредством ЛВС 1204 производства серверов безопасности. Как показано на фиг. 33Б, серверы 1184 безопасности получают различную информацию о безопасности, которую они передают другим модулям. Серверы безопасности обеспечивают безопасное обслуживание сети 1198 электронной

денежной системы и банковских ЛВС 1200, например, входа в сеть, когда серверы передают обновленную информацию о безопасности. Серверы 1184 безопасности получают эту информацию от основных серверов 1182 безопасности по сети 1196 безопасности. Денежные модули 1186 транзакций связываются с сетью 1198 электронной денежной системы через сетевые серверы 1206. Подключенные к системе банки имеют денежные модули 1188 банковских кассиров, а также генератор (ы) 1190 денег, соединенные со своей банковской ЛВС 1200.

Сеть 1196 безопасности является сетью с зашифрованными линиями связи. Кроме того, основные серверы безопасности и серверы безопасности совместно используют общий симметричный ключ (ключ шифрования сети безопасности). Этот ключ периодически меняется определенным основным сервером 1182 при помощи ключа общего пользования. Основной сервер 1182 шифрует симметричный ключ при помощи своего частного ключа, подписывает ключ и передает изменения другим основным серверам 1182 по ЛВС 1194 безопасности, а серверам 1184 безопасности - по сети 1196 безопасности.

Список неверных идентификаторов контролируется определенным основным сервером 1182. Этот список пополняется при взаимодействии с банками-участниками, органами обеспечения правопорядка и абонентами системы.

Длина ключей общего пользования для серверов безопасности и модулей периодически меняется. Длина ключа обычно увеличивается для поддержания высокого уровня безопасности. Новые назначенные длины ключей передаются основным серверам безопасности посредством определенного основного сервера. Новые длины передаются серверам безопасности посредством основных серверов, когда посылаются новые списки неверных идентификаторов или после пересертификации. В случае возникновения опасности "взлома" системы основной сервер безопасности может вызвать глобальную пересертификацию.

Длина ключа общего пользования для каждого основного сервера не меняется. Создается временная таблица, которая определяет график внедрения и прекращения эксплуатации основных серверов безопасности. Новые серверы наиболее вероятно будут иметь более длинные ключи, кроме случаев, когда они внедряются из-за увеличения объема транзакций. Список ключей общего пользования активного основного сервера безопасности создается основным сервером безопасности и шифруется этим сервером при помощи его частного ключа. Затем список передается другим серверам безопасности.

На фиг. 35А показаны функциональные компоненты сервера 1184 безопасности. Функция 1208 "Внешний интерфейс" обеспечивает взаимодействие с сетью на уровне передачи данных. Функция 1210 "Менеджер сеанса связи" управляет различными аспектами безопасности сеанса транзакции. Функция 1212 "Вход в сеть" управляет функциями безопасности для входа в сеть. Функция 1214 "Создание сертификата" создает сертификат для любого денежного модуля (в основном

сервере безопасности эта функция сертифицирует серверы безопасности). Функция 1216 "Создание профиля счета" сертифицирует и подписывает профиль банковского счета, который разрешает денежному модулю доступ к другим банковским счетам абонента. Функция 1218 "Распределение сертификационных ключей" распределяет список действительных ключей общего пользования основного сервера безопасности сертификационного агентства среди денежных модулей (основной сервер безопасности также распространяет глобальное сертификационное сообщение). Функция 1220 "Управление списком неверных идентификаторов" ведет список неверных идентификаторов и распространяет его. Функция 1222 "Синхронизация даты/времени" поддерживает синхронизацию функции "Часы/таймер" денежного модуля с системным временем. Функции 1224 "Часы/таймер" и функция 1226 "Криптография" идентичны этим же функциям в денежных модулях.

На фиг. 35Б показаны функциональные компоненты сетевого сервера 1206. Функция 1226 "Внешний интерфейс" обеспечивает взаимодействие с сетью на уровне передачи данных. Функция 1230 "Менеджер связи" управляет сеансом связи между денежными модулями и между денежным модулем и сервером безопасности. Функция 1232 "Вход в сеть" управляет процессом входа денежного модуля в сеть. Функция 1234 "Маршрутизация сообщений" обеспечивает направленную пересылку сообщений, управление пересылкой сообщений во время входа в систему и во время сеанса связи с денежным модулем. Функция 1236 "Связь напрямую с банком" обеспечивает предоставление информации об услугах, оказываемых банками-участниками. Функция 1238 "Криптография" обеспечивает выполнение функции 1240 "Симметричный ключ" и функции 1242 "Генератор случайных чисел". Функция 1240 "Симметричный ключ" шифрует сообщения между сетевым сервером 1206 и модулями, имеющими доступ к сети, а также между сетевым сервером 1206 и серверами 1184 безопасности, функция 1242 "Генератор случайных чисел" создает случайные числа для шифрования ключей и проверочных сообщений.

Вход в сеть.

Общий обзор процедуры входа в сеть описан со ссылками на фиг. 36. Протокол входа в систему описывает ситуацию, когда модулю 1243 требуется доступ к сети 1198 электронной денежной системы для пересертификации, депонирования денег, снятия денег или по каким-либо другим причинам. Модуль 1243 может быть денежным модулем 1186 транзакций, денежным модулем 1188 банковского кассира, модулем 1190 генератора денег или модулем 1192 обслуживания клиентов.

(а) Устанавливается связь между модулем 1243 и сетевым сервером 1206.

(б) Сертификат модуля передается сетевому серверу 1206.

(в) Сетевой сервер 1206 вырабатывает случайное проверочное число V и случайный ключ K; затем сетевой сервер передает сертификат модуля, V и K серверу 1184 безопасности (зашифрованными при помощи ключа связи сетевого сервера с сервером безопасности (CC/CB)).



(г) Модуль 1243 и сервер 1184 безопасности устанавливают безопасный сеанс связи (при помощи ключа связи денежного модуля с сервером безопасности (ДМ/СБ)).

(д) Сервер 1184 безопасности передает дату/время, обновленный список неверных идентификаторов, обновленный список ключей общего пользования основного сервера безопасности, длину ключа общего пользования, сообщение о глобальной пересертификации (при необходимости) и пересертифицированный сертификат модуля (при необходимости).

(е) Сеанс связи с модулем 1243 заканчивается, модулю 1243 посылаются V и K.

(ж) V шифруется при помощи K и посылается сетевому серверу 1206.

(з) Сетевой сервер 1206 подтверждает модулю 1243 вход в сеть.

(и) Модуль 1243 информирует затем сетевой сервер 1206 об адресате информации в сети (если таковых несколько), с которым он хотел бы связаться.

(к) Сетевой сервер 1206 устанавливает связь с адресатом информации.

Процесс входа в сеть построен таким образом, чтобы никто не мог "обмануть" модуль 1243 или перехватить в явном виде какую-либо его информацию. На фиг. 37 представлен подробный процесс входа в сеть.

Функция "Коммуникации А" устанавливает связь с сетью 1198 электронной денежной системы (шаг 1244). Функция "Поддержание безопасности А" посылает сетевому серверу 1206 свой сертификат (шаг 1246). Функция "Вход в сеть сетевого сервера" получает сертификат (шаг 1248). Функция "Генератор случайных чисел сетевого сервера" вырабатывает случайный ключ K и случайное проверочное число V (шаг 1250). Функция "Симметричный ключ сетевого сервера" шифрует сертификат модуля, V и K при помощи ключа СС/СБ (шаг 1252). Ключи СС/СБ являются локальными симметричными ключами, устанавливаемыми на сетевых серверах 1206 и серверах 1184 безопасности, которые связываются для входа в сеть. Функция "Вход в сеть сетевого сервера" посылает сертификат, V и K серверу 1184 безопасности, а функция "Вход в сеть сервера безопасности" принимает это сообщение, после чего функция "Симметричный ключ сервера безопасности" дешифрует это сообщение (шаги 1254-1258). Функция "Вход в сеть сервера безопасности" сохраняет K и V, а затем посылает сертификат модуля функции "Ключ общего пользования сервера безопасности" для подтверждения (шаги 1260-1264).

Если сертификат модуля недействителен, то функция "Вход в сеть сервера безопасности" создает сообщения для запрета доступа, передаваемые сетевому серверу 1206 и модулю 1243 (шаг 1266). Функция "Ключ общего пользования сервера безопасности" шифрует сообщение для модуля 1243 при помощи ключа общего пользования модуля, а функция "Менеджер сеанса связи сервера безопасности" посылает это сообщение сетевому серверу (шаги 1268-1270). Функция "Вход в сеть сетевого сервера" принимает сообщения и отмечает, что доступ запрещен. Зашиф-

рованное сообщение затем отсылается модулю, а сетевой сервер отсоединяется (шаг 1272). Функция "Менеджер сеанса связи А" принимает сообщения, функция "Ключ общего пользования А" расшифровывает сообщение, а функция "Менеджер сеанса связи А" отмечает, что во входе в систему было отказано (шаги 1274-1278). Если устройство, запрашивавшее вход в систему, было денежным модулем транзакций, то функция "Связь с абонентом А" соответственно информирует абонента (шаги 1280-1282). В других случаях функция "Связь с банком А" информирует банк (шаг 1284).

Если же, с другой стороны, сертификат модуля действителен, то функция "Управление списком неверных идентификаторов сервера безопасности" проверяет, есть ли идентификатор модуля в списке неверных идентификаторов (шаги 1286-1288). Если идентификатор есть в этом списке, то доступ к сети запрещается. В противном случае функция "Генератор случайных чисел сервера безопасности" создает случайное число R и проверочное сообщение (шаг 1290). Функция "Вход в сеть сервера безопасности" компонует из R, проверочного сообщения и сертификата сервера безопасности одно сообщение, которое шифруется при помощи ключа общего пользования А функцией "Ключ общего пользования сервера безопасности" (шаги 1292-1294). Это сообщение посылается к А, где функция "Ключ общего пользования А" расшифровывает сообщение и проверяет сертификат сервера безопасности (шаг 1298).

Если сертификат недействителен, то А записывает прерывание сеанса связи и соответственно информирует абонента или банк (шаги 1304-1306). Если же сертификат действителен, то функция "Поддержание безопасности А" проверяет, находится ли идентификатор сервера безопасности в списке неверных идентификаторов (шаги 1308-1310). Если идентификатор находится в этом списке, то сеанс связи прерывается (шаги 1300-1306). Если идентификатора нет в списке, то функция "Генератор случайных чисел А" создает случайное число R(A) (шаг 1312). Функция "Поддержание безопасности А" формирует ключ сеанса связи (СС/СБ) при помощи операции ИСКЛЮЧАЮЩЕЕ ИЛИ над R(A) и R и затем сохраняет этот ключ сеанса связи (шаг 1314).

Проверочное сообщение и R(A) компонуется в одно сообщение, которое шифруется при помощи ключа общего пользования сервера безопасности (шаг 1316). Функция "Менеджер сеанса связи А" посылает это сообщение функции "Вход в сеть сервера безопасности", а функция "Ключ общего пользования сервера безопасности" расшифровывает это сообщение (шаги 1318-1322).

Функция "Вход в сеть сервера безопасности" проверяет, является ли проверочное сообщение одним из тех, которые она создала (шаги 1324-1326). Если это не так, то сервер безопасности запрещает доступ к сети. Если проверочное сообщение правильное, то функция "Симметричный ключ сервера безопасности" формирует ключ сеанса связи (СС/СБ) путем выполнения операции ИСКЛЮЧАЮЩЕЕ ИЛИ над R(A) и R (шаг 1328). Функция "Менеджер сеанса связи сервера безопасности" отмечает начало сеанса связи и по-

сылает А подтверждение о приеме при помощи подпрограммы "Посылка сообщения" (шаги 1330-1332). Функция "Менеджер сеанса связи А" получает подтверждение о приеме и отмечает начало сеанса связи (шаг 1334).

Функция "Часы/таймер А" посылает значения времени и даты функции "Менеджер сеанса связи", который отправляет их серверу безопасности (шаги 1336-1340). Функция "Синхронизация даты/времени сервера безопасности" принимает дату и время и проверяет, соответствуют ли они заданным параметрам (шаги 1342-1344). Если они не соответствуют заданным параметрам, то функция "Синхронизация даты/времени сервера безопасности" посылает новые значения даты и времени функции "Менеджер сеанса связи А" (шаги 1346-1350). Затем функция "Часы/таймер А" настраивает дату и время (шаг 1352). После этого А снова посылает свои дату и время серверу безопасности для повторной проверки. Если попытка синхронизации часов осуществляется более установленного количества раз, то о неисправности часов сообщается абоненту или банку, которые затем при необходимости могут еще раз осуществить эту попытку (шаги 1354-1362).

Если же, однако, время и дата соответствуют заданным параметрам, то функция "Вход в сеть сервера безопасности" компонует сообщение, содержащее список неверных идентификаторов, новый список ключей общего пользования основного сервера безопасности (который берется у функции "Распространение сертификационных ключей") и длину ключа общего пользования (размер ключей общего пользования периодически меняется) (шаг 1364). Функция "Создание сертификата сервера безопасности" проверяет, была ли назначена глобальная пересертификация, и устанавливает, что период времени для глобальной пересертификации не истек (шаги 1366-1368). Такой период времени должен быть достаточным, чтобы каждый сертификат был пересертифицирован либо истек срок его действия. Эта функция должна также проверять, когда модуль был в последний раз пересертифицирован, т.к. если он был сертифицирован в период глобальной пересертификации, то не будет необходимости пересертифицировать его заново.

При необходимости пересертификации функция "Создание сертификата сервера безопасности" добавляет к предыдущему сообщению, что "модуль следует пересертифицировать" (шаг 1370). Затем, независимо от того, вызвана пересертификация или нет, функция "Ключ общего пользования сервера безопасности" подписывает сообщение (шаг 1372). Сообщение посылается к А, где функция "Ключ общего пользования А" проверяет цифровую подпись на сообщении (шаги 1374-1378). Если подпись недействительна, то сеанс связи прерывается. Если подпись действительна, то функция "Ключ общего пользования А" расшифровывает список ключей общего пользования основного сервера безопасности при помощи существующего ключа общего пользования основного сервера безопасности (шаг 1380). Обновленный список ключей общего пользования основного сервера безопасности был предварительно зашифрован при помощи частного ключа ис-

ходного основного сервера безопасности. Функция "Поддержание безопасности А" затем обновляет свой список неверных идентификаторов, список ключей общего пользования и длину ключа (шаг 1382).

Затем модуль А проверяет, требуется ли пересертификация его сертификата (либо по причине команды на глобальную пересертификацию, либо вследствие истечения срока действия сертификата) (шаги 1384-1386). Если требуется новый сертификат, то функция "Поддержание безопасности А" инициирует создание нового сертификата (шаг 1388). Функция "Ключ общего пользования А" вырабатывает новые ключи и подписывает новый ключ общего пользования своим старым ключом общего пользования (шаг 1390). Функция "Менеджер сеанса связи А" посылает подписанный новый ключ функции "Создание сертификата сервера безопасности" (шаги 1392-1396). Затем функция "Ключ общего пользования сервера безопасности" проверяет подпись на новом ключе общего пользования (шаги 1398-1400). Если подпись недействительна, то сервер безопасности запрещает доступ к сети. Если подпись действительна, то функция "Ключ общего пользования сервера безопасности" подписывает новый сертификат модуля и посылает его модулю (шаг 1402). Функция "Менеджер сеанса связи А" принимает сертификат, функция "Поддержание безопасности А" проверяет сертификат, а функция "Ключ общего пользования А" проверяет подпись (шаги 1404-1410).

Если сертификат недействителен, то функция "Менеджер сеанса связи А" посылает серверу безопасности сообщение "Сертификат недействителен" и сертификат (шаг 1412). Функция "Вход в сеть сервера безопасности" принимает сообщение, а функция "Ключ общего пользования сервера безопасности" проверяет подпись (шаги 1414-1418). Если сервер безопасности определяет, что сертификат фактически действителен, то он запрещает модулю доступ к сети. Если же сертификат недействителен, то функция "Менеджер сеанса связи сервера безопасности" информирует сетевой сервер, что он отсоединится от сети (шаг 1420). Функция "Вход в сеть сетевого сервера" информирует модуль о неисправности (шаг 1422). Затем модуль посылает запрос абоненту или банку на повтор попытки (шаги 1424-1432).

Если же, с другой стороны, модуль определяет, что его новый сертификат действителен, то функция "Менеджер сеанса связи А" посылает подтверждение о приеме серверу безопасности (шаг 1434). Аналогично этому, если не требовалось нового сертификата, функция "Поддержание безопасности А" посылает подтверждающее сообщение серверу безопасности (шаги 1436-1438). В любом случае функция "Менеджер сеанса связи сервера безопасности" принимает подтверждение о приеме и отмечает конец своего сеанса связи с модулем (шаг 1440). Затем функция "Регистрация в сети сервера безопасности" посылает К и V к А (шаги 1442-1444). Функция "Менеджер сеанса связи А" принимает это сообщение, а функция "Симметричный ключ А" шифрует V при помощи К и посылает это сообщение сетевому серверу (шаги 1446-1448). Функция "Вход в сеть сетевого сервера" принимает сообщение, а функция "Симметрич-

ный ключ сетевого сервера" расшифровывает это сообщение и проверяет, является ли V тем же самым V, которое было сформировано ранее (шаги 1450-1454).

Если V неправильное, то функция "Вход в сеть сетевого сервера" посылает A сообщение об отказе во входе в систему и затем отсоединяется (шаги 1456-1458). Если V правильное, то функция "Вход в сеть сетевого сервера" посылает A подтверждение приема (шаг 1460). В завершение функция "Менеджер сеанса связи A" принимает подтверждение о приеме и отмечает, что A вошел в сеть 1198 электронной денежной системы (шаг 1462).

Установление сеанса связи.

На фиг. 38 показан протокол установления сеанса связи, функция "Менеджер сеанса связи A" проверяет, требуется ли соединение по сети с денежным модулем или сервером безопасности (шаги 1464-1466). Если такое соединение требуется, то функция "Симметричный ключ A" шифрует при помощи ключа K требуемого адресата информации в сети (шаг 1468). Функция "Менеджер сеанса связи A" передает данные о требуемом адресате информации сетевому серверу (шаг 1470). Затем сетевой сервер устанавливает связь с адресатом информации B и посылает подтверждение о приеме, которое принимается функцией "Менеджер сеанса связи A" (шаги 1472-1474).

Функция "Поддержание безопасности A" посылает свой сертификат функции "Менеджер сеанса связи A", который передает его B (шаги 1476-1478). Функция "Менеджер сеанса связи B" получает сертификат, а функция "Поддержание безопасности B" (если B является сервером безопасности, то эта функция реализуется функцией "Менеджер сеанса связи") проверяет этот сертификат (шаги 1480-1484). Если сертификат недействителен, то функция "Менеджер сеанса связи B" отмечает, что сеанс связи прерван, и соответственно информирует абонента или банк (шаги 1486-1492) (если B является сервером безопасности, то B отмечает, что транзакция прекращена).

Если сертификат действителен, то функция "Поддержание безопасности B" проверяет, находится ли A в списке неверных идентификаторов (шаги 1494-1496). Если A находится в этом списке, то сеанс связи прерывается. Если A нет в списке, то функция "Генератор случайных чисел B" создает случайное число R(B) и проверочное сообщение B (шаг 1498). Функция "Часы/таймер B" запрашивает дату и время (шаг 1500). Функция "Поддержание безопасности B" компонует в одно сообщение R(B), проверочное сообщение B, время и дату и сертификат B (шаг 1502). Функция "Ключ общего пользования B" шифрует это сообщение при помощи ключа общего пользования A, а функция "Менеджер сеанса связи B" посылает это сообщение к A (шаги 1504-1506).

Далее функция "Менеджер сеанса связи A" принимает сообщение, функция "Ключ общего пользования A" расшифровывает сообщение, а функция "Поддержание безопасности A" проверяет сертификат B (шаги 1508-1514). Если сертификат недействителен, то функция "Менеджер сеанса связи A" отмечает, что сеанс связи прер-

ван, и соответственно информирует абонента или банк (шаги 1516-1522). Если сертификат действителен, то функция "Поддержание безопасности A" проверяет, находится ли B в списке неверных идентификаторов (шаги 1524-1526). Если B находится в этом списке, то сеанс связи прерывается. Если B нет в списке, то функция "Поддержание безопасности A" затребует дату и время и сравнивает их с датой и временем B (шаги 1528-1530). Если дата и время находятся вне установленных пределов, то сеанс связи прерывается.

Если же дата и время находятся в установленных пределах, то функция "Генератор случайных чисел A" создает случайное число R(A) и проверочное сообщение A (шаг 1532). Функция "Поддержание безопасности A" затем формирует ключ сеанса связи путем операции ИСКЛЮЧАЮЩЕЕ ИЛИ над R(A) и R(B) (шаг 1534). Проверочное сообщение A, проверочное сообщение B, время, дата и R(A) компонуются в одно сообщение и шифруются при помощи ключа общего пользования B (шаг 1536). Это сообщение посылается к B функцией "Менеджер сеанса связи A" (шаг 1538). Функция "Менеджер сеанса связи B" принимает сообщение, функция "Ключ общего пользования B" расшифровывает сообщение, а функция "Поддержание безопасности B" проверяет проверочное сообщение B (шаги 1540-1546). Если проверочное сообщение B неправильное, то сеанс связи прерывается. Если проверочное сообщение B правильное, то функция "Поддержание безопасности B" формирует ключ сеанса связи путем операции ИСКЛЮЧАЮЩЕЕ ИЛИ над R(A) и R(B) (шаг 1548). После этого затребуются значения времени и даты, которые сравниваются со временем и датой A для проверки, находятся ли они в соответственно заданных друг по отношению к другу пределах (шаг 1550). Если время и дата вне этих пределов, то сеанс связи прерывается. Если время и дата в заданных пределах, то функция "Менеджер сеанса связи B" отмечает начало сеанса связи (шаг 1552).

Затем функция "Менеджер сеанса связи" посылает A подтверждение о приеме и проверочное сообщение A (шаги 1554-1556). Функция "Менеджер сеанса связи A" принимает сообщение, а функция "Поддержание безопасности A" проверяет проверочное сообщение A (шаги 1558-1562). Если проверочное сообщение неправильное, то сеанс связи прерывается. Если же проверочное сообщение правильное, то функция "Менеджер сеанса связи A" отмечает начало сеанса связи (шаг 1564).

Передача банкнот.

На фиг. 39 показан протокол передачи банкнот. Функция "Каталог банкнот X" выбирает банкноты и суммы для передачи (шаг 1566). Возможными отправными точками в выборе банкнот для передачи, например, могут быть: (1) минимизация количества цифровых подписей (которые требуют времени на обработку); (2) минимизация размера пакета; (3) максимизация пригодности электронных банкнот, оставшихся у передающего абонента (т.е. передача банкнот, до истечения срока действия которых осталось наименьшее количество времени). Эти задачи могут быть решены при помощи следующего алгоритма передачи банкнот:

(1) определить все возможные альтернативы, содержащие минимальное количество банкнот; (2) определить, какие из этих альтернатив имеют наименьшее число передач; (3) если из шага 2 следует более одного выбора, то выбрать тот, который имеет наименьшее число банкнотодней. "Банкнотодни" представляют собой остаточное значение передаваемой банкноты, умноженное на количество дней, оставшееся до окончания срока действия банкноты, просуммированное по всем банкнотам в пакете.

Функция "Банкноты X" создает трансфер, добавляемый к каждой передаваемой банкноте (шаг 1568). Функция "Ключ общего пользования X" создает подписи для банкноты (шаг 1570). Функция "Менеджер пакета X" затем komponует банкноты и их новые трансферы и подписи в пакет и посылает пакет к Y (шаги 1572-1574). Функция "Менеджер пакета Y" принимает пакет и дизассемблирует (разбирает) его (шаг 1576).

Функция "Проверка Y" проверяет все сертификаты в банкнотах (например, сертификат генератора денег и все сертификаты трансферов). Затем все трансферы к сертификатам проверяются при помощи подтверждения, что все отправители и получатели соответствуют друг другу в предыстории передачи электронной банкноты. Кроме того, проверяется соответствие переданной суммы ожидаемой сумме (шаги 1578-1580). Если такого соответствия нет, то транзакция прекращается (шаг 1582).

Если же соответствие есть, а Y является денежным модулем транзакций, то функция "Проверка Y" проверяет сроки действия банкнот(ы) (шаги 1584-1588). Если банкноты(а) просрочены(а), то транзакция прекращается. Если же они не просрочены, то функция "Проверка Y" сверяет каждый идентификатор из трансферов банкноты со списком неверных идентификаторов (шаги 1590-1592). Если хотя бы один из идентификаторов трансферов находится в списке неверных идентификаторов, то транзакция прекращается.

Если идентификаторов трансферов нет в списке неверных идентификаторов (либо Y не является денежным модулем транзакций), то функция "Ключ общего пользования Y" проверяет действительность подписей банкнот(ы) (шаги 1594-1596). Если подписи недействительны, транзакция прекращается. Если же подписи действительны, то функция "Банкноты Y" помещает банкноты (банкноту) в держатель денег (шаг 1598). В завершение функция "Каталог банкнот Y" обновляет местонахождение и количество банкнот (шаг 1600).

Обмен иностранной валюты.

На фиг. 40 показан протокол транзакции, выполняемой для обмена иностранной валюты на примере долларов и фунтов. Первоначально A дает согласие обменять B доллары \$ на фунты (£) по обменному курсу \$/£ (шаг 1602). Затем A и B входят в систему, подсоединяясь к своим денежным модулям, и приглашают своих абонентов ввести тип транзакции (шаги 1604-1610). A выбирает покупку иностранной валюты, а B выбирает соответственно продажу (шаги 1612-1614). После этого A и B устанавливают безопасный транзакционный сеанс связи (шаги 1616-1620).

Функция "Связь с абонентом A" запрашивает владельца/держателя A о сумме в долларах, которую он желает обменять (шаг 1622). Функция "Платеж/обмен A" принимает сумму, а функция "Каталог банкнот A" проверяет, имеет ли A достаточно средств (шаги 1624-1628). Если средств недостаточно, то функция "Связь с абонентом A" запрашивает новую сумму, которая вновь сверяется с имеющимися в наличии средствами (шаги 1630-1632). Если новая сумма не задана, то транзакция прекращается (шаг 1634).

Если средств достаточно, то функция "Платеж/обмен A" посылает сумму в долларах B (шаги 1636-1638). Функция "Связь с абонентом B" посылает запрос владельцу/держателю B выбрать либо сумму в фунтах, которую он хочет обменять на доллары, либо просто обменный курс для долларов (шаг 1640). Функция "Каталог банкнот B" проверяет наличие достаточных средств (шаги 1642-1644). Если средств недостаточно, то функция "Связь с абонентом B" запрашивает новый курс и снова сверяет наличие средств (шаги 1646-1648). Если же новый курс не выбран, то функция "Платеж/обмен B" информирует A о нехватке средств (шаги 1650-1652). Затем A может выбрать новую сумму для обмена или прекратить транзакцию (шаги 1630-1634).

Если B имеет достаточно средств для транзакции, то функция "Платеж/обмен B" посылает A уведомление и сумму в фунтах для обмена (также посылается эквивалентный курс) (шаги 1654-1656). Функция "Связь с абонентом A" запрашивает проверку суммы в фунтах и курса (шаги 1658-1660). Если сумма и курс неправильные, то функция "Платеж/обмена A" информирует B, что сумма и курс неправильные (шаги 1662-1664). Затем функция "Связь с абонентом B" запрашивает новый курс (шаги 1666-1668). Если не выбрано никакого нового курса, то транзакция прекращается (шаг 1670).

Если же, однако, A удостоверяется в правильности суммы и курса, то функция "Платеж/обмен A" передает сумму в долларах держателю денег (шаг 1672). Затем долларовые банкноты передаются от A к B (шаг 1674). Функция "Платежа/обмен B" передает сумму в фунтах своему держателю денег (шаг 1676). Затем фунтовые банкноты передаются от B к A (шаг 1678).

В этот момент транзакции и A, и B условно имеют правильные суммы иностранных банкнот. Каждый из A и B принял участие в двух трансферах: трансферы A:

(1) A передал доллары B; (2) A принял фунты от B; трансферы B: (1) B передал фунты A; (2) B принял доллары от A. Для завершения транзакции обмена валюты A в этот момент должен зафиксировать (т.е. завершить и окончательно записать в своем журнале транзакций) оба своих трансфера. Точно так же B должен зафиксировать оба своих трансфера. Следует отметить, что A может совершать трансферы обмена валюты A → B (доллары от A к B) и B → A (фунты от B к A) отдельно. Точно так же и B может совершать трансферы обмена валюты A → B и B → A отдельно.

Следующая часть протокола обмена валюты построена таким образом, чтобы ни одна из сторон не знала порядок, в котором денежные мо-

дули будут фиксировать транзакцию. Такая неопределенность воспрепятствует преднамеренным попыткам какой-либо из сторон осуществить мошенничество. За основание берется функция  $S(X)$ , определяемая как  $S(0) = A$  и  $S(1) = B$ , где  $A$  и  $B$  соответствуют денежным модулям  $A$  и  $B$ . Таким образом, если  $X$  выбирается случайным образом из 0 и 1, то случайным образом помечаются денежные модули  $A$  и  $B$ .

Следующая процедура используется с той целью, чтобы позволить  $A$  и  $B$  совместно установить случайные значения  $X$ .  $R(A)$  и  $R(B)$  являются случайными числами, выработанными  $A$  и  $B$  соответственно во время выполнения подпрограммы "Установление сеанса связи". Определяется четность операции ИСКЛЮЧАЮЩЕЕ ИЛИ от  $R(A)$  и  $R(B)$  (при помощи ИСКЛЮЧАЮЩЕГО ИЛИ для всех бит операции  $R(A)$  ИСКЛЮЧАЮЩЕЕ ИЛИ  $R(B)$ ). Эта четность является случайным числом  $X$ .  $\bar{X}$  является дополнением  $X$  ( $\bar{X} = X$  ИСКЛЮЧАЮЩЕЕ ИЛИ 1).

Как показано на фиг. 40, функция "Журнал транзакций  $A$ " условно обновляет свой журнал транзакций для записи трансфера  $S(X)$  в  $S(\bar{X})$  (шаг 1680). Если  $X$  рассчитано равным 0, то условно записывается трансфер от  $A$  к  $B$  (т.е. передача долларов). Если  $X$  рассчитывается как 1, то условно записывается трансфер от  $B$  к  $A$  (т.е. передача фунтов). Поскольку записи условные, то журнал может быть возвращен в исходное состояние в случае, если денежный модуль  $A$  прекратит транзакцию. Изменения в журнале становятся окончательными, как только изменения будут объявлены безусловными (либо в соответствии с тем, как это показано на блок-схеме алгоритма, либо во время фиксации). Затем функция "Менеджер сеанса связи  $A$ " посылает  $B$  сообщение "Журнал обновлен" (шаги 1682-1684). В ответ функция "Журнал транзакций  $B$ " также условно обновляет свой журнал для записи трансфера  $S(X)$  в  $S(X)$  (шаг 1686).

Если  $X=1$ , то функция "Журнал транзакций  $B$ " объявляет изменения в журнале безусловными (шаги 1688-1690). Таким образом, в этот момент  $B$  зафиксировал свой трансфер фунтов к  $A$ . Далее  $B$  следует протоколу фиксации (шаг 1692), описанному ниже со ссылкой на фиг. 41. В этой ситуации  $A$  фиксирует оба своих трансфера (т.е. передачу долларов и получение фунтов), а  $B$  фиксирует один свой невыполненный (незафиксированный) трансфер, а именно получение долларов.

Если же, однако,  $X=0$  (шаг 1688), то функция "Менеджер сеанса связи  $B$ " посылает  $A$  сообщение "Начать фиксацию" (шаги 1694-1696). Затем функция 1 "Журнал транзакций  $A$ " объявляет изменения в своем журнале безусловными (шаг 1698), фиксируя таким образом свой трансфер долларов. Затем вызывается протокол фиксации по фиг.41 (шаг 1700). Во время выполнения этого протокола (описанного ниже)  $B$  фиксирует оба своих трансфера (т.е. передачу фунтов и получение долларов), а  $A$  фиксирует один свой невыполненный трансфер, а именно получение фунтов.

Таким образом, протокол обмена валюты гарантирует, что ни одна из сторон не знает, чей трансфер (передача долларов от  $A$  или передача фунтов от  $B$ ) будет зафиксирован первым. Это

уменьшает стимул какой-либо из сторон к мошенничеству.

Фиксация (для модуля).

На фиг. 41 показан протокол фиксации для модулей, функция "Менеджер сеанса связи  $X$ " посылает  $Y$  сообщение "Готов к фиксации" (шаги 1702-1704). Это сообщение обязывает модуль, принявший его, зафиксировать транзакцию. В обычном процессе передачи денег такая методика передачи сообщения, обязывающего осуществить фиксацию первым, используется с той целью, чтобы сторона, передающая деньги, фиксировала транзакцию первой, исключая тем самым возможность дублирования денег.

Затем функция "Менеджер сеанса связи  $Y$ " посылает к  $X$  подтверждение о приеме (шаги 1706-1708) и фиксирует все невыполненные транзакции путем обновления своего журнала транзакций (шаг 1710). Кроме того, если  $Y$  является денежным модулем транзакций, то функция "Связь с абонентом  $Y$ " сообщает абоненту об успешной транзакции (шаги 1712-1714). Затем функция "Менеджер сеанса связи  $Y$ " записывает конец сеанса связи (шаг 1716).

Функция "Журнал транзакций  $X$ " принимает подтверждение о приеме от  $Y$  и обновляет свой журнал транзакций, фиксируя таким образом все невыполненные трансферы.  $X$  завершает свою фиксацию таким же образом, что и  $Y$  (шаги 1718-1724).

Прекращение транзакции (для модуля).

На фиг. 42 показан протокол прекращения транзакции для модулей. Функция "Менеджер сеанса связи" отменяет изменения и отмечает, что транзакция прекращена (шаг 1726). Затем функция "Менеджер сеанса связи  $X$ " проверяет, было ли послано сообщение "Готов к фиксации" (шаги 1728-1730). Если сообщение было послано, то  $X$  обновляет свой журнал транзакций (шаг 1732), записывая, что  $X$  зафиксировал транзакцию после отправки сообщения о готовности к фиксации, и записывая идентификаторы банкнот и номиналы всех банкнот, полученных при выполнении протокола передачи банкнот. Таким образом, протокол прекращения регистрирует информацию, в то время как в течение неудачного выполнения подпрограммы фиксации вызывается подпрограмма "Прекращение".

Если  $X$  является денежным модулем 1186 транзакций и было послано сообщение о готовности к фиксации, то функция "Связь с абонентом  $X$ " информирует своего абонента, что транзакция была прекращена и что могла быть ошибка передачи денег (шаги 1734-1738).

Если  $X$  является денежным модулем 1188 банковского кассира, то функция "Связь с банком  $X$ " информирует банк, что он должен отменить свои бухгалтерские операции, т.е. транзакции, связанные с бухгалтерским учетом (при помощи соответствующих дебетов и кредитов) (шаги 1740-1742). Если  $X$  является денежным модулем 1186 транзакций и не было послано сообщения о готовности к фиксации, то функция "Связь с абонентом  $X$ " информирует абонента, что транзакция была прекращена (шаг 1744).

В любом случае функция "Менеджер сеанса связи  $X$ " посылает  $Y$  сообщение о том, что тран-

закция не может быть завершена (шаги 1746-1748). Функция "Менеджер сеанса связи Y" отменяет свои изменения и отмечает, что транзакция прекращена (шаг 1750). Затем Y информирует своего абонента, что транзакция прекращена (шаги 1752-1754) либо информирует банк о необходимости отменить транзакции, связанные с бухгалтерским учетом (шаги 1756-1758).

Как описано выше, если транзакция прерывается при выполнении протокола фиксации, то возникает возможность потери банкнот. Если это происходит, то получатель прекратит транзакцию, а передающий совершит передачу банкнот. В этом случае денежный модуль получателя записывает информацию о банкнотах, которые он должен был получить, и сообщает абоненту, что существует потенциальная проблема (т.е. что он не получил банкноты, посланные А). Необходимо отметить, что в этих условиях до тех пор, пока денежный модуль передающего задействован, он правильно передает банкноты.

Абонент денежного модуля получателя может затем подать требование о возмещении денег в сертификационное агентство. Требование будет содержать журнальную запись неудавшейся транзакции. Затем сертификационное агентство может проверить при помощи банков-эмитентов, были ли банкноты согласованы. Через некоторое время, если банкноты не были согласованы, абонент может заново востребовать свои деньги.

Платеж на месте продажи.

На фиг. 43 показан протокол платежа на месте продажи, или через кассовый терминал. Протокол платежа на месте продажи предназначен для упрощения платежей, совершаемых между денежным модулем 1186 транзакций покупателя и денежным модулем 1186 транзакций продавца. Денежный модуль 1186 транзакций продавца может быть, например, установлен в кассовом терминале супермаркета.

Сначала А дает согласие на приобретение товаров или услуг у В (шаг 1760). Владелец/держатель денежного модуля А транзакций подсоединяется к денежному модулю (шаг 1762). Функция "Связь с абонентом А" запрашивает у владельца/пользователя транзакцию, а А выбирает выполнение платежа на месте продажи (шаги 1764-1766). В то же время продавец определяет общую цену покупки (шаг 1768). Функция "Связь с абонентом В" запрашивает транзакцию, а В выбирает получение платежа на месте продажи (шаги 1770-1772). Затем А и В устанавливают безопасный сеанс связи (шаги 1774-1776).

Функция "Связь с абонентом В" сообщает сумму платежа, а функция "Платеж/обмен В" принимает сумму и посылает ее к А (шаги 1778-1782). Затем функция "Связь с абонентом А" посылает запрос своему абоненту проверить требуемую сумму (шаги 1784-1786). Более того, абонента просят выбрать банкноты, которыми он будет платить (например, наличными или в кредит) и их количество, чтобы итог равнялся требуемой сумме. Если требуемая сумма неправильная, то функция "Платеж/обмен А" посылает В сообщение, указывающее на то, что требуемая сумма неправильная (шаги 1788-1790). Затем функция "Связь с абонен-

том В" приглашает ввести своего владельца новую сумму (шаги 1792-1794). Если новая сумма не выбрана, то транзакция прекращается (шаг 1796).

Если требуемая сумма правильная, то функция "Платеж/обмен А" принимает суммы в зависимости от типов банкнот (шаг 1798). Затем функция "Каталог банкнот А" проверяет наличие достаточных средств (шаги 1800-1802). Если средств недостаточно, то функция "Связь с абонентом А" запрашивает новые суммы, выраженные типом банкнот (шаги 1804-1806). Если новая сумма не задана, то функция "Платеж/обмен А" посылает к В сообщение, что средств А недостаточно (шаги 1808, 1790). Функция "Связь с абонентом В" приглашает своего владельца ввести новую сумму (шаги 1792-1794). Если новая сумма не выбрана, то транзакция прекращается (шаги 1796). Если же новая сумма выбрана, то транзакция платежа начинается снова.

Если средств достаточно, то функция "Платеж/обмен А" передает сумму держателю денег (шаг 1810). Затем банкноты передаются от А к В (шаг 1812). В завершение денежные модули транзакций фиксируют транзакцию (шаг 1814).

Таким образом, платеж на месте продажи упрощен для покупателя, поскольку представляет собой платеж, инициализируемый получателем платежа.

Связывание счетов.

На фиг. 44 показан протокол связывания счетов путем создания или обновления профилей счетов. Покупатель сможет связать свой денежный модуль транзакций со своим счетом в банке с помощью протокола связывания счетов (денежный модуль 1188 банковского кассира в корреспондентском банке также может быть связан с банковскими счетами в банке-эмитенте). Профиль счетов хранится денежным модулем 1186 транзакций (либо денежным модулем 1188 банковского кассира) для доступа к каждому из связанных счетов. Этот профиль будет подписан банковским сервером 1184 безопасности. Банку не требуется поддерживать список доступа для каждого клиента, поскольку этот банк может проверять цифровую подпись клиента, когда денежный модуль клиента предъявляет профиль счета. Это должно повысить безопасность по сравнению с существующими в настоящее время методами доступа через банковский автомат (банкомат) или с помощью кредитных карт.

Модули 1192 обслуживания клиентов представляют собой защищенные от несанкционированного доступа устройства, используемые для создания и обновления профилей счетов. Модуль 1192 обслуживания клиентов содержит уникальный сертификат, аналогичный сертификатам, находящимся в денежных модулях и серверах безопасности. Модуль обслуживания клиентов может устанавливать безопасный сеанс связи с другими модулями (например, с серверами безопасности).

Для связывания счетов владелец денежного модуля 1186 транзакций лично приходит в свой банк и подсоединяет свой денежный модуль к банковской сети 1200. Как показано на фиг. 44, денежный модуль выбирает доступ к банку для связывания счетов (шаг 1816). Затем денежный мо-

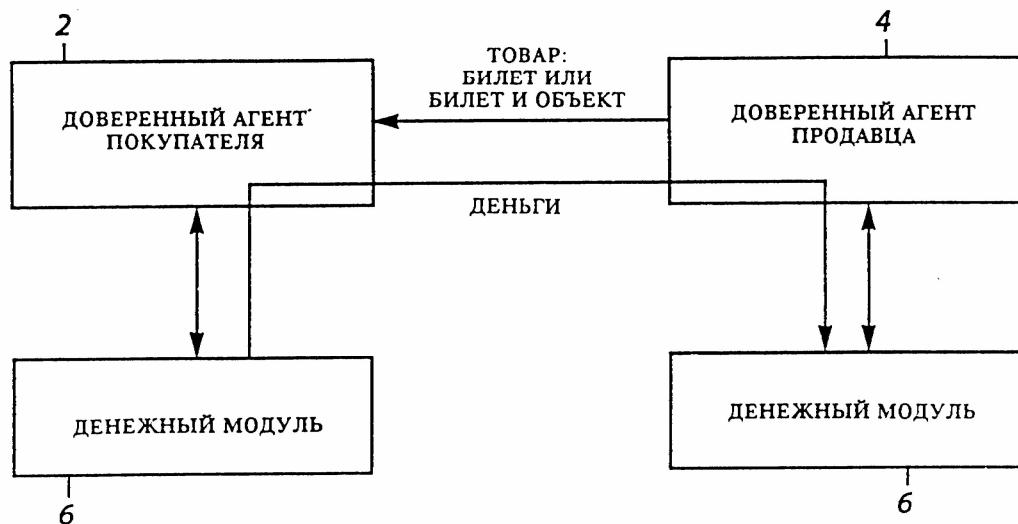
дуль 1186 устанавливает безопасный сеанс связи с сервером 1184 безопасности (шаг 1818). После этого денежный модуль 1186 посылает запрос на связывание счетов вместе со своим текущим банковским профилем (если такой существует) серверу безопасности (шаг 1820). Сервер безопасности принимает запрос на связывание (и банковский профиль) (шаг 1822). Сервер безопасности устанавливает сеанс связи с модулем 1192 обслуживания клиентов (шаг 1824). Затем сервер безопасности посылает запрос на связывание (и банковский профиль) модулю обслуживания клиентов (шаг 1826).

После этого владелец денежного модуля транзакций предъявляет свои идентификационные документы представителю клиентской службы банка (шаг 1828). Представитель клиентской службы банка вводит имя клиента, а модуль обслуживания клиентов вызывает список счетов клиента (шаг 1830). Затем владелец денежного модуля выбирает счета, которые будут связаны для доступа к ним денежного модуля (шаг 1832). Модуль обслуживания клиентов отмечает счета, которые будут связаны (шаг 1834). Владелец денежного модуля и представитель клиентской службы после

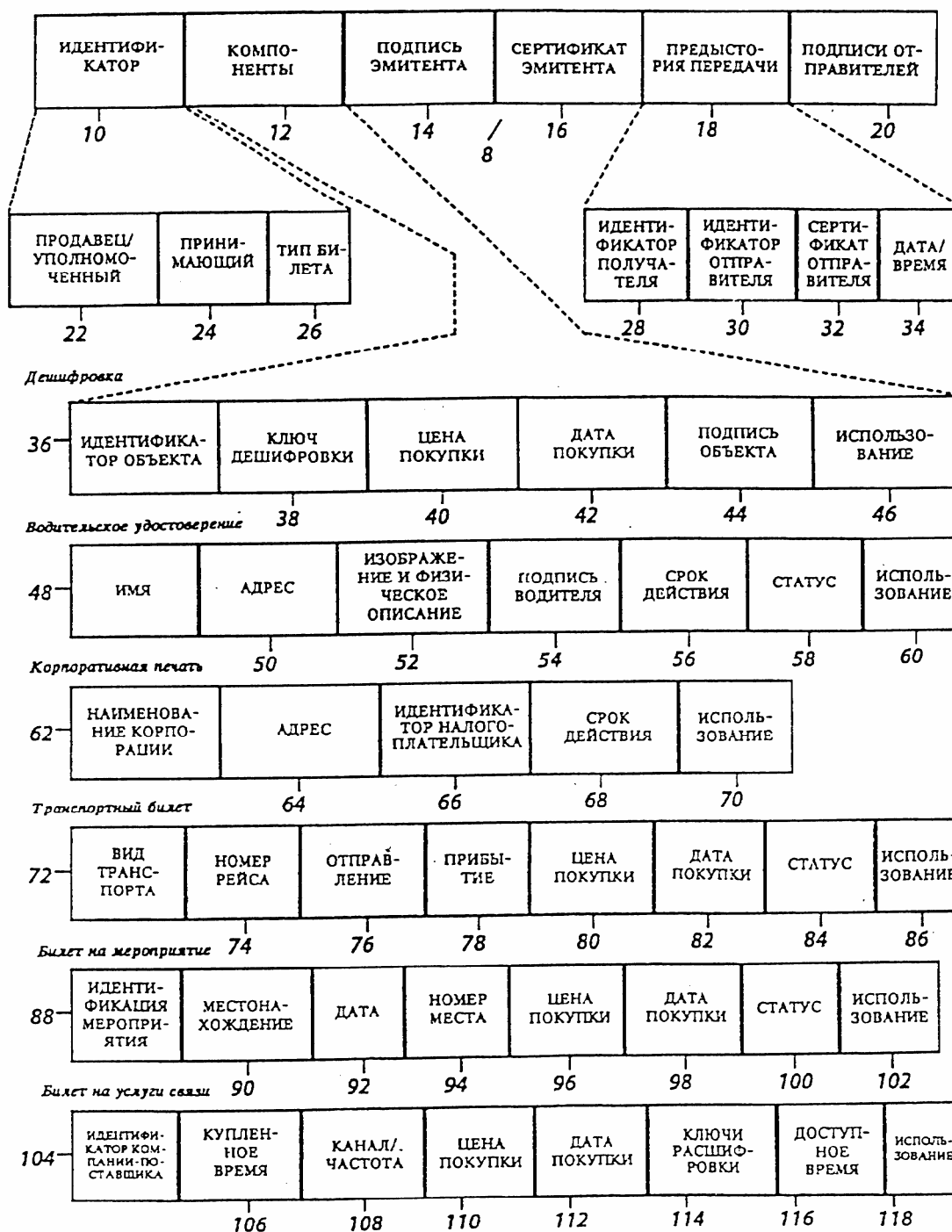
этого проверяют связи счетов (шаги 1836-1838). Если связи неправильные, то сеанс связи модуля обслуживания клиентов (МОК) с сервером безопасности и сеанс связи сервера безопасности с денежным модулем прекращаются (шаги 1840-1842).

Если связи счетов правильные, то модуль 1192 обслуживания клиентов посылает профиль счетов серверу 1184 безопасности (шаг 1844). Сервер 1184 безопасности в цифровом виде подписывает новый (или обновленный) профиль (шаг 1846). Сервер 1184 безопасности затем посылает подписанный профиль денежному модулю 1186 (шаг 1848). В заключение фиксируются транзакция денежного модуля с сервером безопасности (шаг 1850) и транзакция сервера безопасности с модулем обслуживания клиентов (шаг 1852).

В настоящем описании представлены и описаны предпочтительные варианты выполнения настоящего изобретения; при этом предполагается, что настоящее изобретение может использоваться в других различных комбинациях и условиях и в него можно вносить различные изменения и модификации, не выходящие за его объем.

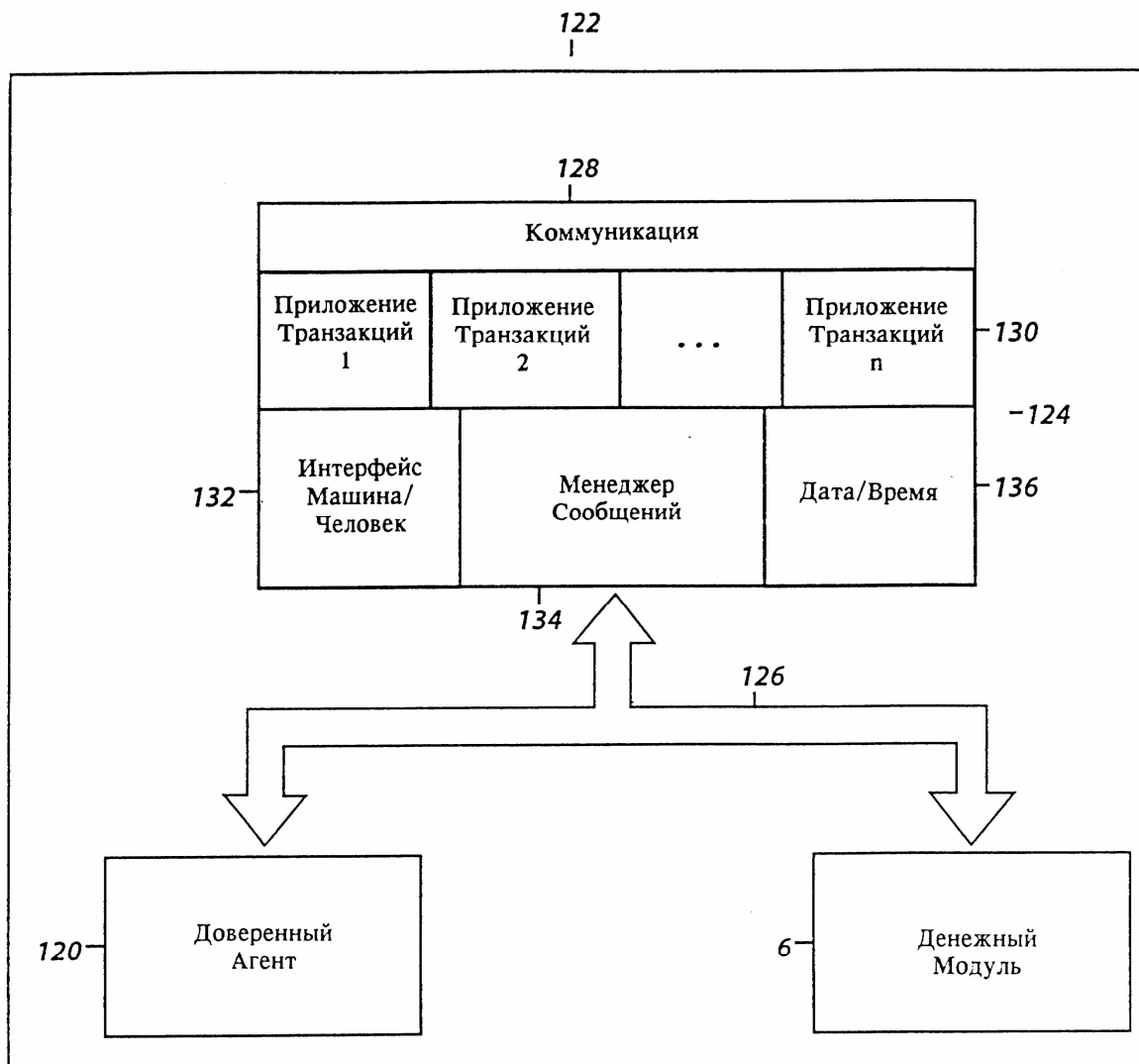


Фиг. 1

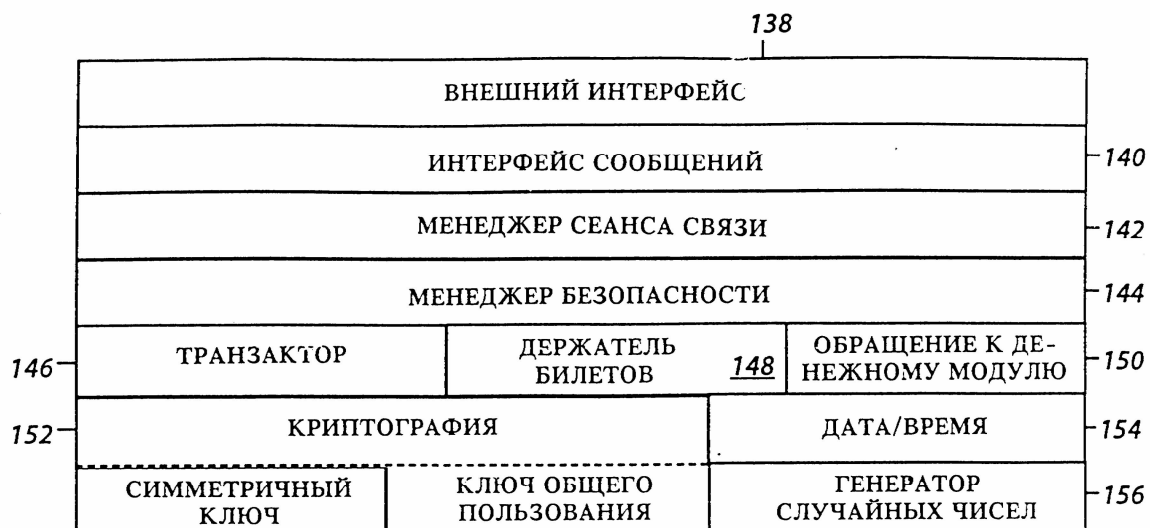


Фиг. 2

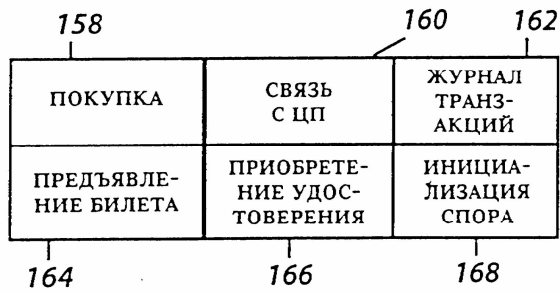




Фиг. 3



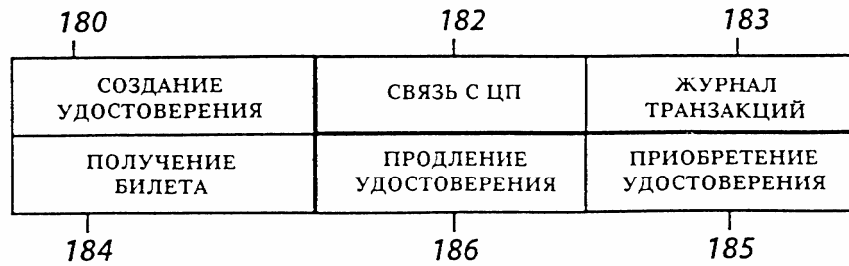
Фиг. 4А



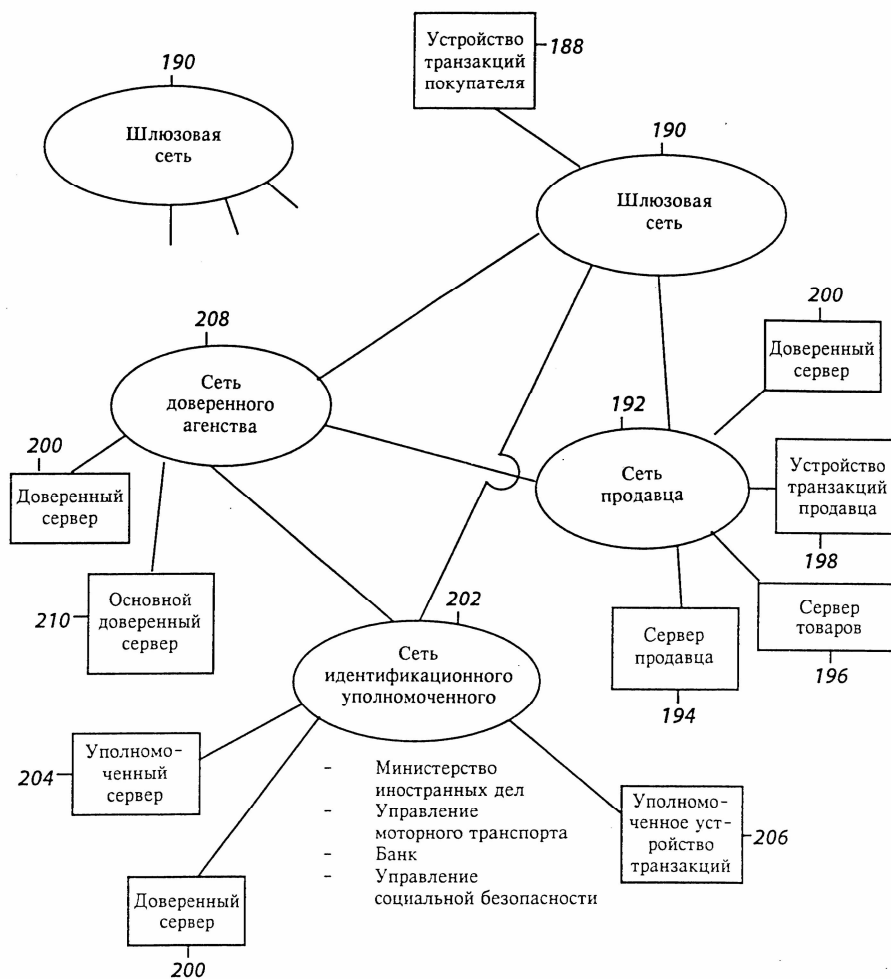
Фиг. 4Б



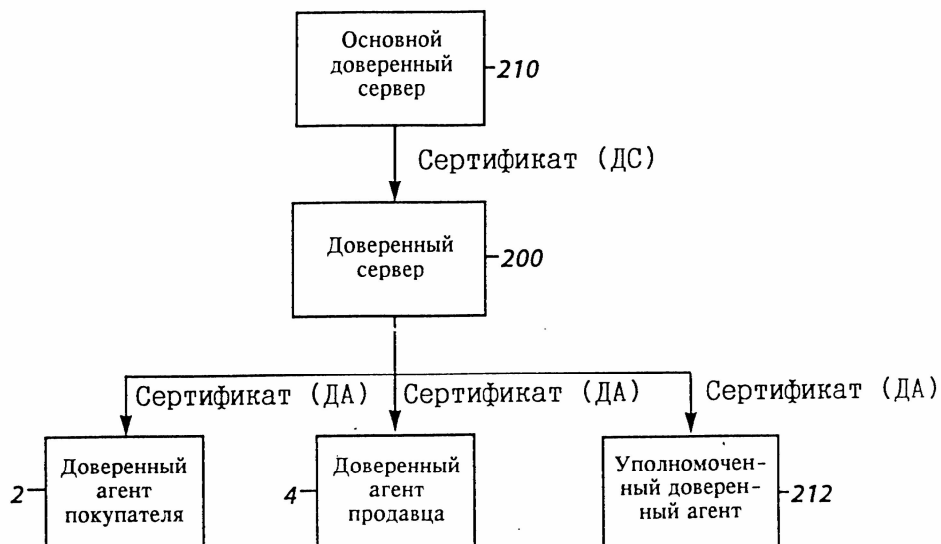
Фиг. 4В



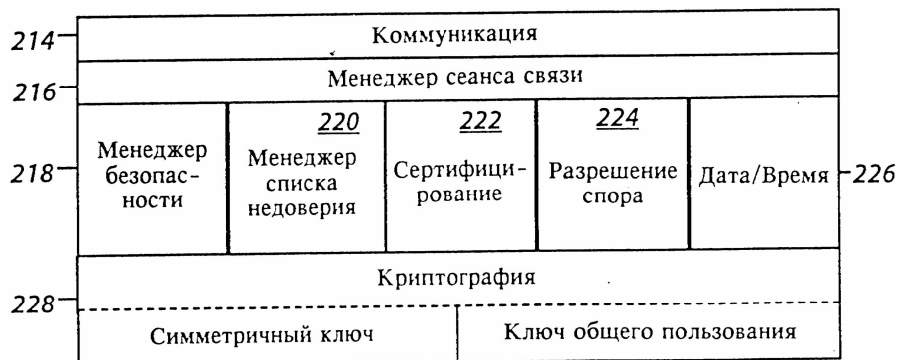
Фиг. 4Г



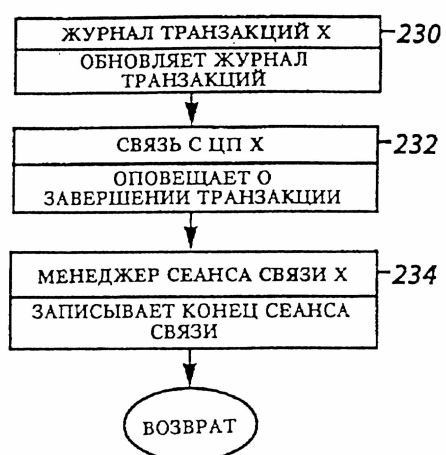
Фиг. 5



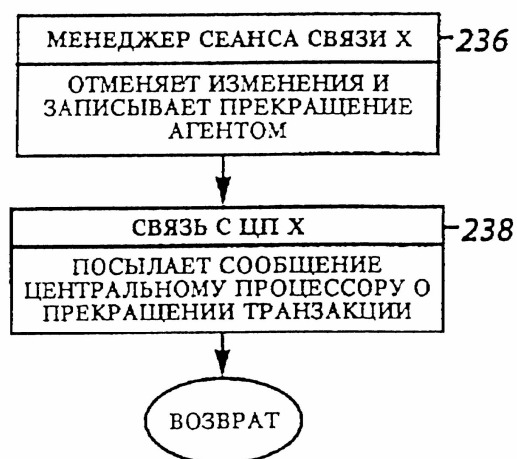
Фиг. 6А



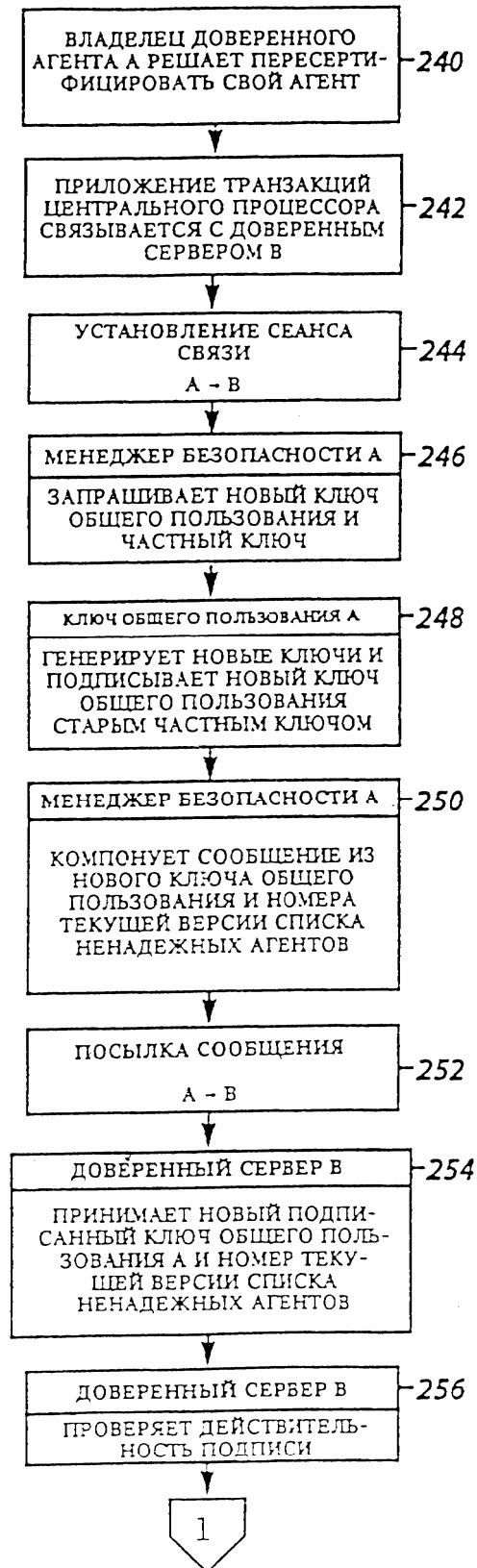
Фиг. 6Б



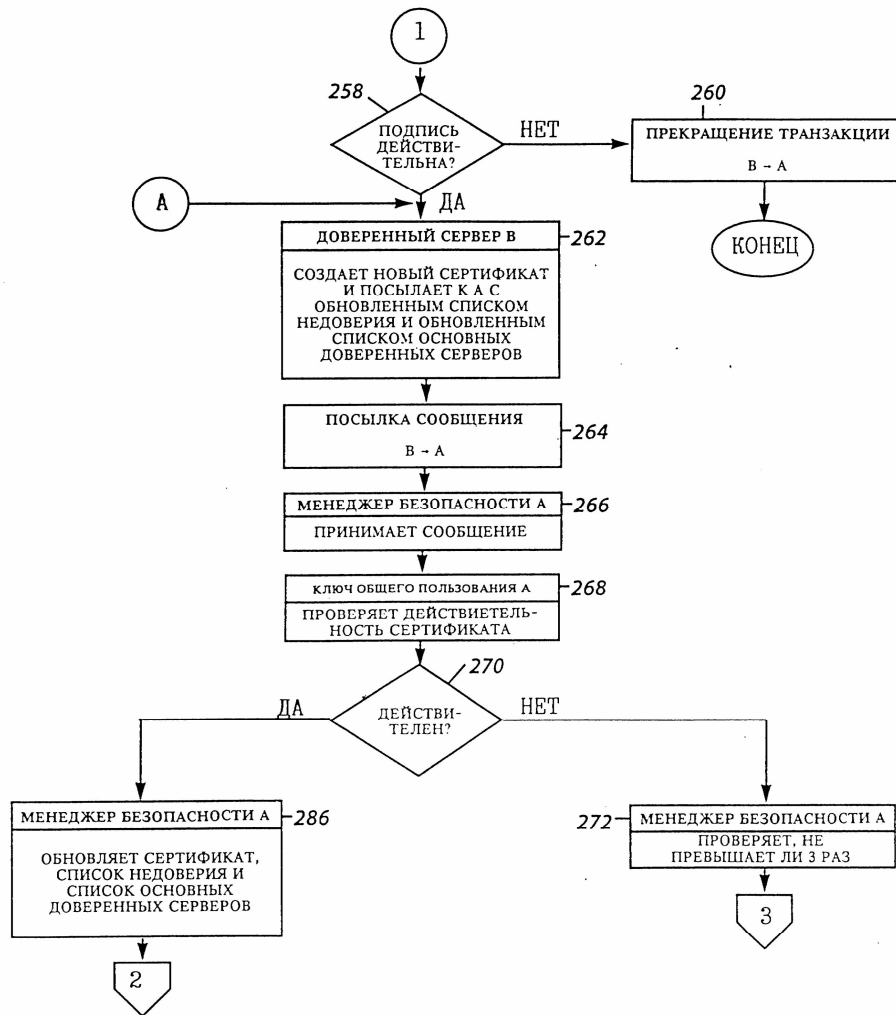
Фиг. 7А



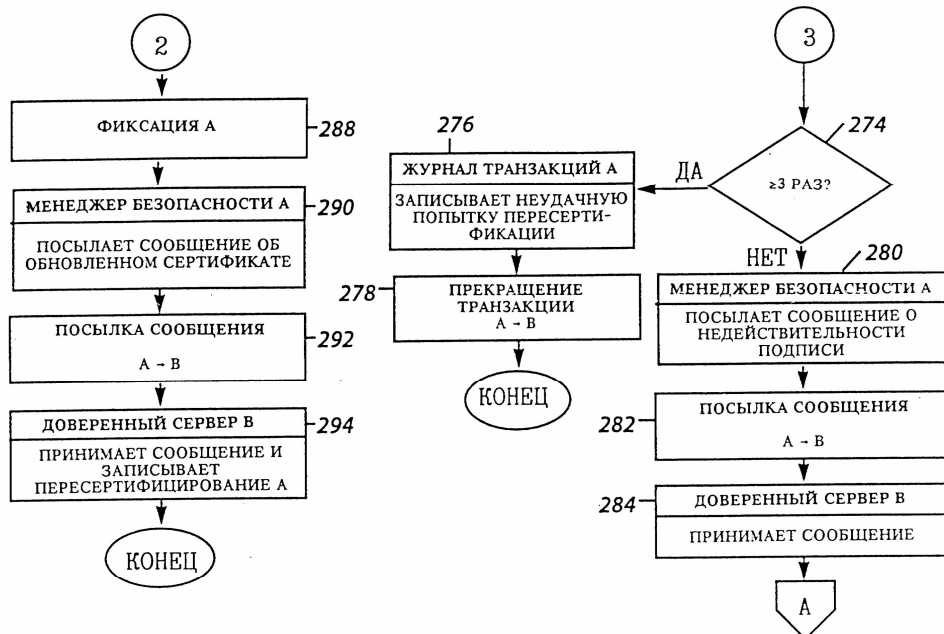
Фиг. 7Б



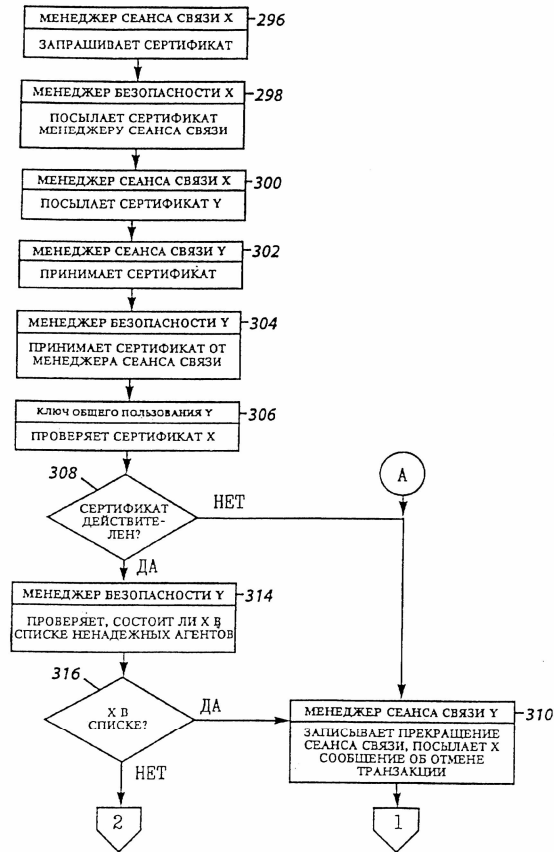
Фиг. 8А



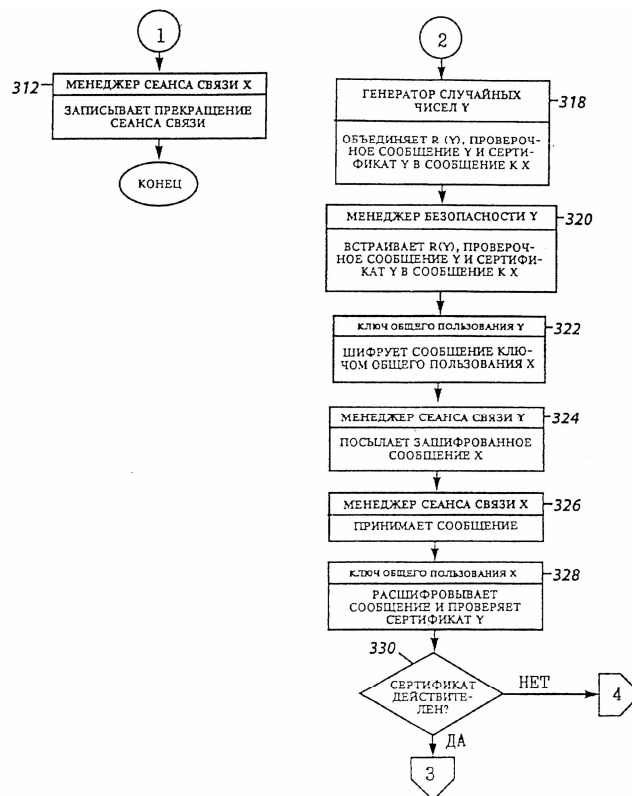
Фиг. 8Б



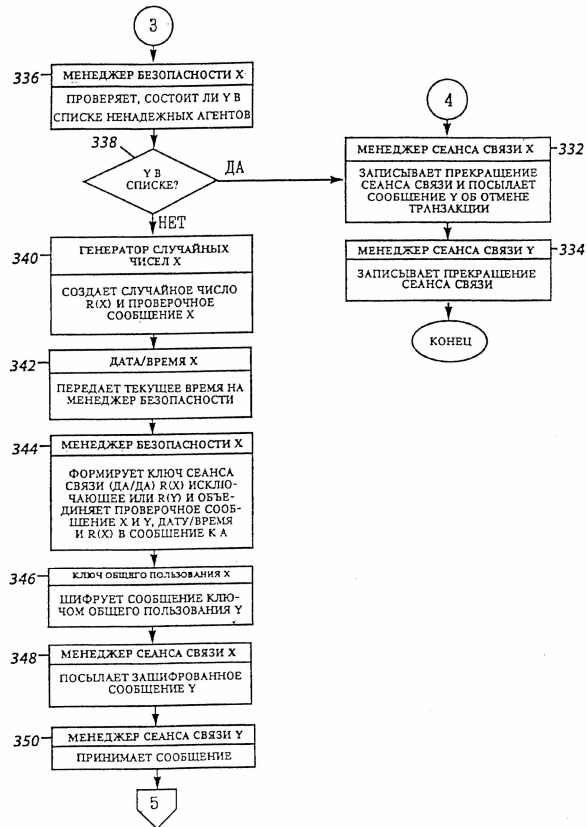
Фиг. 8В



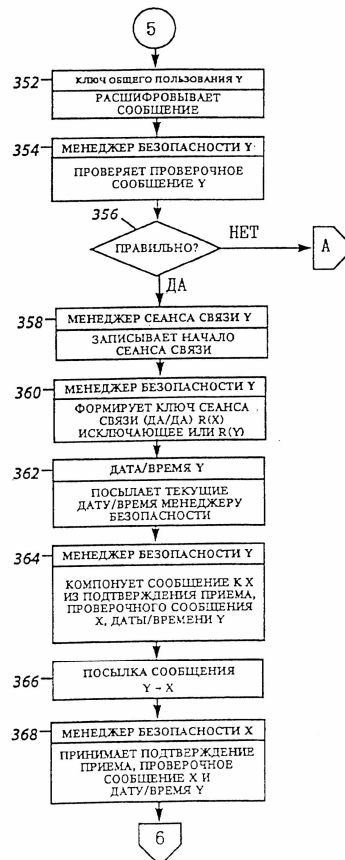
Фиг. 9А



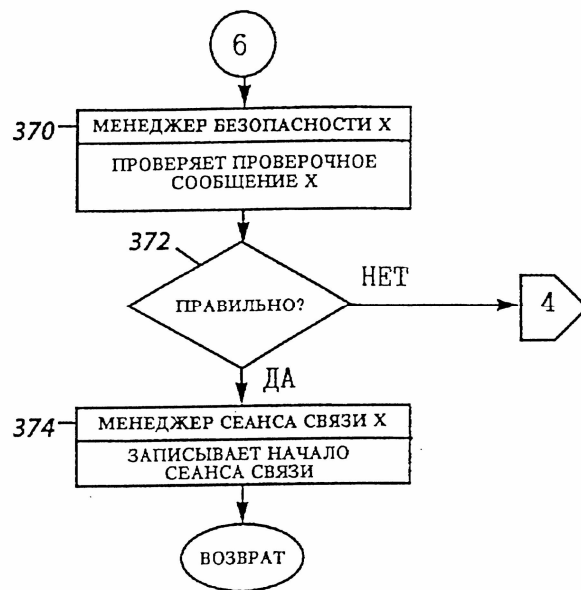
Фиг. 9Б



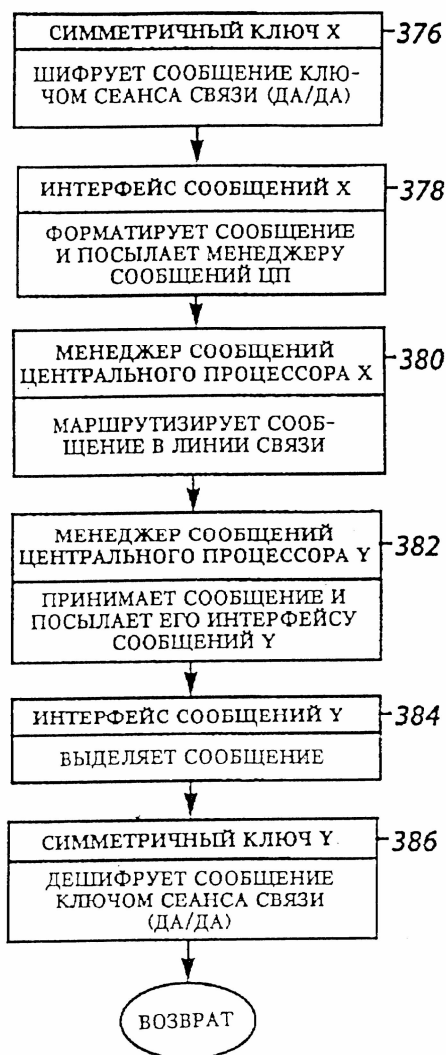
Фиг. 9В



Фиг. 9Г

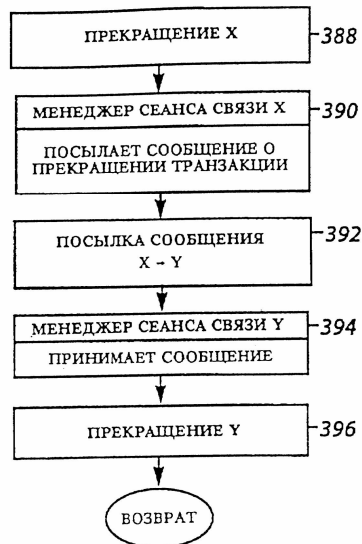


Фиг. 9Д

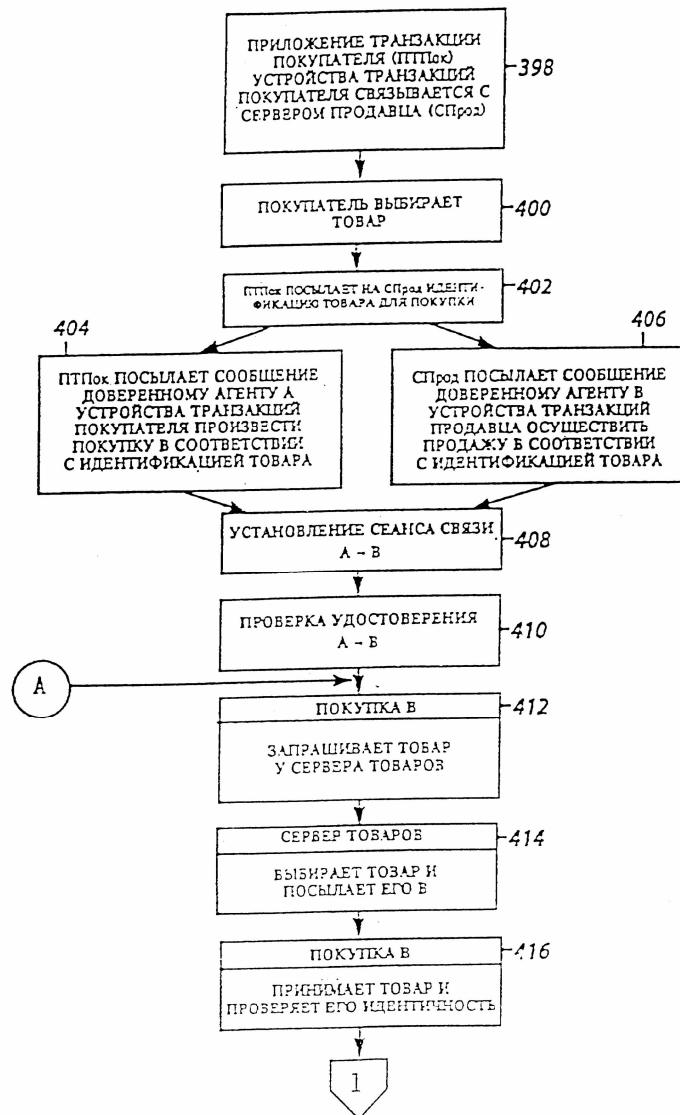


Фиг. 10

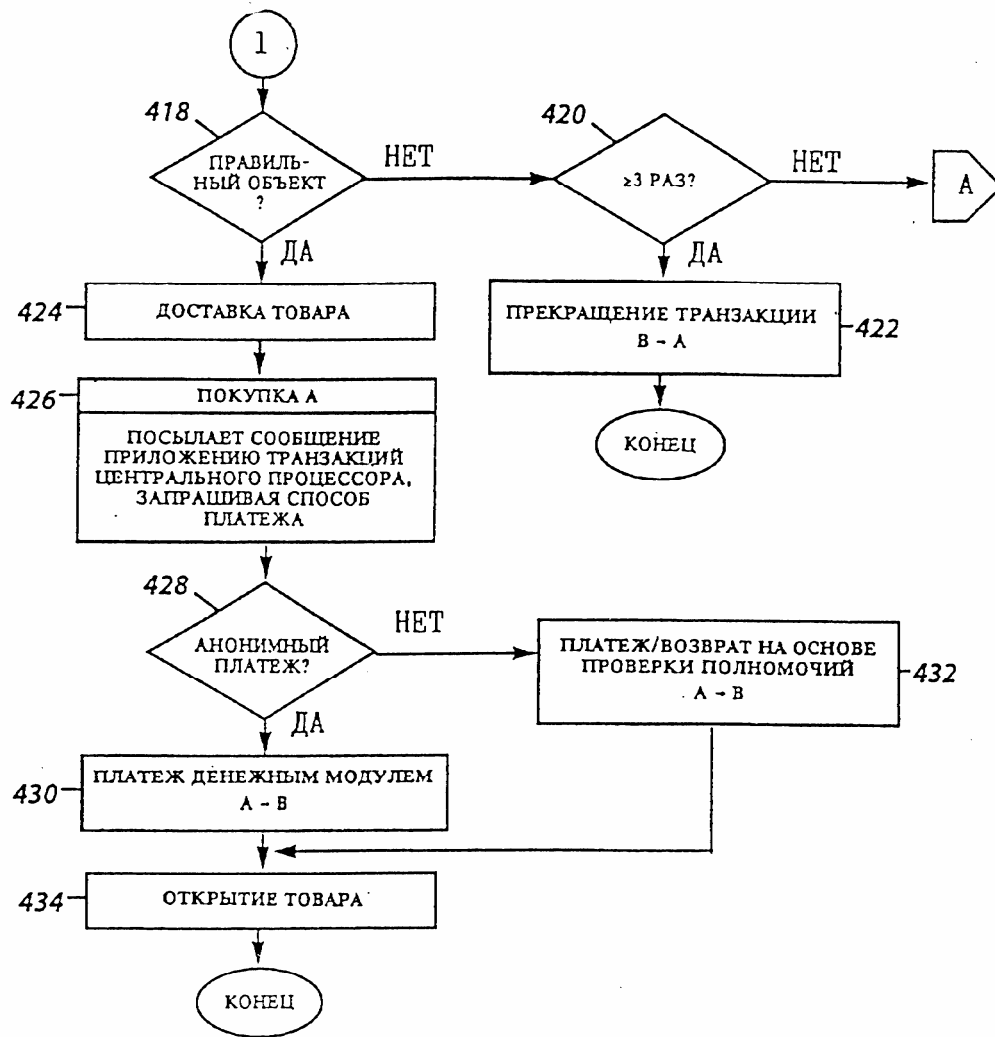




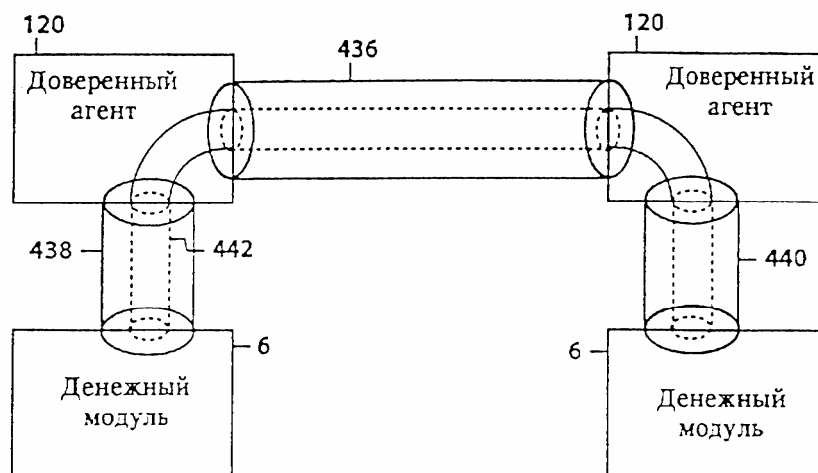
Фиг. 11



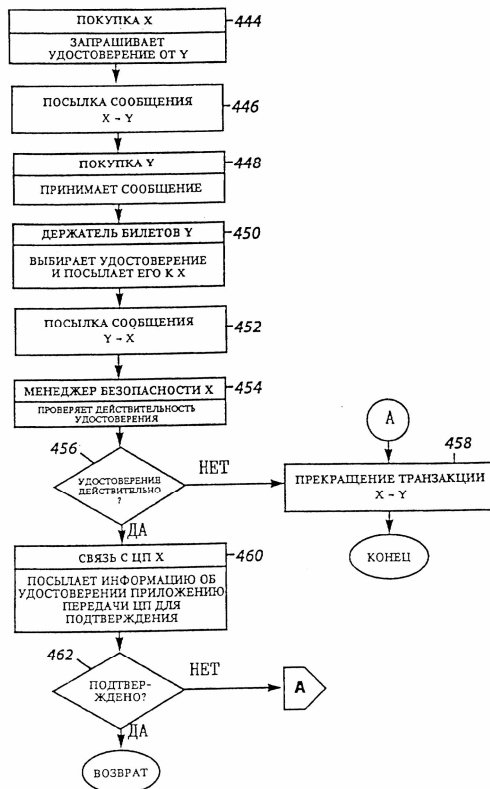
Фиг. 12А



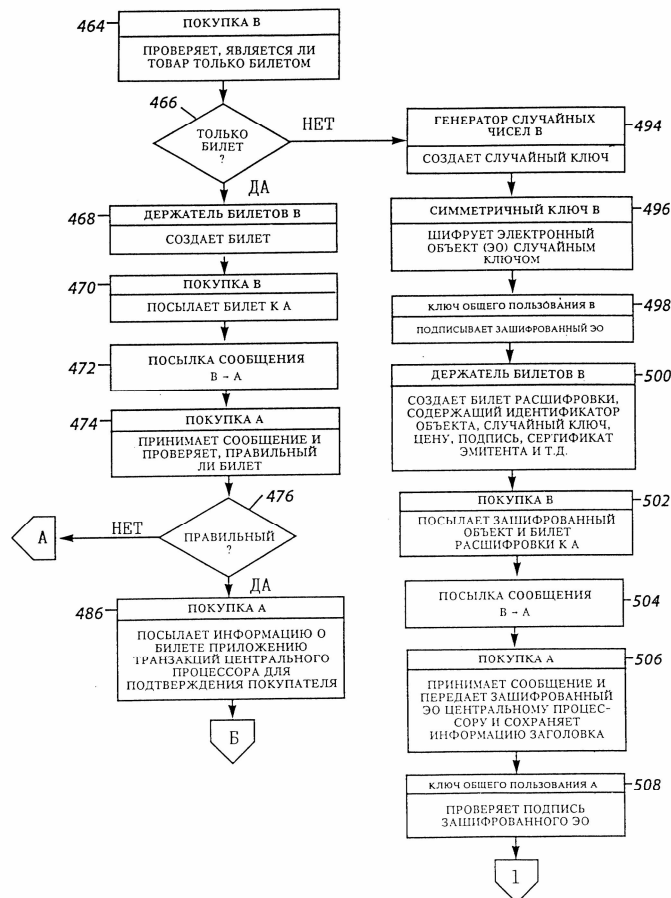
Фиг. 12Б



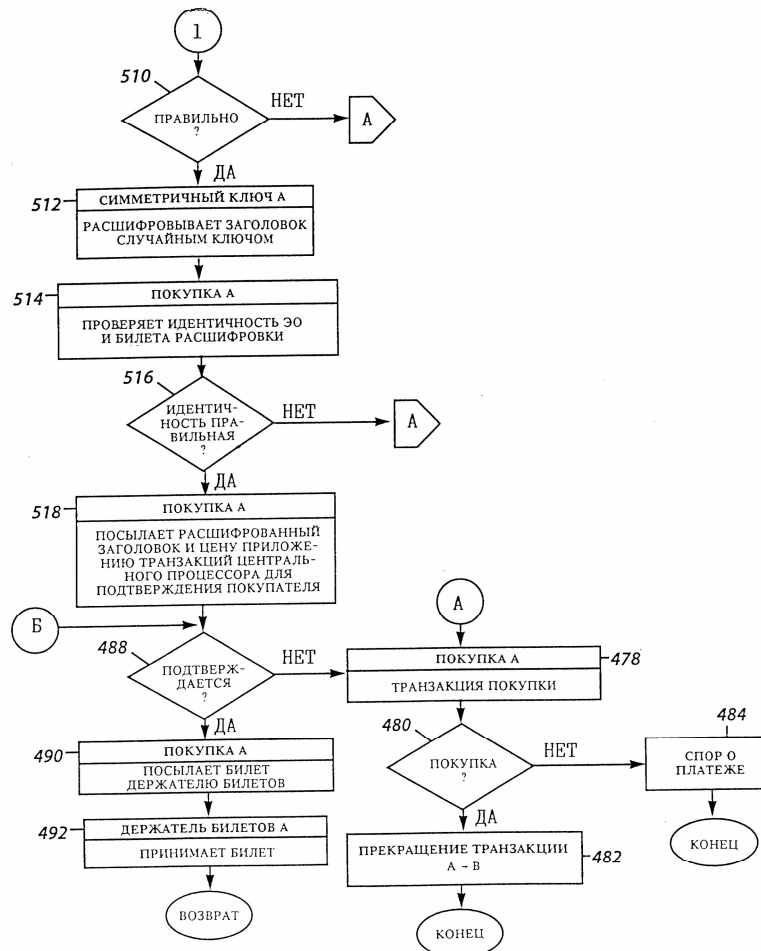
Фиг. 13



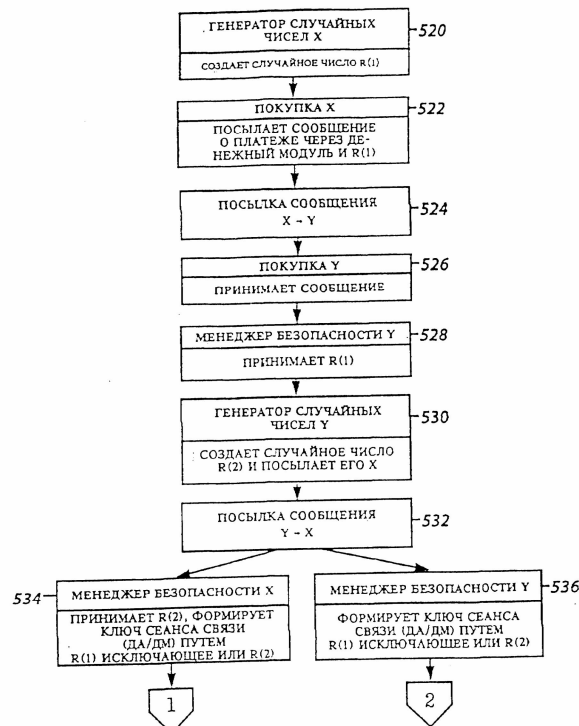
Фиг. 14



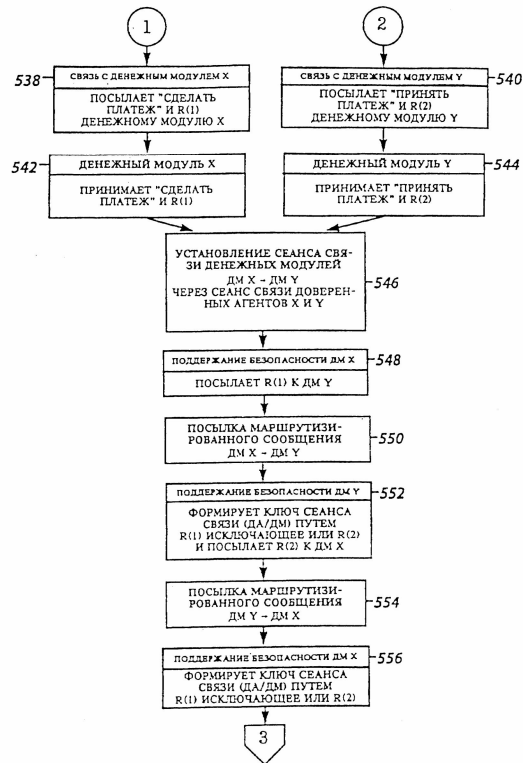
Фиг. 15А



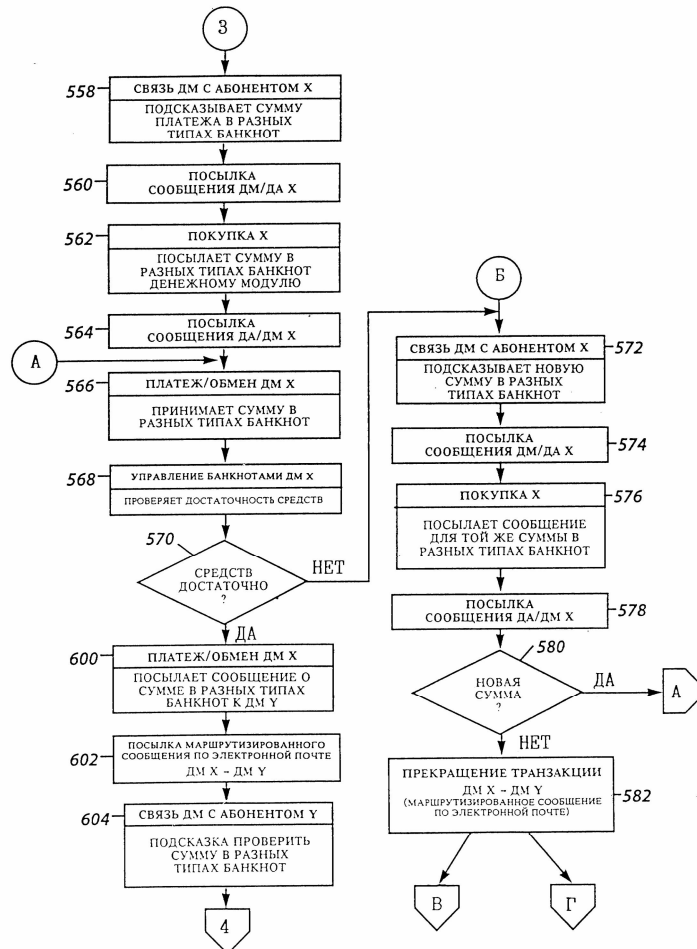
Фиг. 15Б



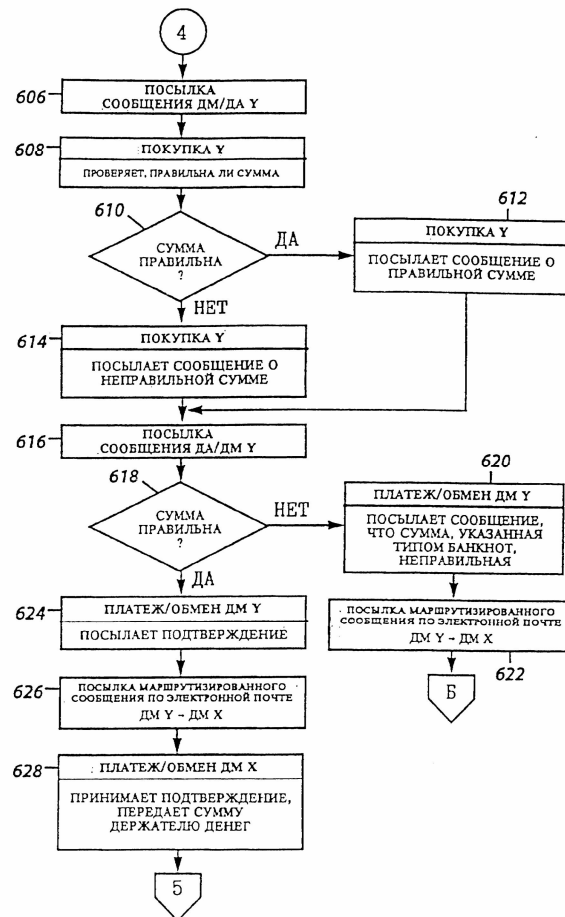
Фиг. 16А



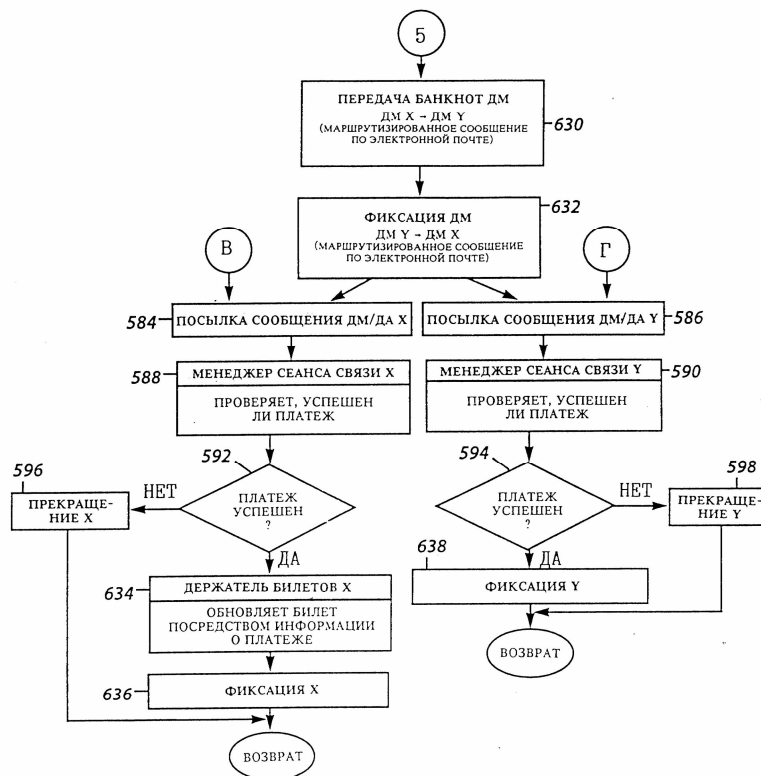
Фиг. 16Б



Фиг. 16В



Фиг. 16Г



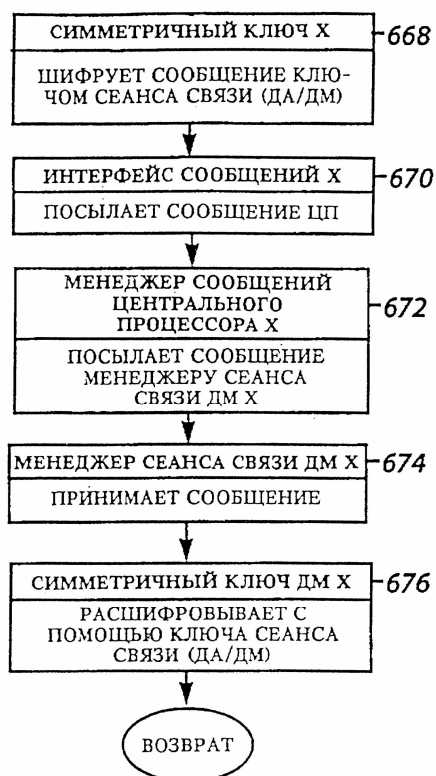
Фиг. 16Д



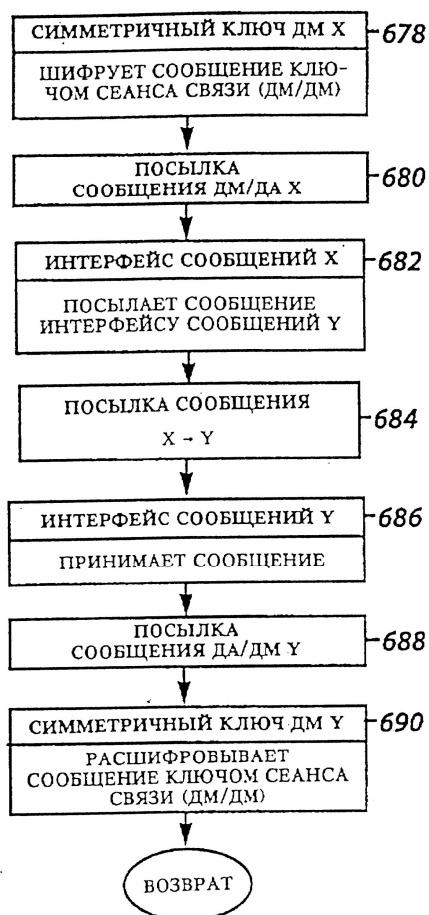
Фиг. 17



Фиг. 18

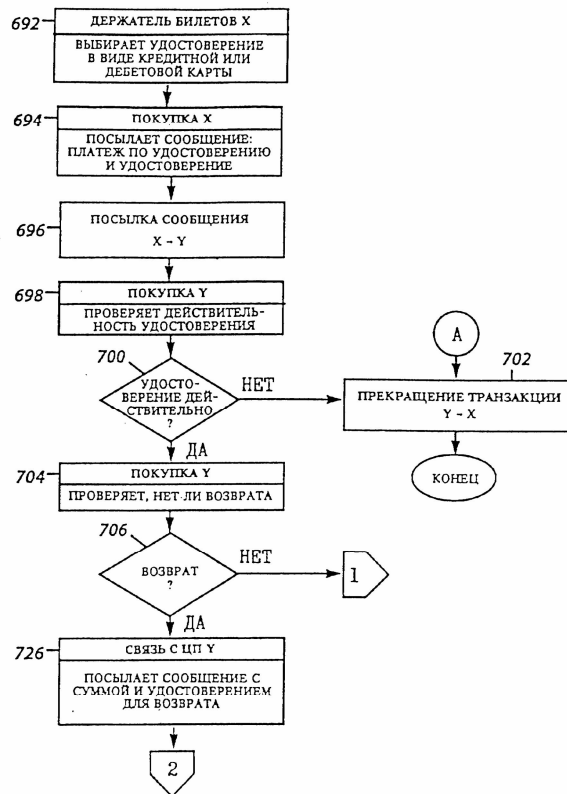


Фиг. 19

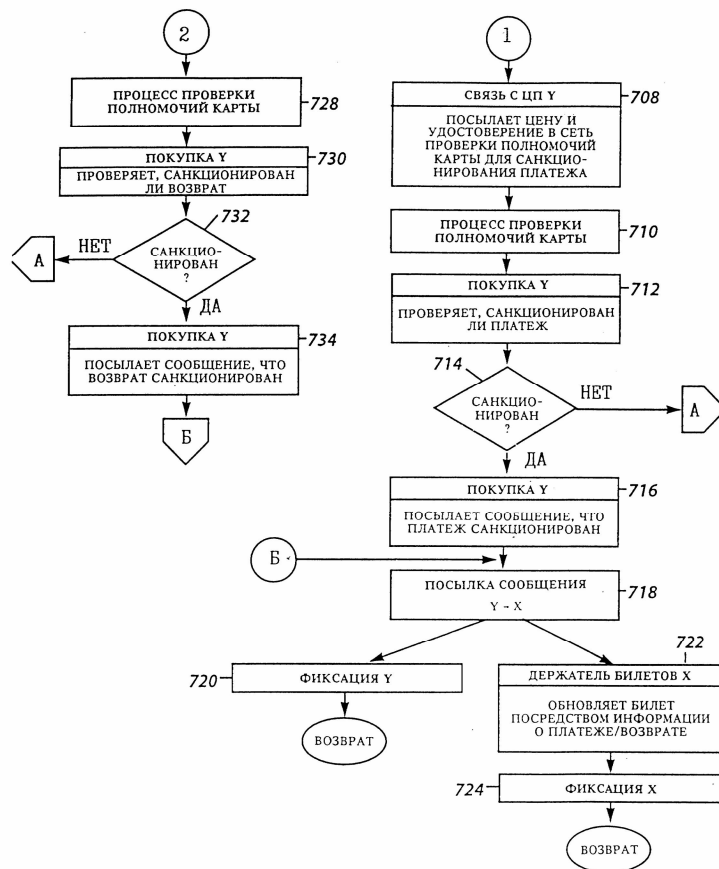


Фиг. 20

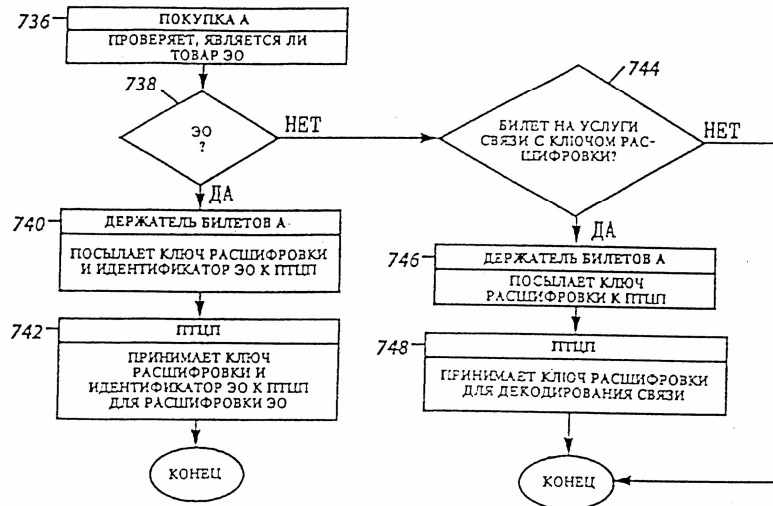




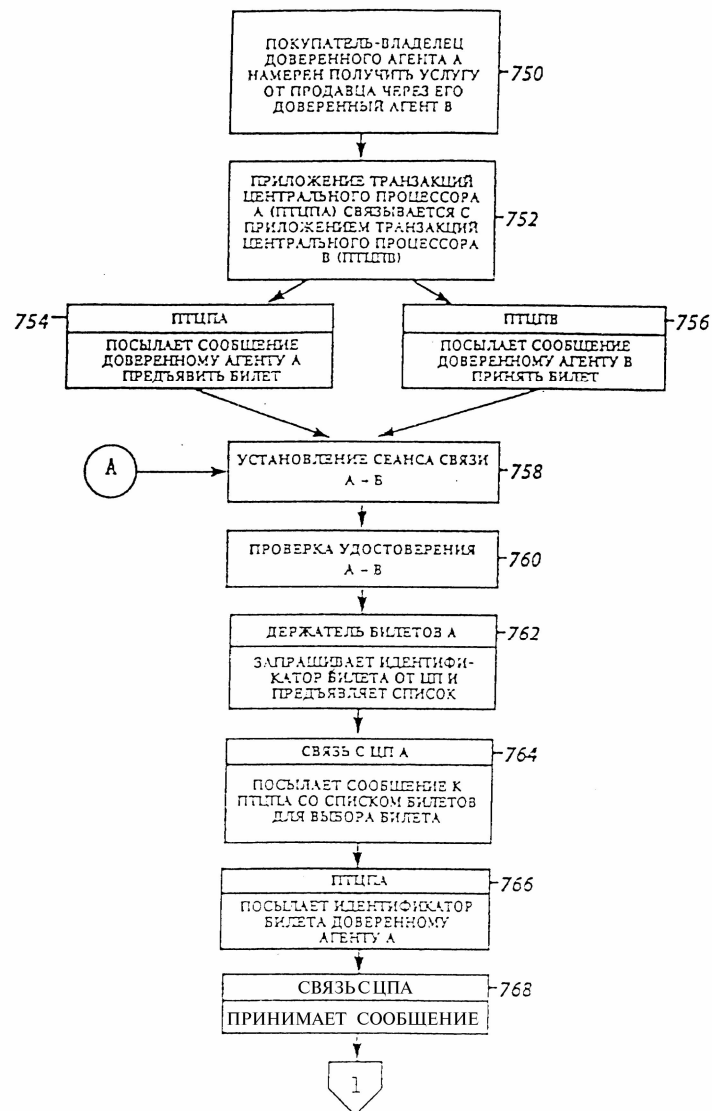
Фиг. 21А



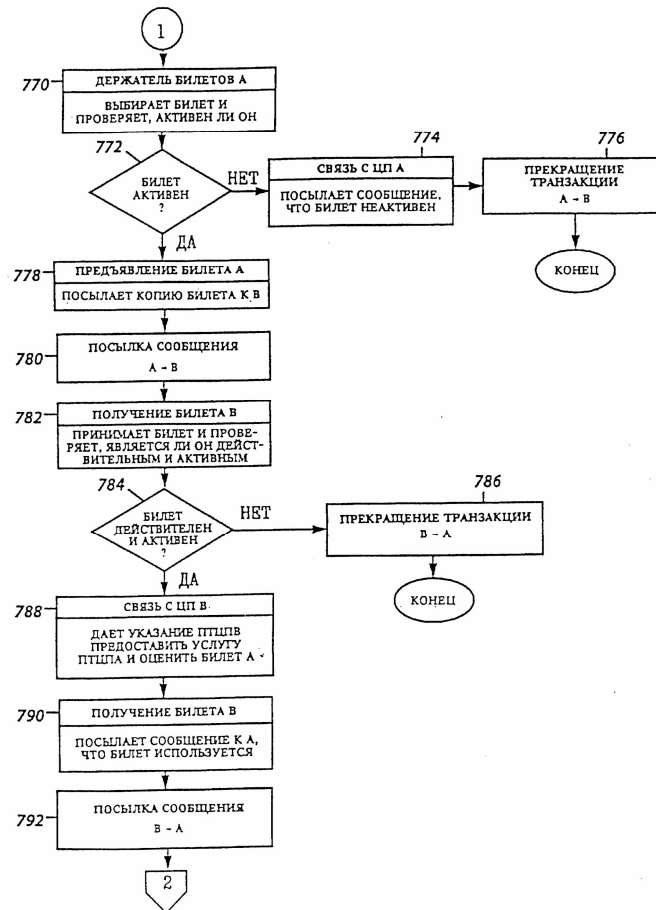
Фиг. 21Б



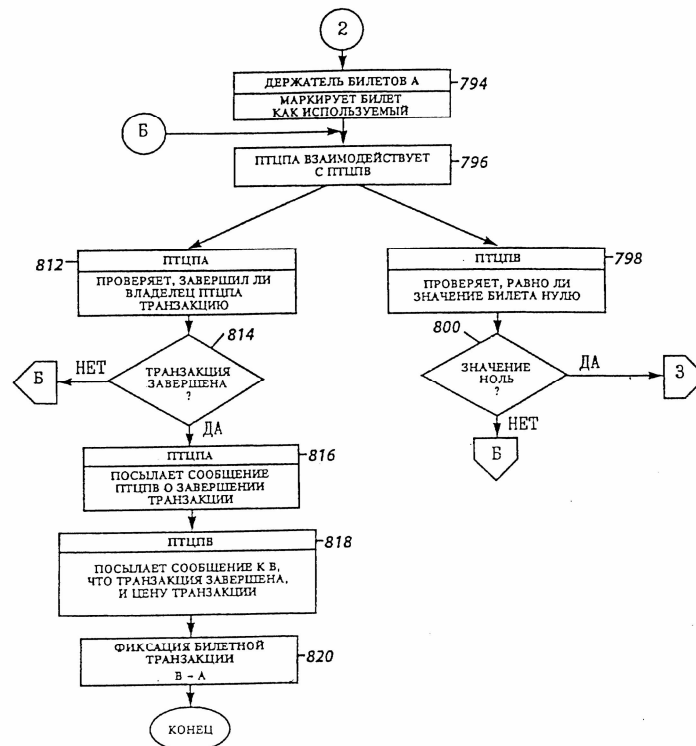
Фиг. 22



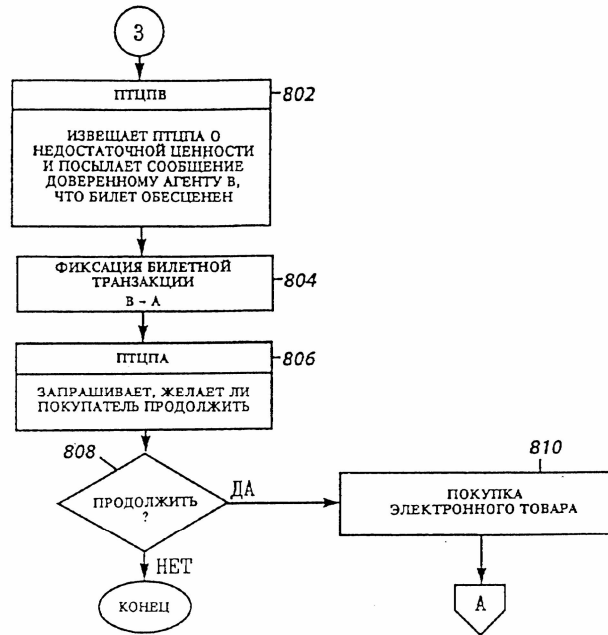
Фиг. 23А



Фиг. 23Б



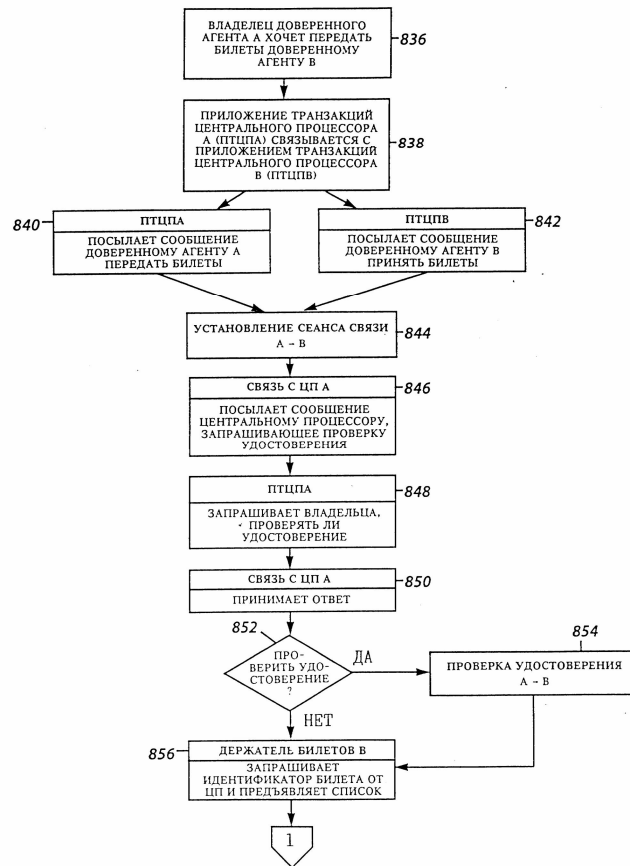
Фиг. 23В



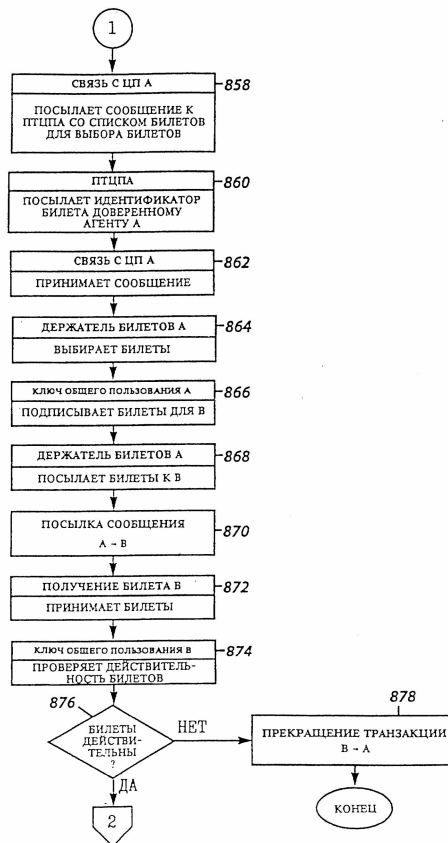
Фиг. 23Г



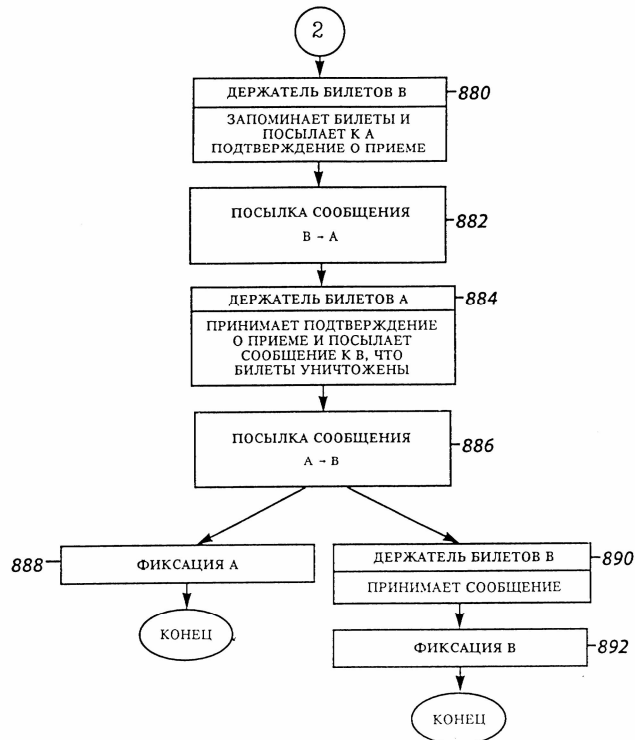
Фиг. 24



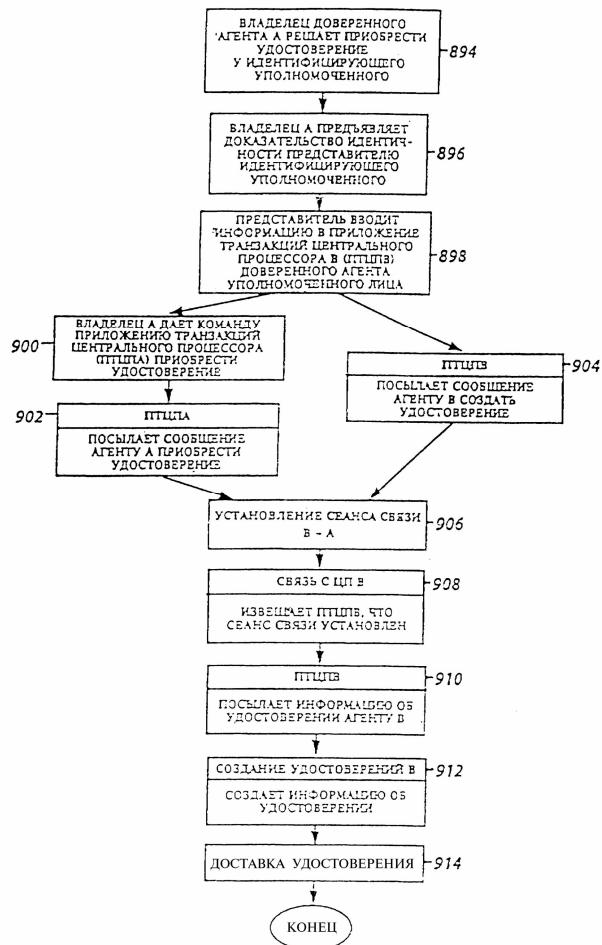
Фиг. 25А



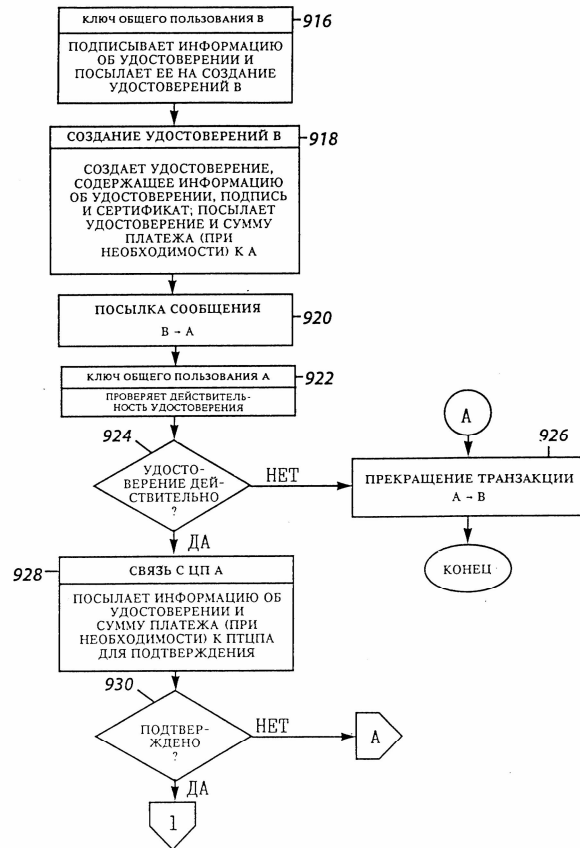
Фиг. 25Б



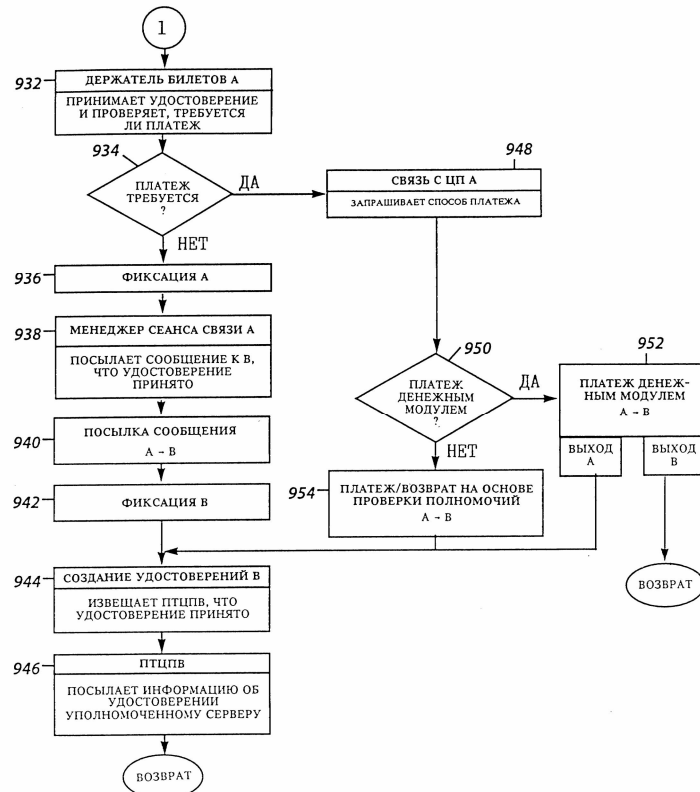
Фиг. 25В



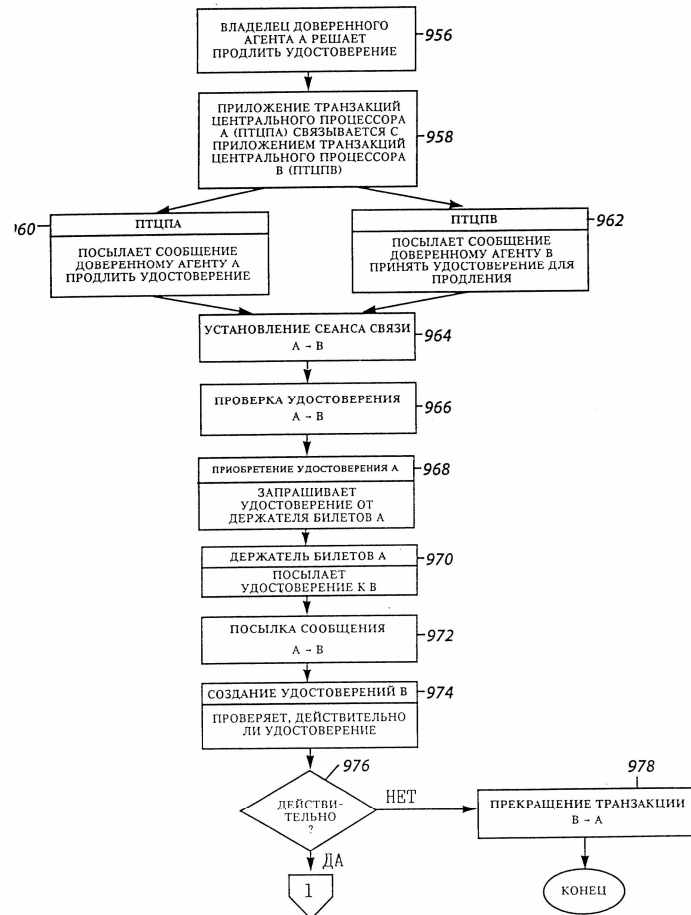
Фиг. 26



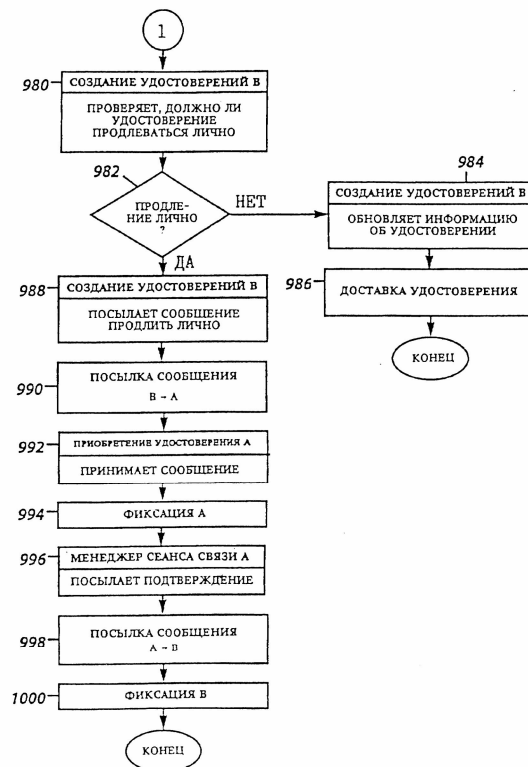
Фиг. 27А



Фиг. 27Б

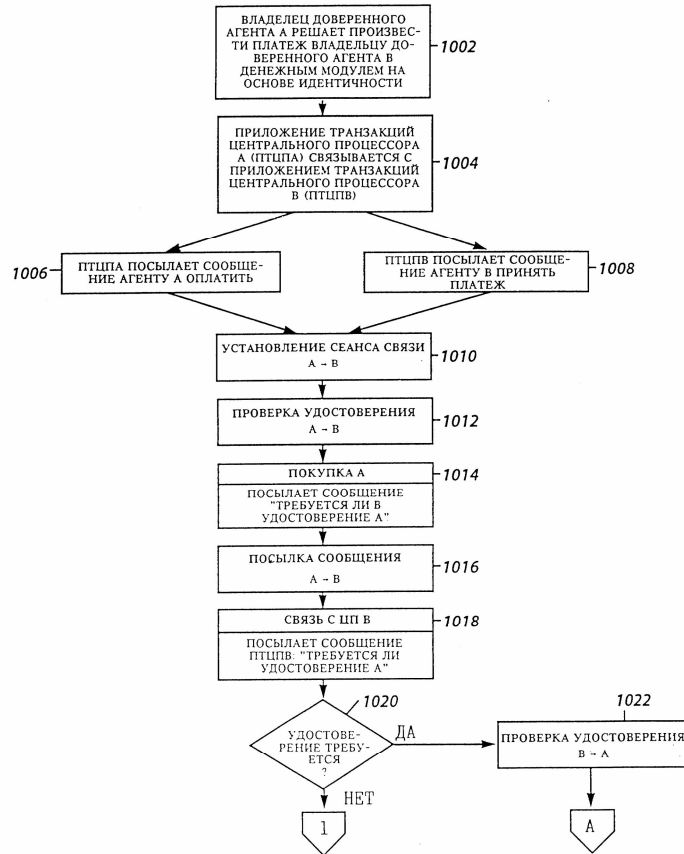


Фиг. 28А

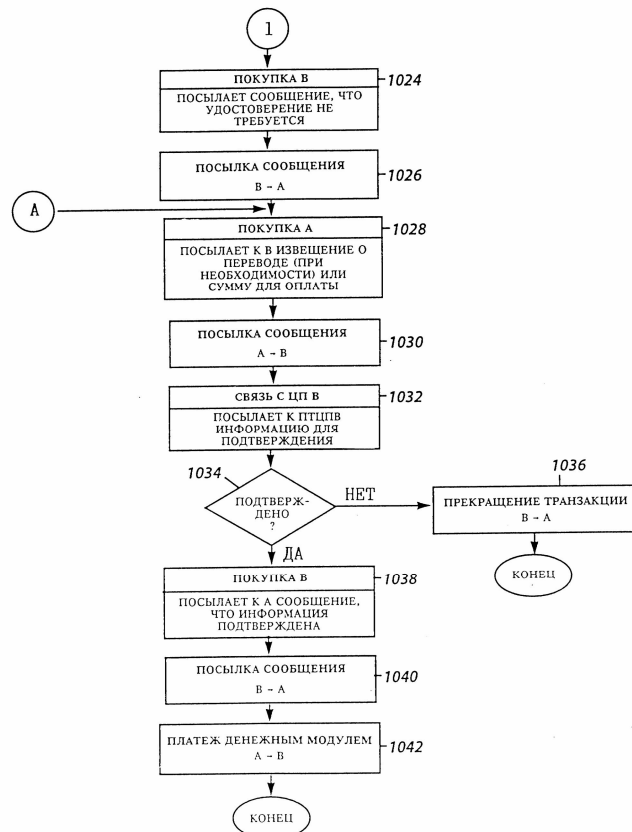


Фиг. 28Б

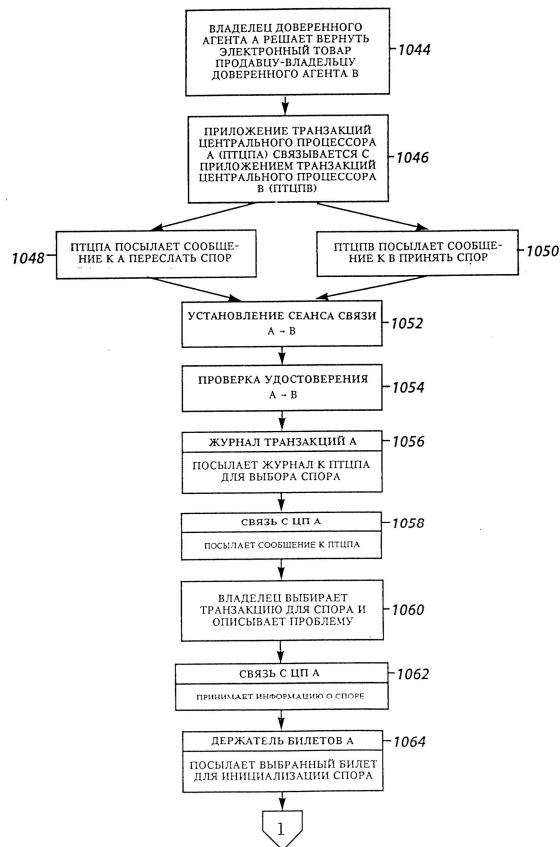




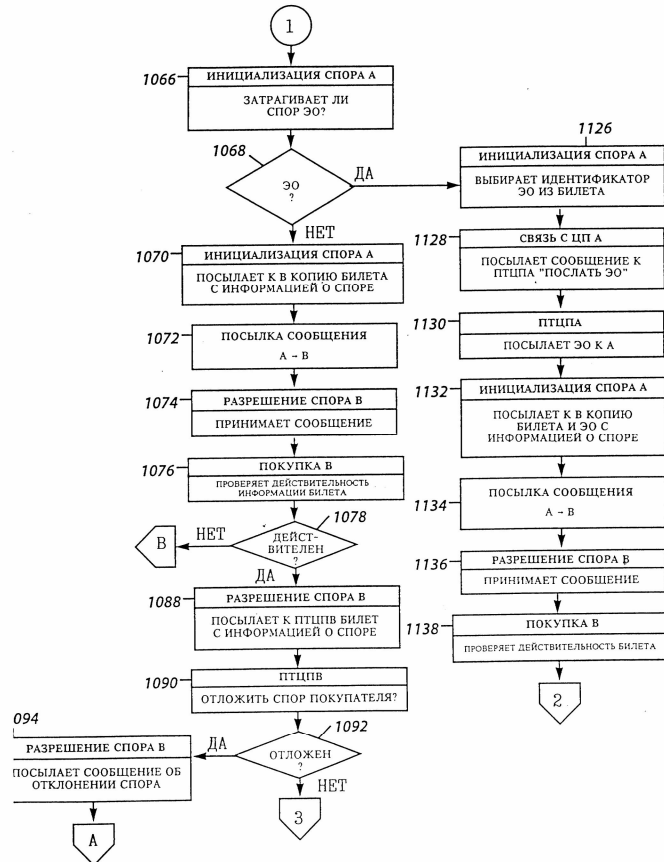
Фиг. 29А



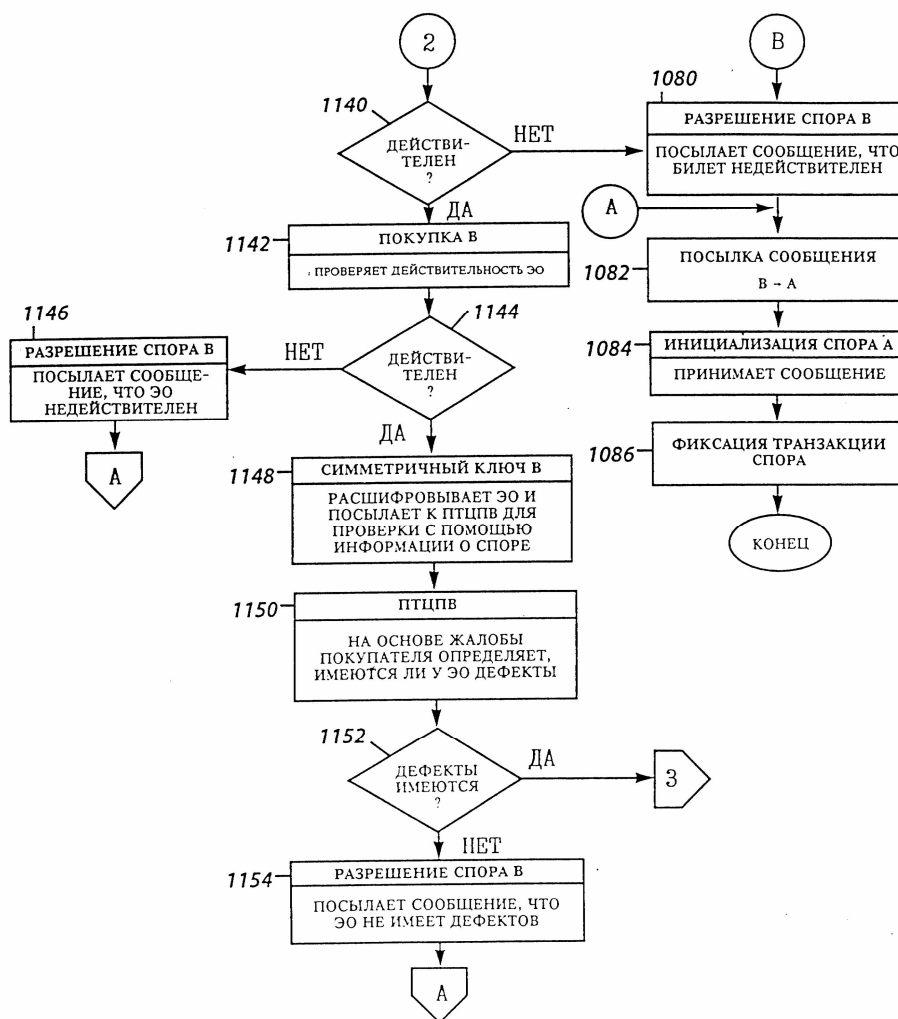
Фиг. 29Б



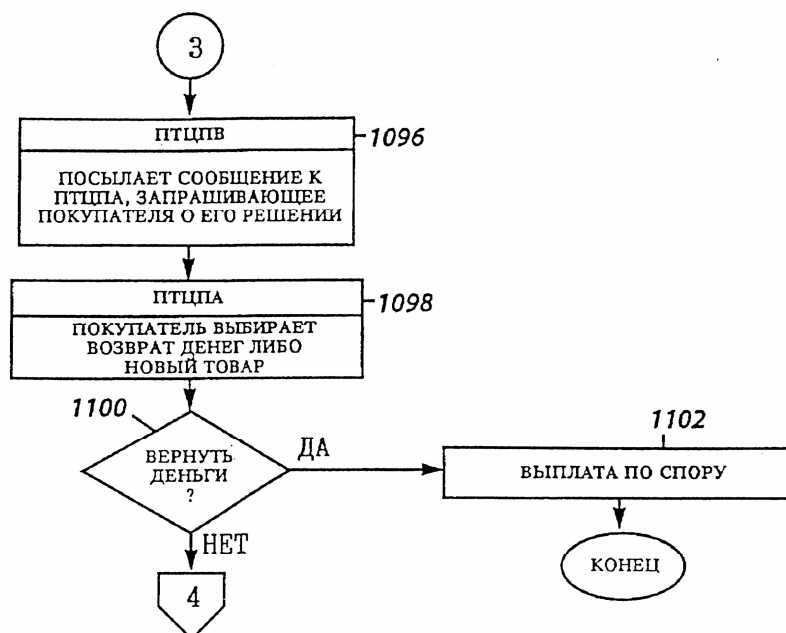
Фиг. 30А



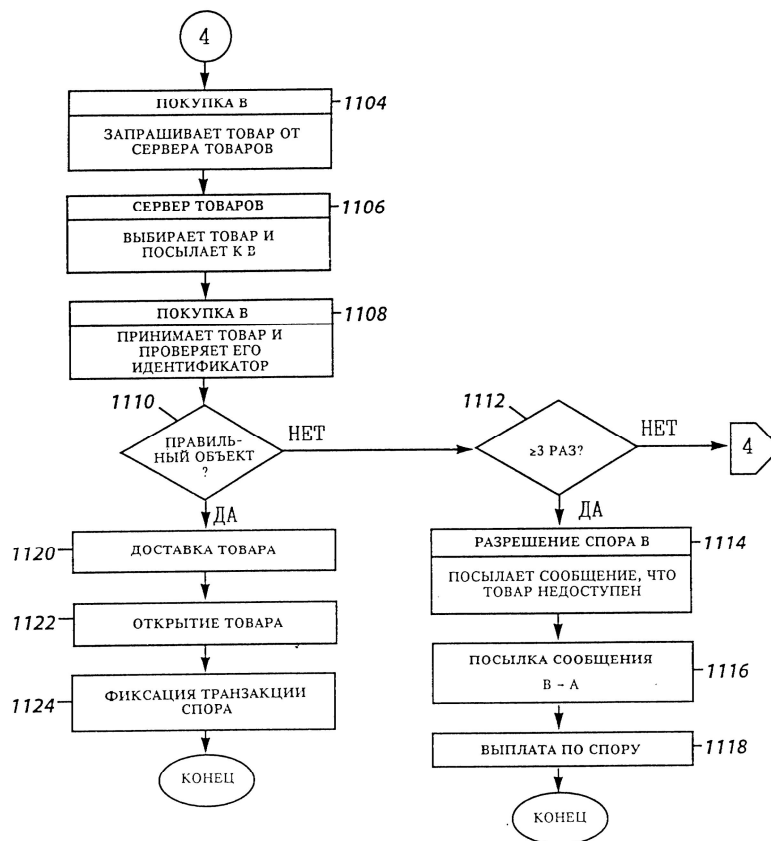
Фиг. 30Б



Фиг. 30В



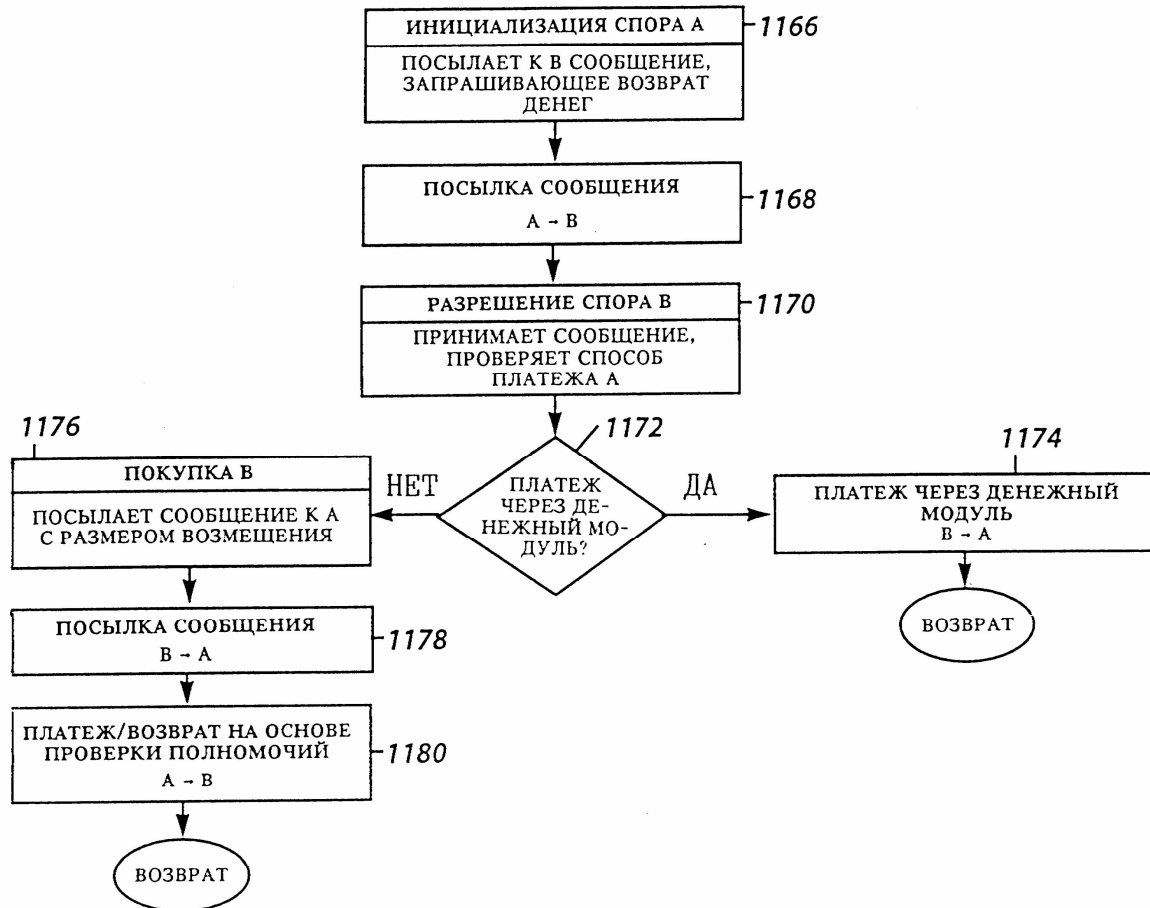
Фиг. 30Г



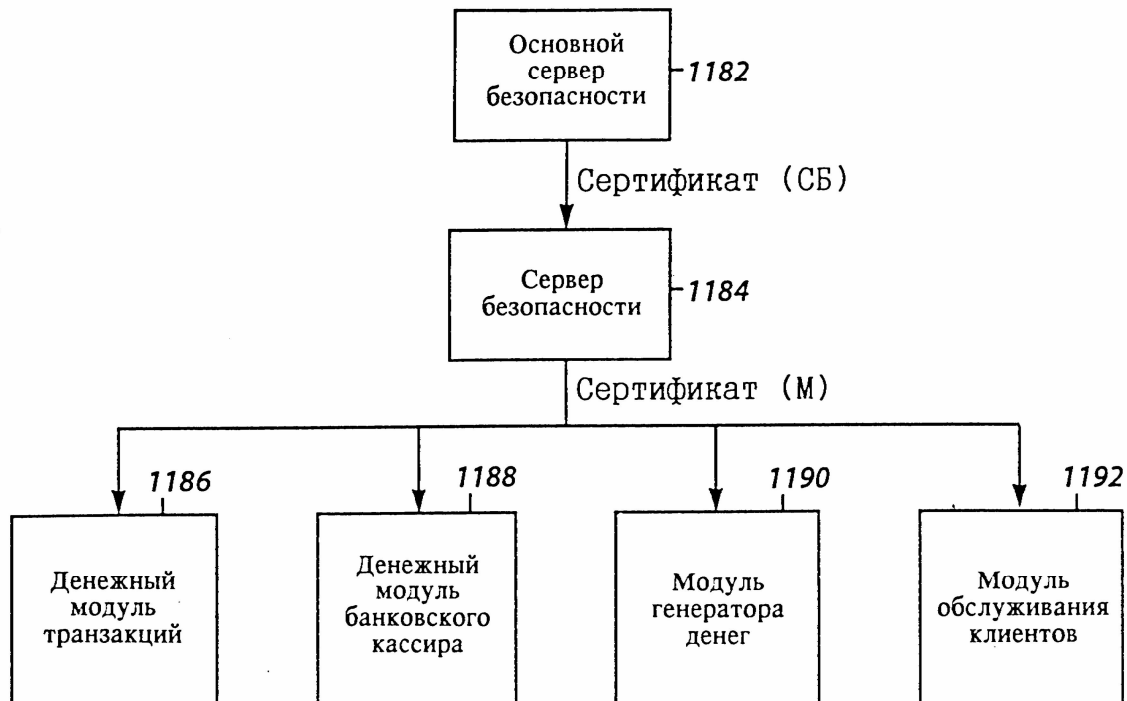
Фиг. 30Д



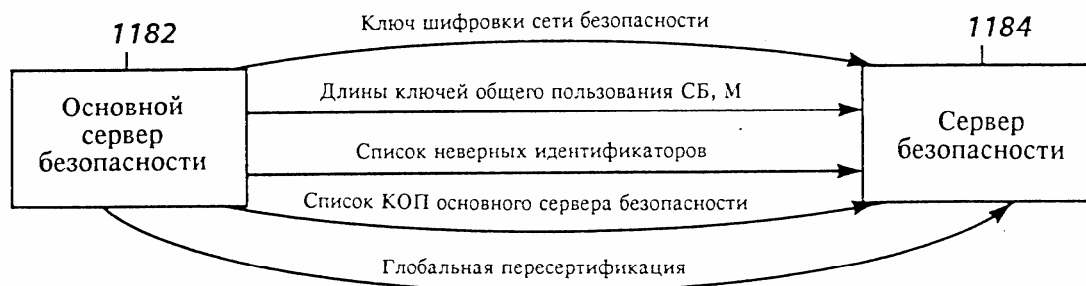
Фиг. 31



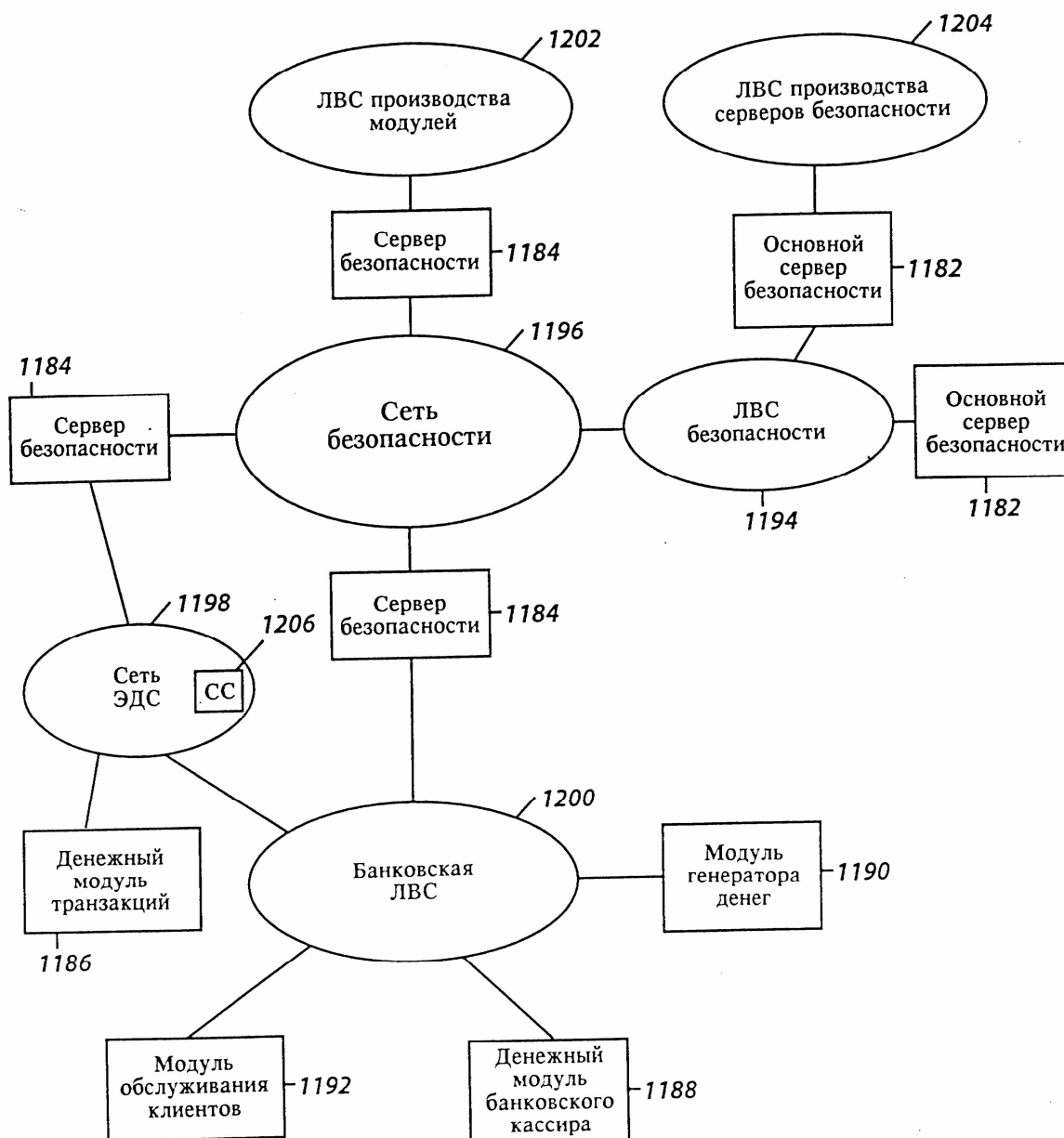
Фиг. 32



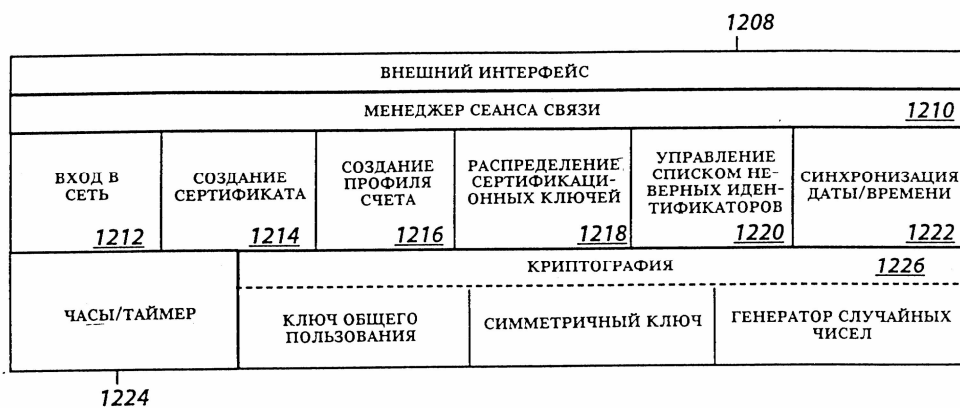
Фиг. 33А



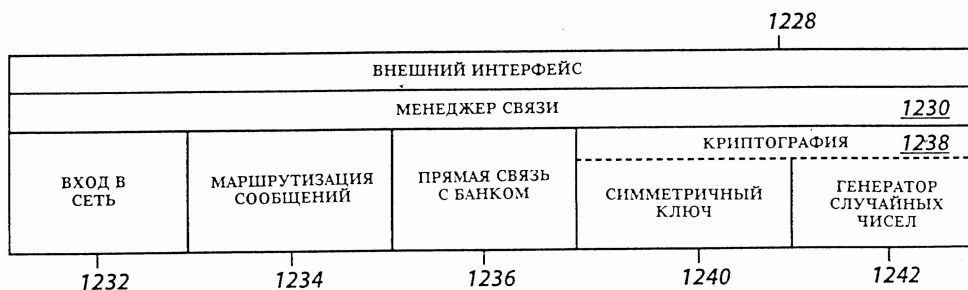
Фиг. 33Б



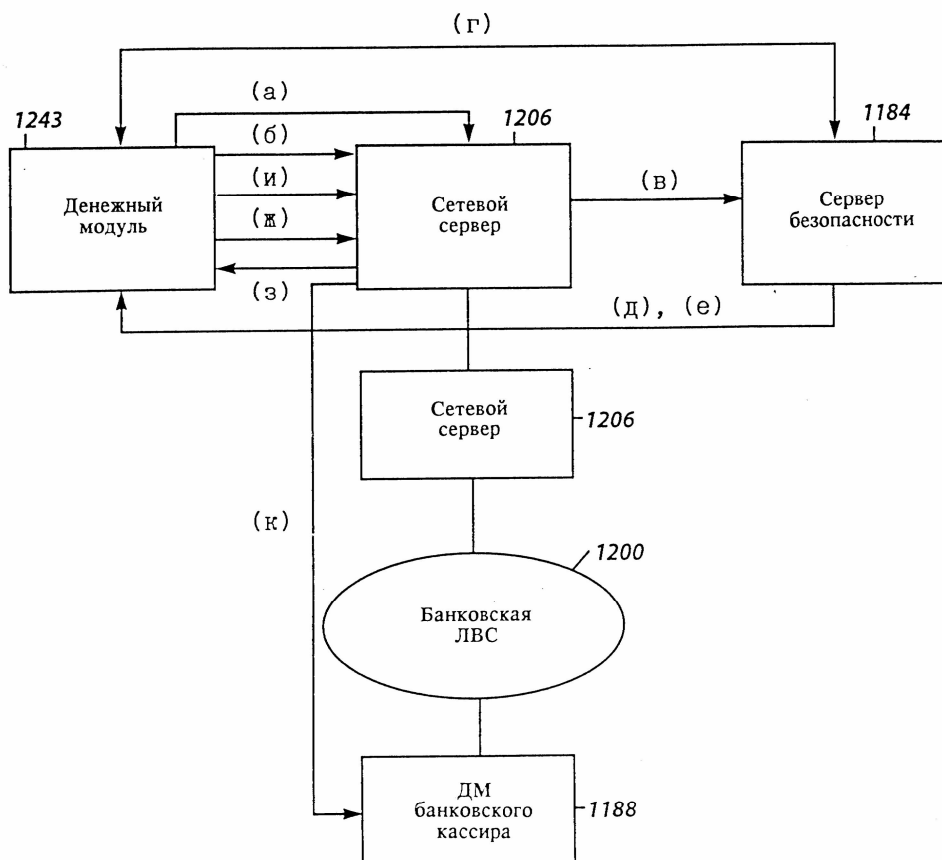
Фиг. 34



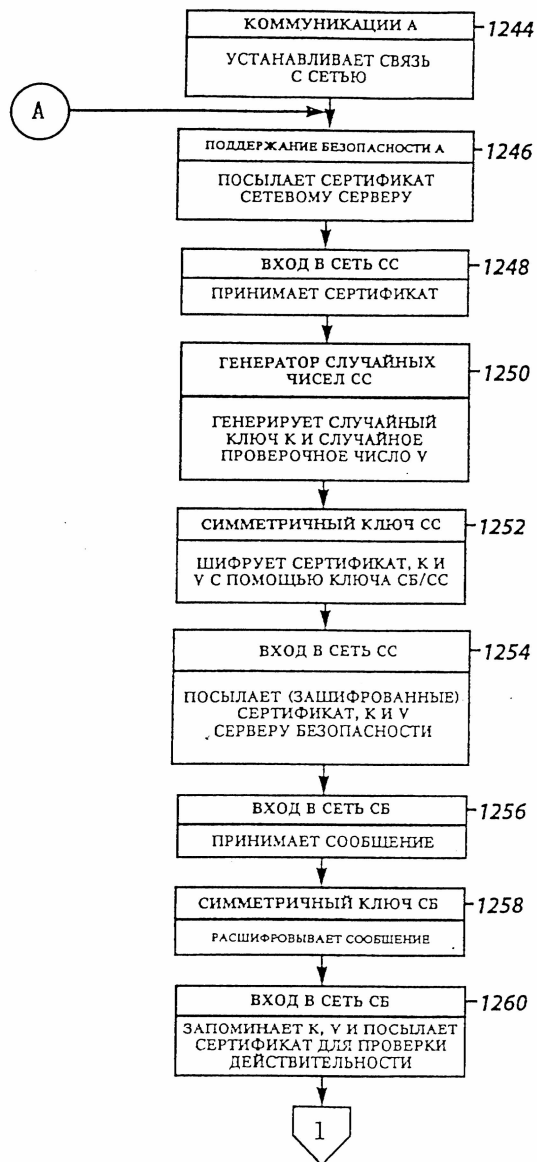
Фиг. 35А



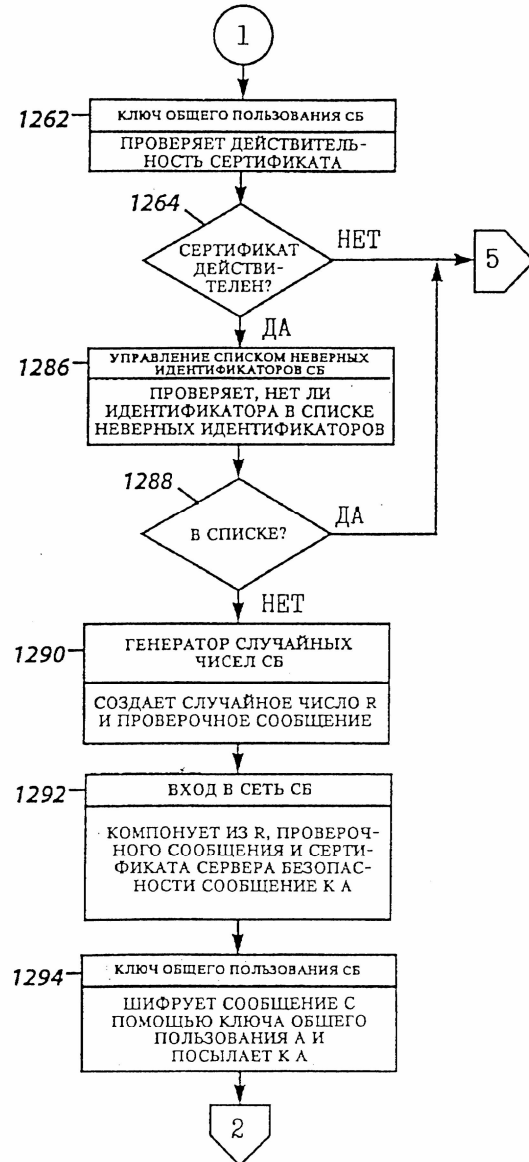
Фиг. 35Б



Фиг. 36

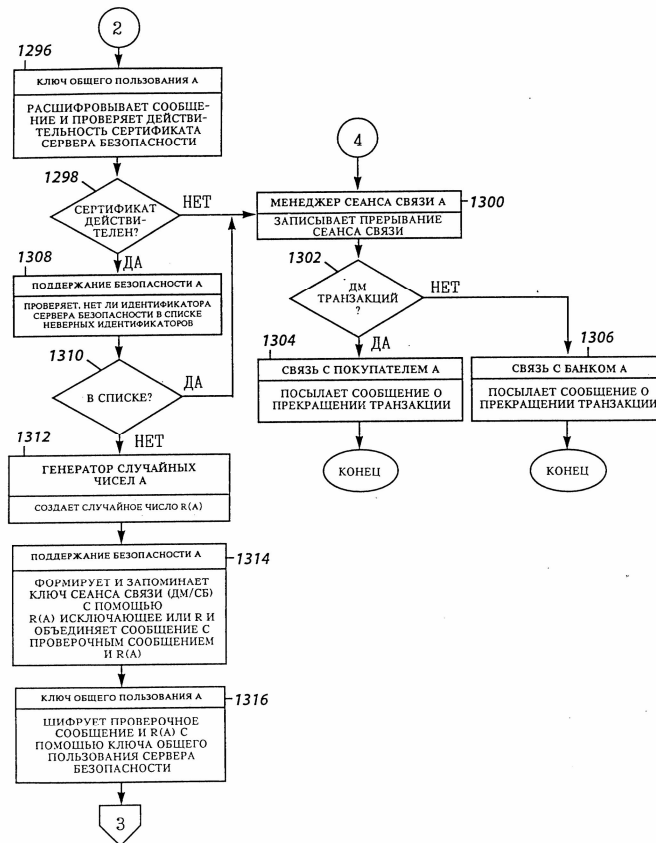


Фиг. 37А

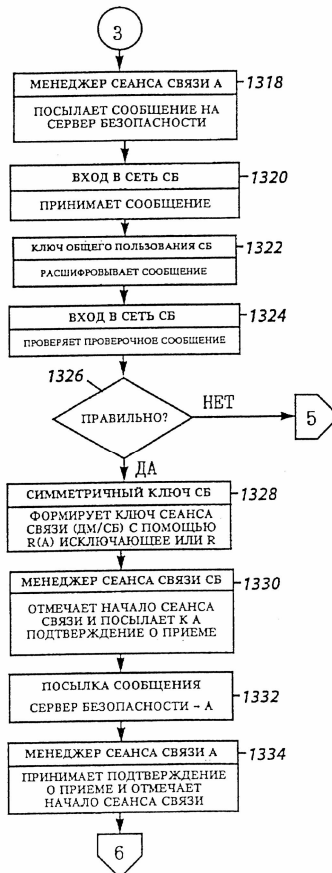


Фиг. 37Б

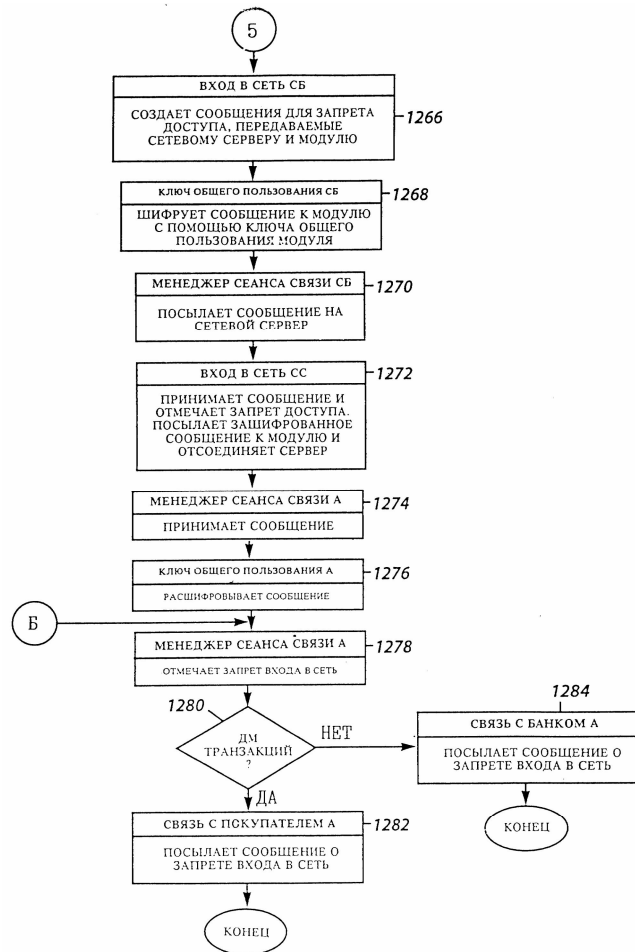




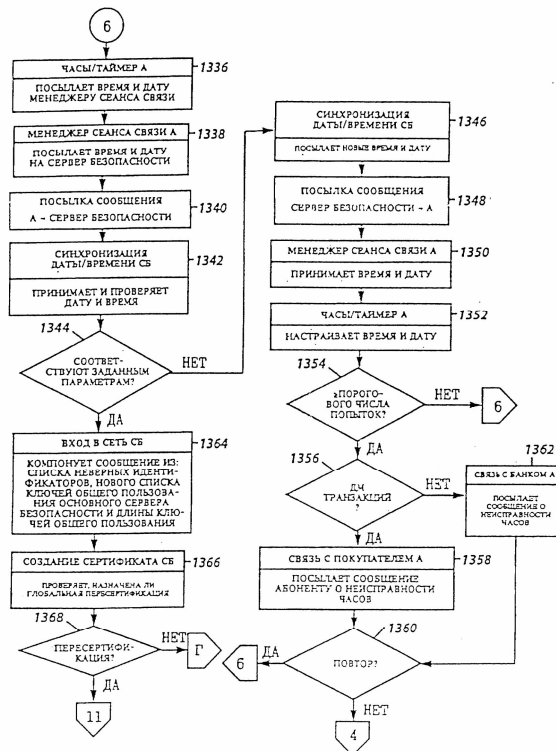
Фиг. 37В



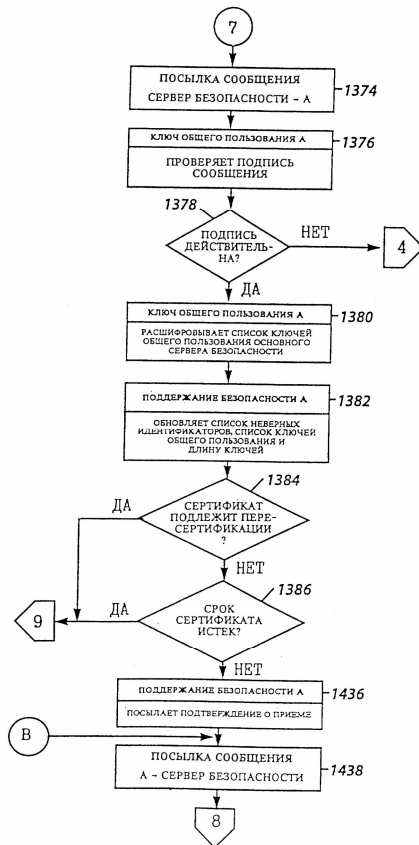
Фиг. 37Г



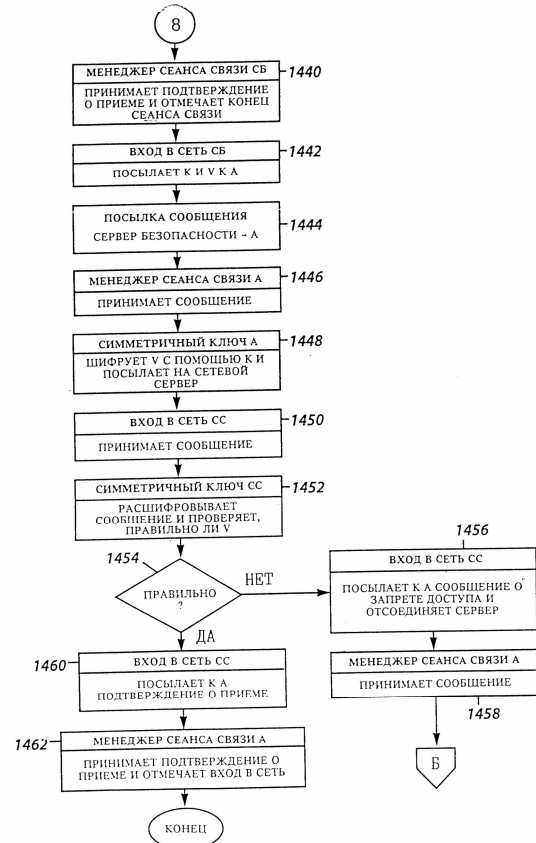
Фиг. 37Д



Фиг. 37Е



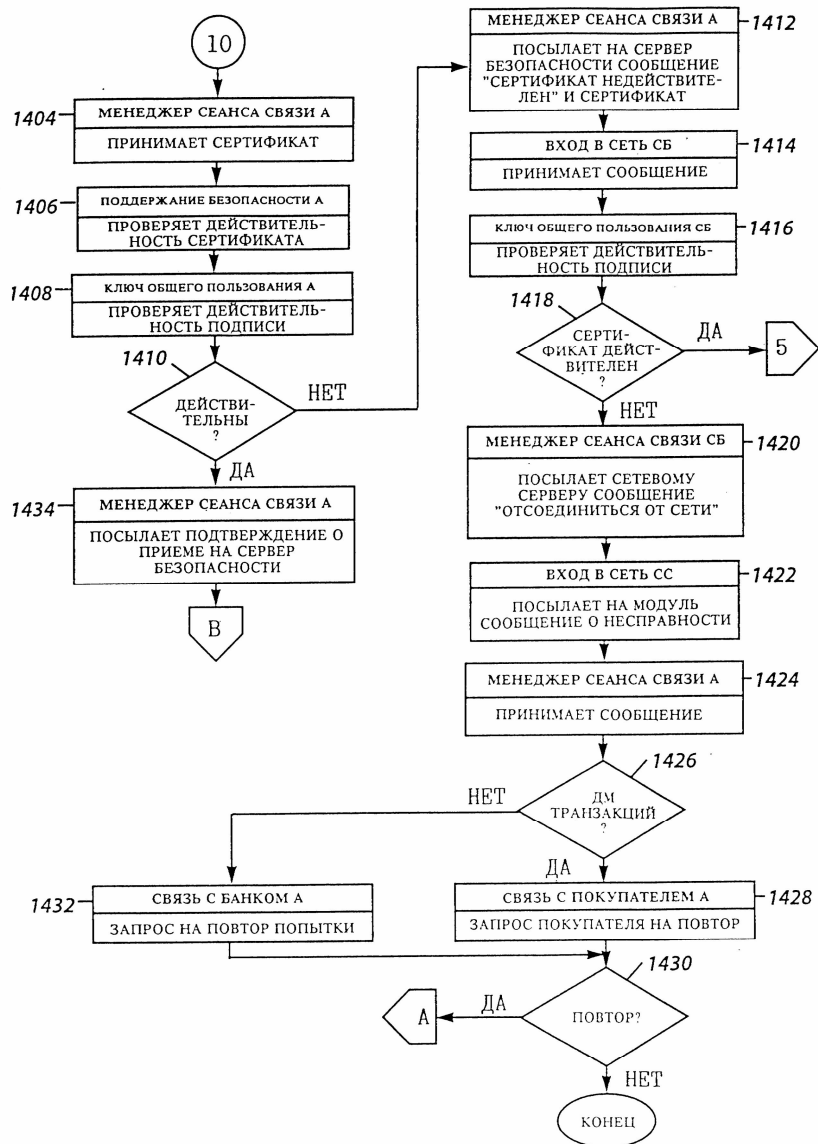
Фиг. 37Ж



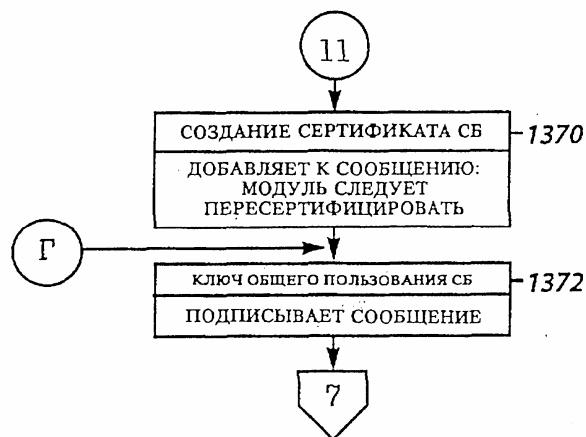
Фиг. 37З



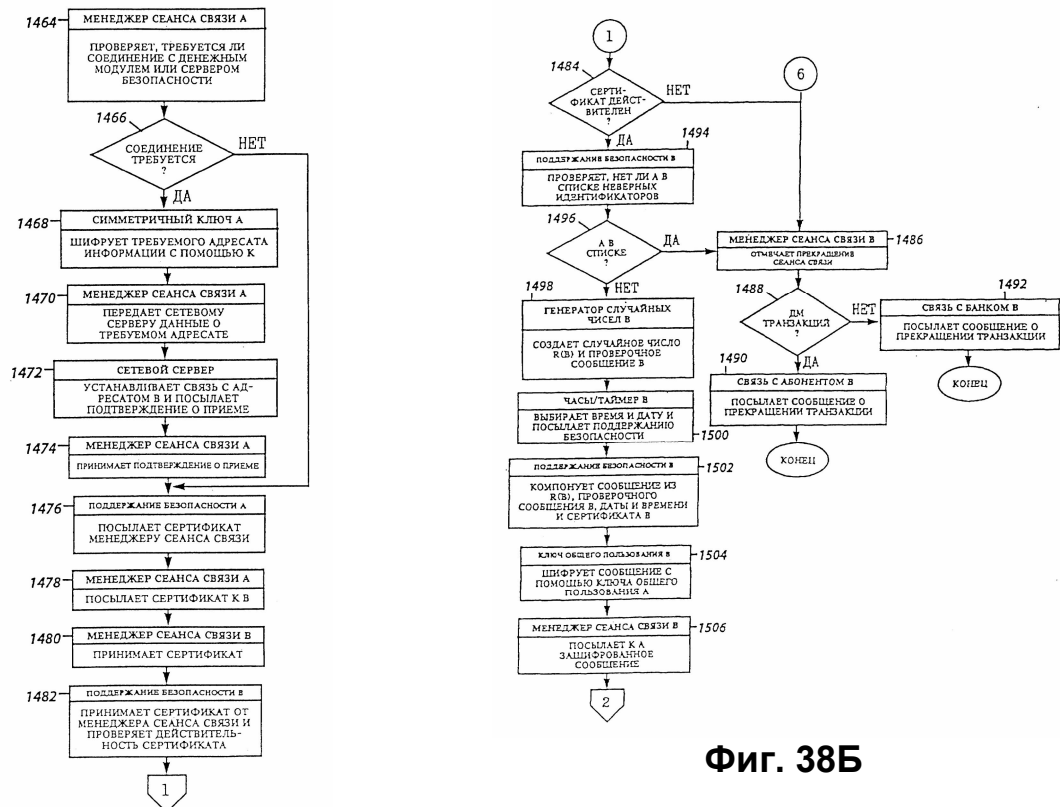
Фиг. 37И



Фиг. 37К

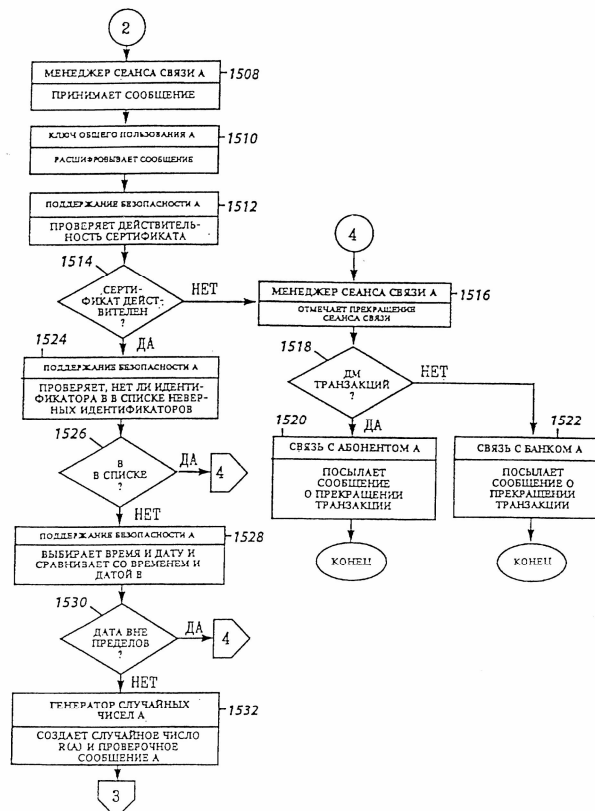


Фиг. 37Л

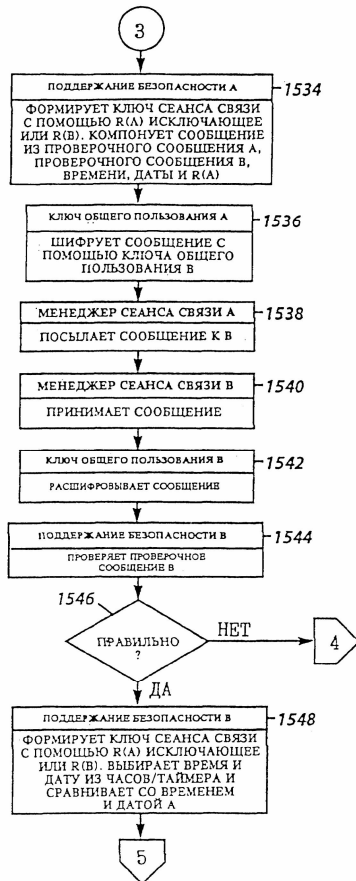


Фиг. 38Б

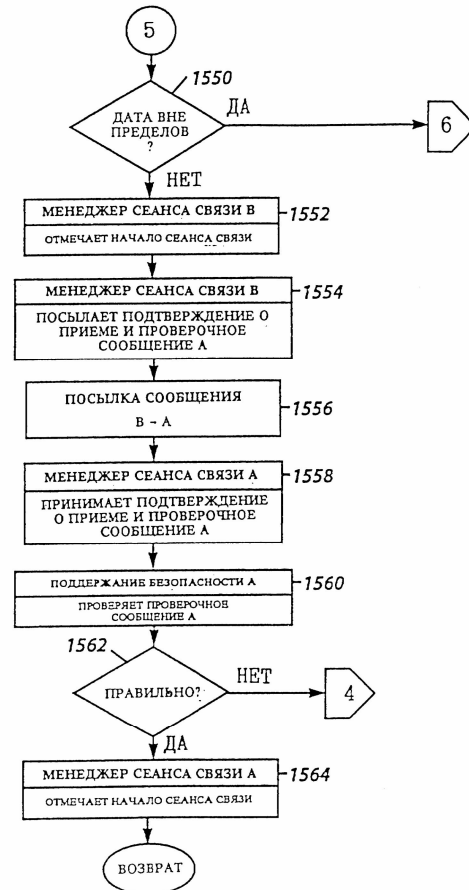
Фиг. 38А



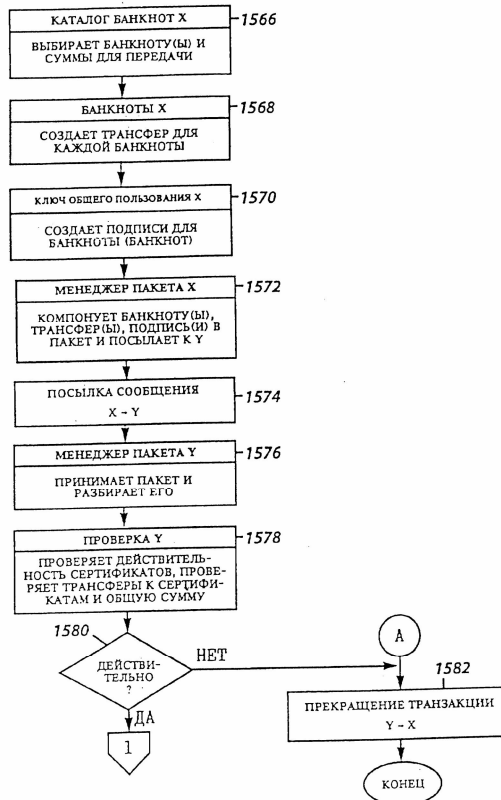
Фиг. 38В



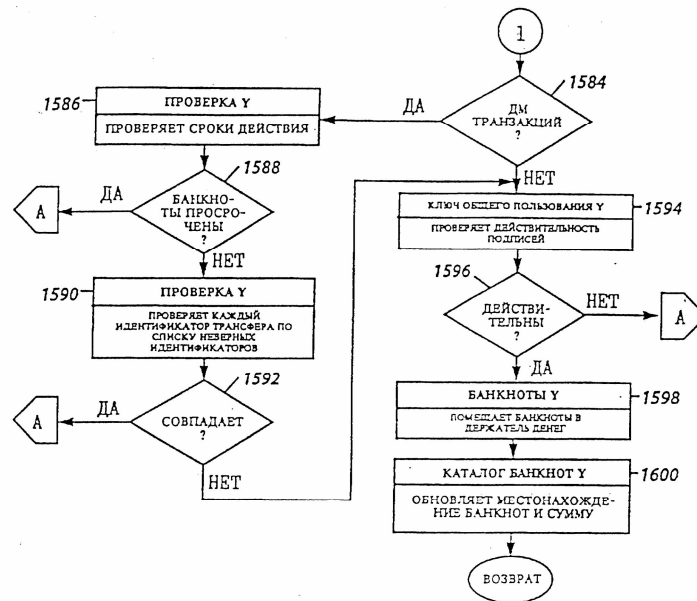
Фиг. 38Г



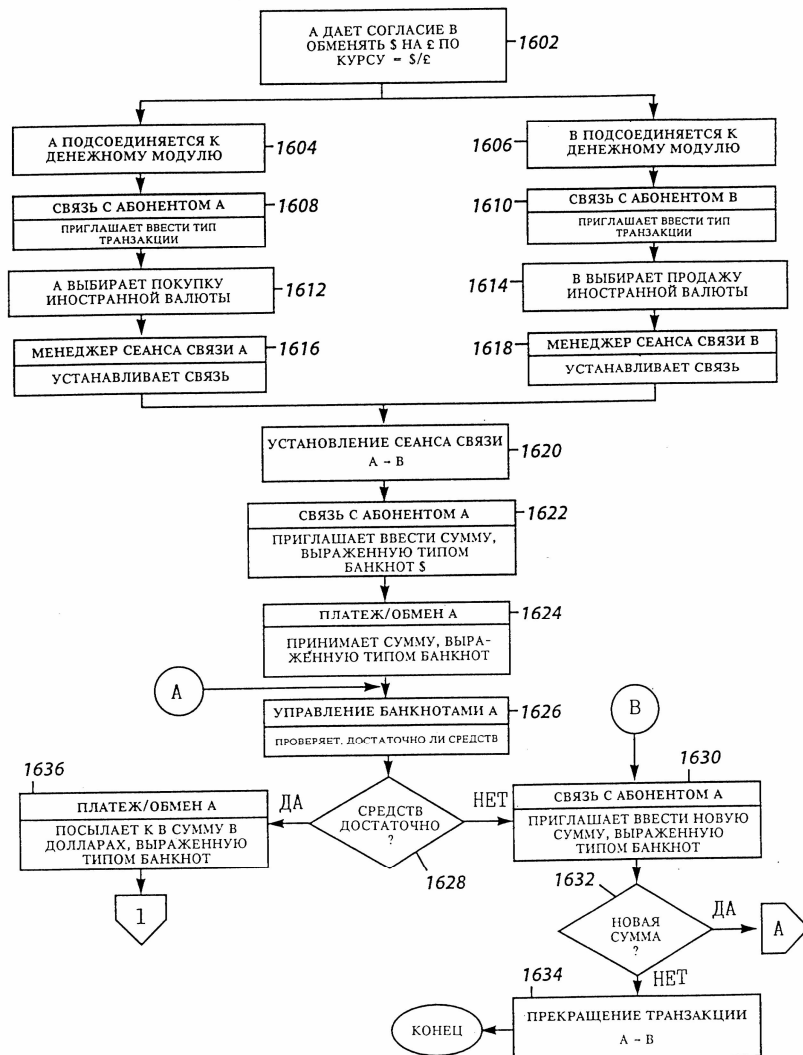
Фиг. 38Д



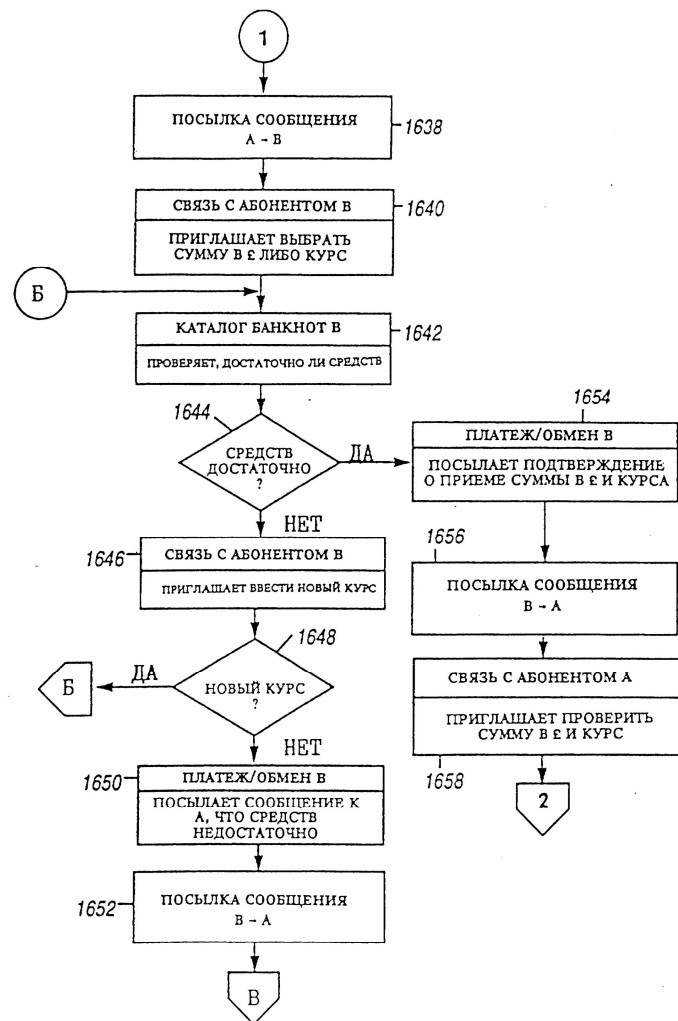
Фиг. 39А



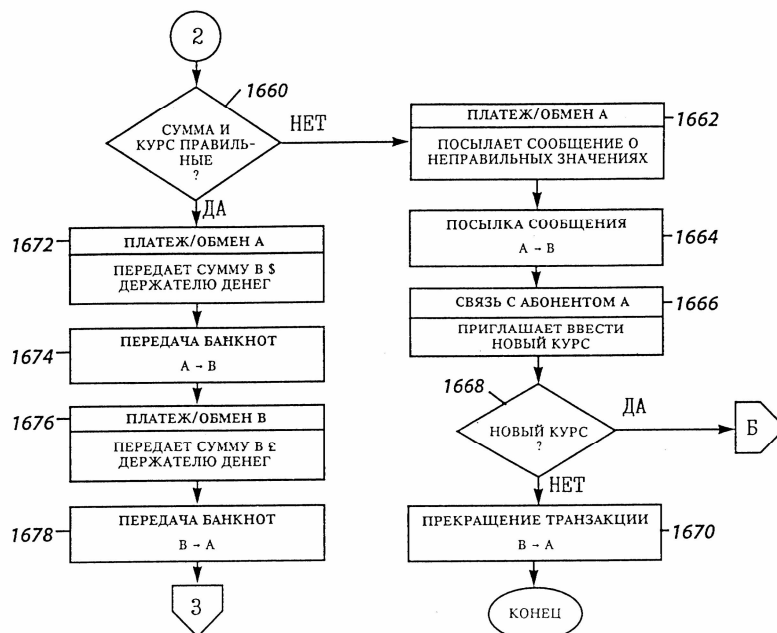
Фиг. 39Б



Фиг. 40А

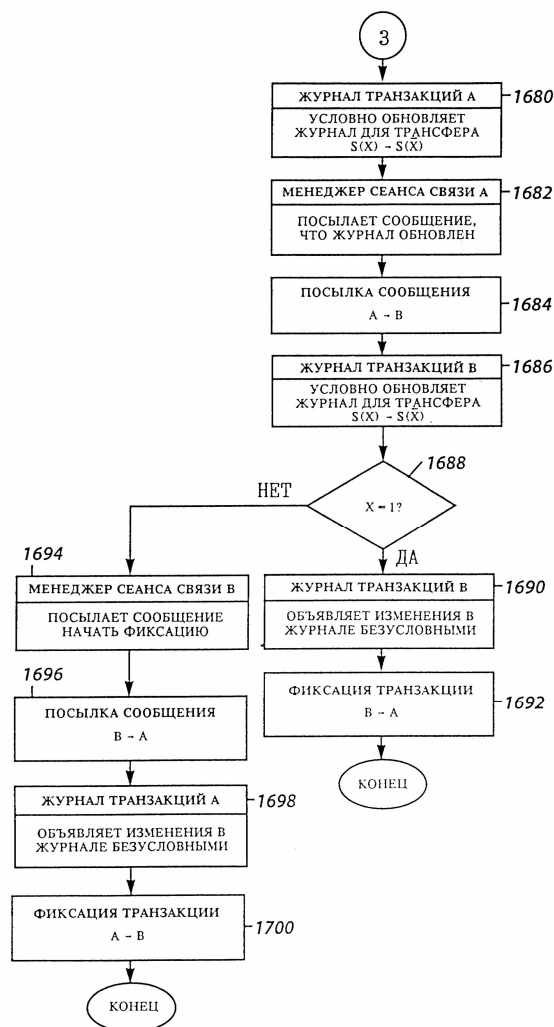


Фиг. 40Б

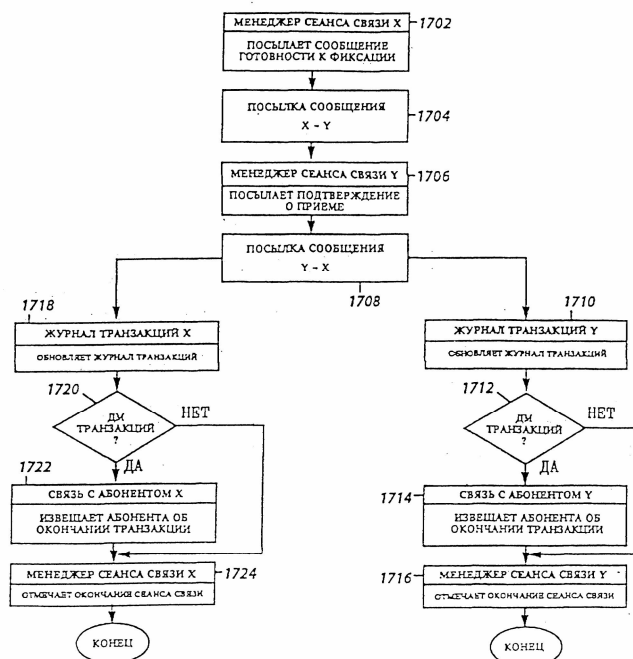


Фиг. 40В

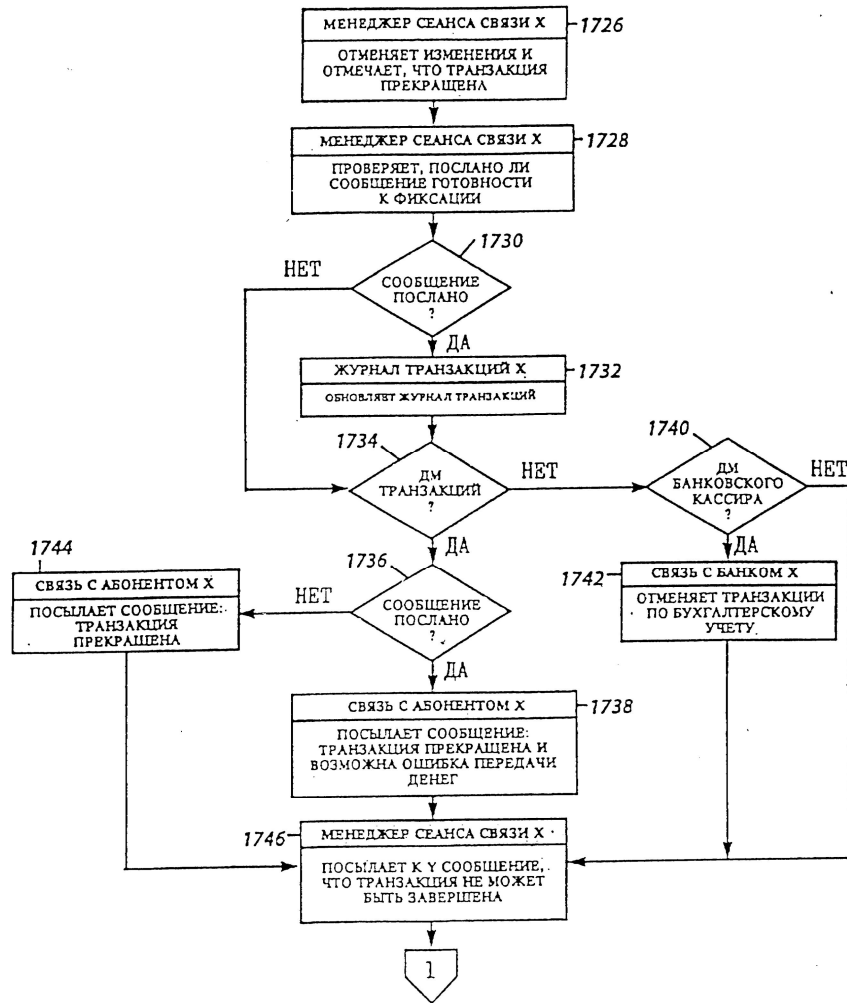




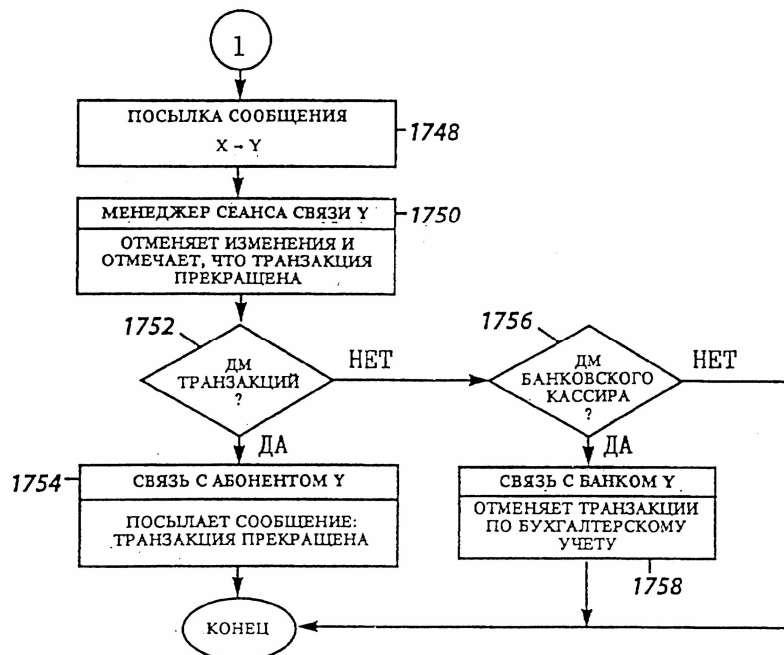
Фиг. 40Г



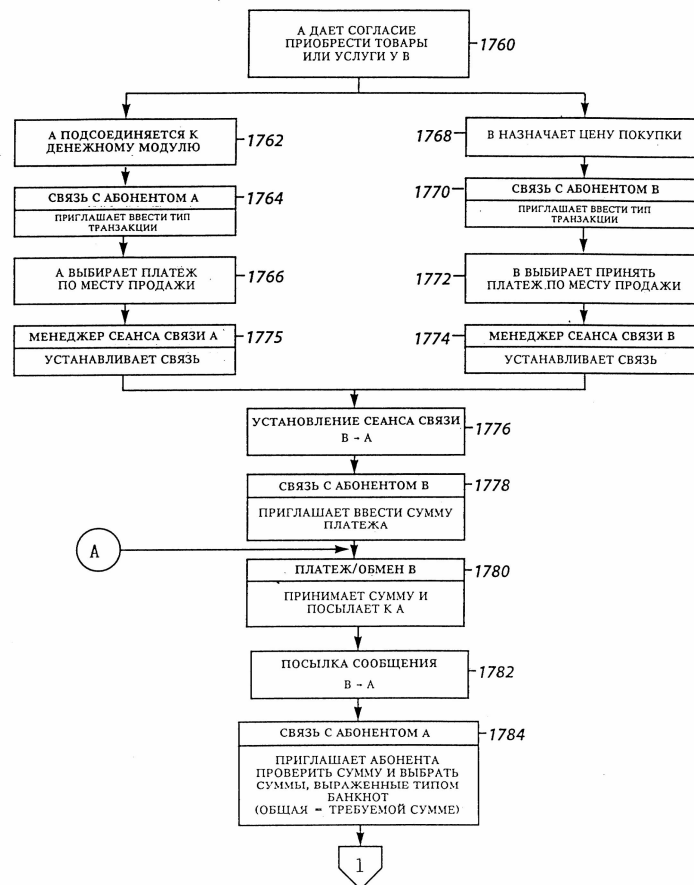
Фиг. 41



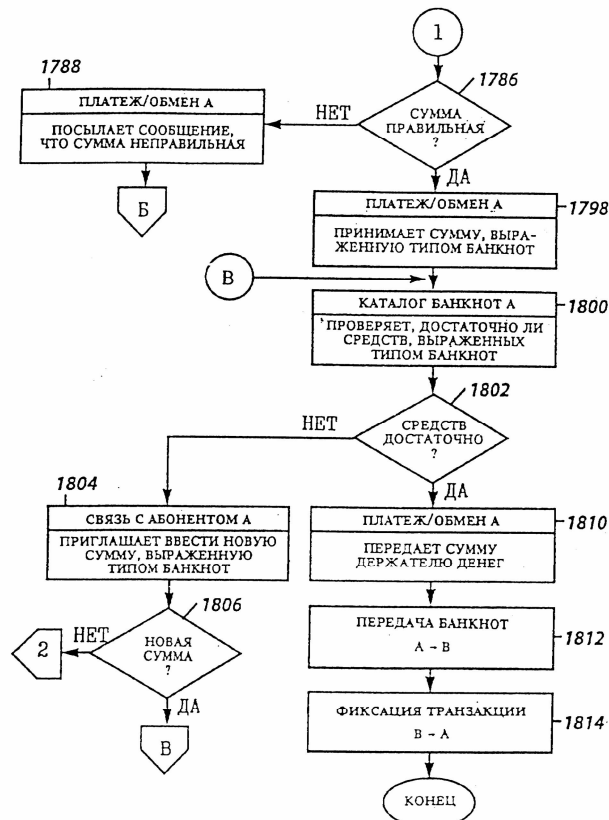
Фиг. 42А



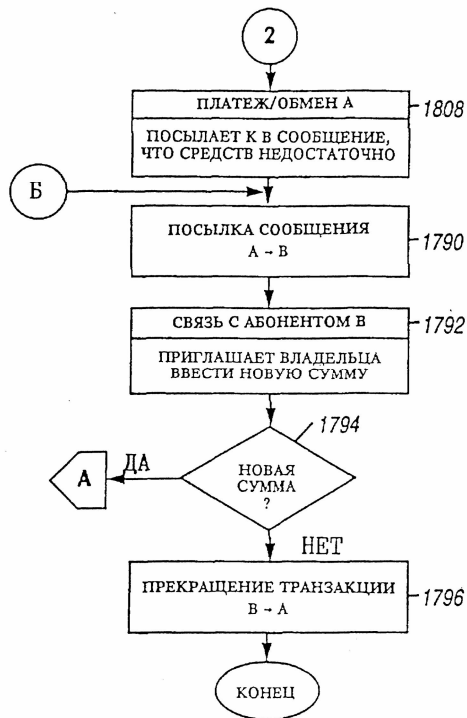
Фиг. 42Б



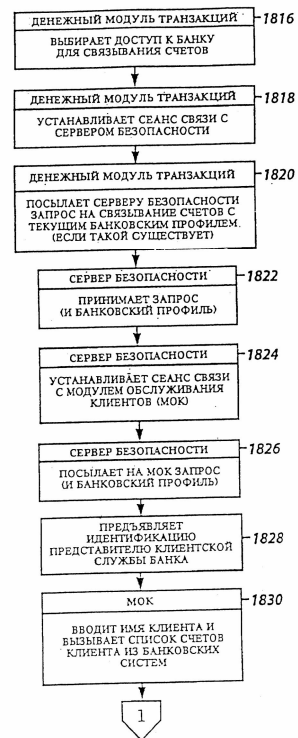
Фиг. 43А



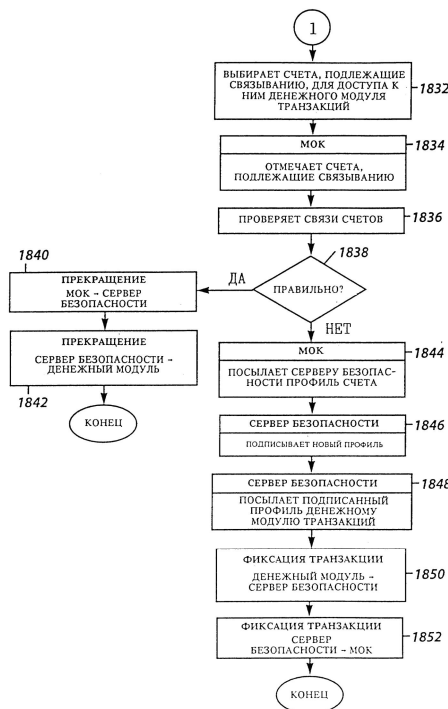
Фиг. 43Б



Фиг. 43В



Фиг. 44А



Фиг. 44Б

Тираж 50 экз.

Відкрите акціонерне товариство «Патент»  
Україна, 88000, м. Ужгород, вул. Гагаріна, 101  
(03122) 3 – 72 – 89 (03122) 2 – 57 – 03