



УКРАЇНА

(19) UA (11) 45399 (13) C2

(51) 6 G07F19/00, G07F7/08

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) ЕЛЕКТРОННА ГРОШОВА СИСТЕМА

1

(21) 97115594
(22) 19 04 1996
(24) 15 04 2002
(86) PCT/US96/05521, 19 04 1996
(31) 08/427,287
(32) 21 04 1995
(33) US
(46) 15 04 2002, Бюл. № 4, 2002 р.
(72) Розен Шолом, US
(73) CITIBENK N A, US
(56) Заявка PCT 93/08545, МПК G07F 19/00, пул 29 04 93
(57) 1 Система для передачі електронних банкнот між електронними модулями, що містить електронні модулі, кожний з яких має процесор, пам'ять та засоби для створення криптографічно безпечного каналу, а також для передачі і приймання електронних банкнот по цьому криптографічно безпечному каналу і в кожному з яких в його пам'яті зберігаються електронні банкноти, кожна з яких містить основну групу полів даних, що має дані про грошову вартість даної електронної банкноти, і групу полів даних передачі, що містить список записів трансфертів, кожна з яких формується електронним модулем відправника і має порядковий номер, який є відмітною ознакою переданої електронної банкноти від однієї або кількох інших електронних банкнот, що передаються від загального електронного модуля відправника і генеруються на основі загальної електронної банкноти
2 Система за п 1, яка відрізняється тим, що грошова вартість є вихідною грошовою вартістю, пов'язаною з електронною банкнотою, а записи передачі додатково мають передану грошову вартість
3 Спосіб платежу, який відрізняється тим, що використовує перший грошовий модуль для передачі електронного подання грошей другому грошовому модулю, і який містить такі кроки
(а) встановлення криптографічно безпечного сеансу зв'язку між першим грошовим модулем і другим грошовим модулем, де перший і другий грошові модулі є модулями, захищеними від несанкціонованого доступу,
(б) нагадування від другого грошового модуля другому абоненту про умови транзакції та надання умов транзакції другим абонентом другому грошо-

2

вому модулю,
(в) посилення другим грошовим модулем умов транзакції першому грошовому модулю через криптографічно безпечний сеанс зв'язку,
(г) нагадування першим грошовим модулем першому абоненту про перевірку умов транзакції та надання першим абонентом перевірки умов транзакції,
(д) передача першим грошовим модулем електронного подання грошей другому грошовому модулю через криптографічно безпечний сеанс зв'язку,
(е) фіксація першим грошовим модулем передачі електронних грошей за допомогою запису передачі електронних грошей до журналу так, щоб перший грошовий модуль не міг більш припинити передачу електронних грошей скасуванням свого стану, та
(є) фіксація другим грошовим модулем передачі електронних грошей за допомогою запису передачі електронних грошей до журналу так, щоб другий грошовий модуль не міг більш припинити передачу електронних грошей скасуванням свого стану
4 Спосіб платежу за п 3, який відрізняється тим, що в ньому умови транзакції містять грошову вартість електронного подання грошей, і в якому крок надання першим абонентом перевірки містить призначення розподілу грошової вартості між готівковими грошима та кредитом
5 Спосіб передачі електронних банкнот між виконавцями на процесорах електронними модулями, який відрізняється тим, що містить такі кроки встановлення криптографічно безпечного сеансу зв'язку між електронним модулем сторони, що передає, та електронним модулем сторони, що приймає,
створення електронної банкноти, що передається, шляхом приєднання запису передачі до електронної банкноти, що зберігається в електронному модулі передавальної сторони, де запис передачі показує, чи передається уся грошова вартість електронної банкноти або ж лише якась її частина,
передача електронної банкноти, що передається, від електронного модуля передавальної сторони електронному модулю приймальної сторони, та в якому запис передачі містить порядковий номер, що відрізняє електронну банкноту, що пере-

(13) C2

(11) 45399

(19) UA

дається, від іншої електронної банкноти, що передається, з грошового модуля передавальної сторони

6 Спосіб входження електронного модуля у електронну грошову мережу з мережним сервером, що зв'язує електронний модуль з сервером безпеки, який відрізняється тим, що містить такі кроки посилання електронним модулем свого сертифіката мережному серверу, вироблення мережним сервером випадкового ключа та випадкового перевірного числа та посилання зашифрованого повідомлення, що містить сертифікат, випадковий ключ і випадкове перевірного число до сервера безпеки, розшифрування сервером безпеки зашифрованого повідомлення, запам'ятовування випадкового ключа і випадкового перевірного числа та перевірка дійсності сертифіката, встановлення сервером безпеки безпечного сеансу зв'язку з електронним модулем, посилання сервером безпеки поновленої інформації про безпеку, яка цифровим чином підписується криптографічним ключем сервера безпеки, до електронного модуля, перевірка електронним модулем дійсності підписаної цифровим чином поновленої інформації про безпеку та поновлення інформації, що запам'ятовується, про безпеку за допомогою поновленої інформації про безпеку, посилання сервером безпеки випадкового ключа і випадкового перевірного номера електронному модулю та закінчення безпечного сеансу зв'язку, вироблення електронним модулем повідомлення адресата шляхом шифрування випадкового перевірного числа і адресата за допомогою випадкового ключа та посилання повідомлення адресата мережному серверу, розшифрування мережним сервером повідомлення і перевірка випадкового перевірного числа, та встановлення мережним сервером зв'язку з адресатом

7 Спосіб за п 6, який відрізняється тим, що в ньому електронний модуль є транзакційним модулем, модулем обслуговування клієнтів, модулем генератора грошей або модулем банківського касира

8 Спосіб за п 6, який відрізняється тим, що додатково містить кроки посилання електронним модулем своєї інформації, про дату та час серверу безпеки, перевірка сервером безпеки інформації про дату та час, щоб визначити, чи перебуває вона поза заздалегідь визначеним прийнятним параметром, та

у випадку, якщо інформація про дату та час перебуває поза прийнятним заздалегідь визначеним параметром, посилання сервером безпеки електронному модулю нових дати і часу для синхронізації електронного модуля

9 Спосіб за п 6, який відрізняється тим, що в ньому зашифроване повідомлення між мережним сервером і сервером безпеки забезпечується за допомогою локального симетричного ключа, який зберігається в мережному сервері та в сервері безпеки

10 Спосіб за п 6, який відрізняється тим, що в ньому поновлена інформація про безпеку містить поновлений список невірних ідентифікаційних номерів електронних модулів і серверів безпеки, поновлений список ключів загального користування і поновлену довжину ключа

11 Спосіб за п 6, який відрізняється тим, що в ньому крок встановлення сервером безпеки безпечного сеансу зв'язку з електронним модулем містить протокол обміну ключів загального користування для забезпечення ключа сеансу зв'язку, спільного для серверу безпеки і електронного модуля

12 Спосіб за п 6, який відрізняється тим, що додатково містить крок пересертифікації сервером безпеки сертифіката

13 Спосіб за п 12, який відрізняється тим, що в ньому крок пересертифікації відбувається у відповідь на те, що сервер безпеки надіслав повідомлення запиту на пересертифікацію електронному модулю

14 Спосіб за п 12, який відрізняється тим, що в ньому сертифікат містить термін закінчення дії і крок пересертифікації відбувається у відповідь на виявлення електронним модулем того, що термін дії сертифіката вичерпано

15 Заснована на електронному модулі система грошових транзакцій, яка відрізняється тим, що має

первинний сервер безпеки, декілька вторинних серверів безпеки, кожний з яких має унікальний сертифікат серверу безпеки, підписаний цифровим чином первинним сервером безпеки,

декілька захищених від несанкціонованого доступу електронних модулів, кожний з яких має унікальний сертифікат модуля, який підписано цифровим чином одним з вторинних серверів безпеки, пам'ять, що зберігає електронні подання грошей, і процесор, пристосований для забезпечення криптографічно безпечного каналу передачі та прийому електронних подань грошей, та

в якому сертифікат сервери безпеки підтверджується, коли вторинний сервер безпеки взаємодіє з електронними модулями або з первинним модулем безпеки, та

в якій сертифікат модуля підтверджується, коли електронний модуль взаємодіє з одним з інших електронних модулів або з серверами безпеки

16 Система за п 15, яка відрізняється тим, що в ній сертифікати модулів і сертифікати серверів безпеки мають терміни закінчення чинності і електронні модулі пристосовані таким чином, щоб не вступати в транзакції з іншими електронними модулями або вторинними серверами безпеки, які мають прострочені сертифікати

17 Система за п 15, яка відрізняється тим, що в ній кожний з декількох електронних модулів, первинний сервер безпеки і кожний з декількох вторинних серверів безпеки має унікальний ідентифікатор, що показує тип сервери або тип електронного модуля

18 Система за п 17, яка відрізняється тим, що в ній типи електронного модуля містять у собі транзакційний модуль, модуль обслуговування клієнтів, модуль генератора грошей і модуль банківського

касира, а типи сервера містять у собі первинний сервер безпеки і вторинні сервери безпеки

19 Система за п. 17, яка **відрізняється** тим, що в ній кожний з типів сервера і кожний з типів електронного модуля пов'язаний з унікальним діапазоном змінної типів та кожний унікальний ідентифікатор відбивається на значення змінної типів у межах унікального діапазону, виділеного для типу сервера або типу електронного модуля відповідно з механізмом відображення, що безпечно зберігається в кожному з електронних модулів, в кожному з вторинних серверів і в первинному сервері

20 Система за п. 19, яка **відрізняється** тим, що в ній кожний унікальний ідентифікатор є унікальним цілочисловим значенням, меншим заздалегідь визначеного простого числа, та в якій значення змінної типу виробляється відповідно до підведення первісного кореня простого числа до ступеня унікального ідентифікатора в модульній арифметиці над заздалегідь визначеним простим числом, та в якій кожний з декількох електронних модулів, первинний сервер безпеки і кожний з вторинних серверів безпеки безпечно зберігає первісний корінь і просте число

21 Система за п. 15, яка **відрізняється** тим, що в ній первинний сервер безпеки підтримує список унікальних ідентифікаторів для невірно працюючих електронних модулів і невірно працюючих вторинних серверів безпеки, та в якій список надається вторинним серверам безпеки і електронним модулям

22 Система за п. 15, яка **відрізняється** тим, що в ній сертифікат сервера безпеки шифрується первинним сервером безпеки, а сертифікат модуля шифрується вторинним сервером безпеки

23 Система за п. 22, яка **відрізняється** тим, що в ній сертифікат сервера безпеки містить перше і друге поля даних, зашифровані приватним ключем первинного сервера, безпеки, причому перше поле даних має унікальний ідентифікатор вторинного сервера безпеки, ключ загального користування серверу безпеки та час закінчення терміну дії сертифіката сервера безпеки, а друге поле даних має перше поле даних, підписане цифровим чином первинним сервером безпеки, та третє поле даних, що має унікальний ідентифікатор первинного сервера безпеки

24 Система за п. 23, яка **відрізняється** тим, що унікальний ідентифікатор первинного сервера безпеки зашифровано

25 Система за п. 22, яка **відрізняється** тим, що в ній сертифікат модуля містить

перше і друге поля даних, зашифровані приватним ключем вторинного сервера безпеки, причому перше поле даних містить унікальний ідентифікатор електронного модуля, ключ загального користування електронного модуля та дату закінчення терміну дії сертифіката модуля, а друге поле даних містить перше поле даних, підписане цифровим чином вторинним сервером безпеки, та третє поле даних, що містить сертифікат сервера безпеки

26 Система за п. 15, яка **відрізняється** тим, що в ній первинний сервер безпеки та вторинні сервери безпеки спільно використовують загальний симетричний ключ, який періодично змінюється за до-

помогою обміну ключа загального користування

27 Система за п. 15, яка **відрізняється** тим, що в ній первинний сервер безпеки вибірково видає команду на глобальну пересертифікацію для сертифікатів серверів безпеки та сертифікатів модулів

28 Спосіб платежу, який **відрізняється** тим, що використовує перший грошовий модуль для передачі електронного подання грошей другому грошовому модулю та містить такі кроки

встановлення криптографічно безпечного сеансу зв'язку між першим грошовим модулем і другим грошовим модулем, причому перший і другий грошові модулі є електронними модулями, захищеними від несанкціонованого доступу, передача першим грошовим модулем електронного подання грошей другому грошовому модулю через криптографічно безпечний сеанс зв'язку,

посилання другим грошовим модулем повідомлення про готовність до фіксації першому грошовому модулю,

посилання першим грошовим модулем другому грошовому модулю оповіщення у відповідь на повідомлення про готовність до фіксації, а після цього фіксація передачі електронних грошей так, що перший грошовий модуль більше не може перервати передачу електронних грошей шляхом скасування свого стану, та

фіксація другим грошовим модулем після прийому оповіщення так, що другий грошовий модуль не може більше перервати передачу електронних грошей шляхом скасування свого стану

29 Спосіб платежу за п. 28, який **відрізняється** тим, що в ньому кожний з грошових модулів може перервати транзакцію до фіксації передачі, дотримуючись процедури переривання, запрограмованої в грошових модулях

30 Спосіб платежу за п. 28, який **відрізняється** тим, що в ньому процедура переривання містить такі кроки, що виконуються грошовим модулем перевірка, чи відправлено повідомлення про готовність до фіксації,

якщо повідомлення про готовність до фіксації було відправлено, запис інформації, пов'язаної з електронним поданням грошей, прийнятої від першого грошового модуля, причому інформація, пов'язана з електронним поданням грошей, може використовуватися для витребування втрачених електронних грошей

31 Спосіб платежу за п. 30, який **відрізняється** тим, що в ньому процедура переривання містить такі кроки, що виконуються грошовим модулем посилання іншому з грошових модулів повідомлення, яке показує, що передача електронних грошей не може бути завершена, і в якому інший з грошових модулів у відповідь на повідомлення скасовує свої зміни, що стосуються передачі електронних грошей, і відмічає, що передачу електронних грошей було перервано

32 Спосіб платежу за п. 31, який **відрізняється** тим, що додатково містить крок посилання другому абоненту повідомлення про те, що електронну передачу перервано, коли інший з грошових модулів є транзакційним грошовим модулем, який використовується другим абонентом

33 Спосіб платежу за п. 31, який **відрізняється**

тим, що додатково містить крок інформування банку обернути транзакції з рахунками, що виконуються для електронної передачі, коли інший з грошових модулів є грошовим модулем банківського касира, зв'язаним з банком

34 Спосіб платежу за п 30, який відрізняється тим, що додатково містить крок скасування змін першим грошовим модулем і запису про те, що транзакцію перервано

35 Спосіб платежу за п 30, який відрізняється тим, що додатково містить крок посилення абоненту повідомлення про те, що електронну передачу перервано, коли грошовий модуль є транзакційним грошовим модулем, який використовується абонентом, і повідомлення про готовність до фіксації не було відіслано

36 Спосіб платежу за п 30, який додатково містить крок посилення абоненту, повідомлення про те, що електронну передачу перервано та що могла виникнути помилка електронної передачі, коли грошовий модуль є транзакційним грошовим модулем, який використовується абонентом, і повідомлення про готовність до фіксації було відправлено

37 Спосіб платежу за п 30, який відрізняється тим, що додатково містить крок інформування банку обернути транзакції з рахунками, що виконуються для електронної передачі, коли грошовий модуль є грошовим модулем банківського касира, який зв'язаний з банком, і повідомлення про готовність до фіксації було відправлено

38 Спосіб встановлення першим пристроєм сеансу зв'язку з другим пристроєм, причому перший і другий пристрої є електронним модулем або сервером в електронній грошовій системі, який відрізняється тим, що містить такі кроки

(а) прийом другим пристроєм сертифіката першого пристрою,

(б) перевірка другим пристроєм дійсності сертифіката першого пристрою,

(в) посилення другим пристроєм повідомлення першому пристрою, причому повідомлення містить частину, зашифровану за допомогою ключа загального користування першого пристрою та сертифікат другого пристрою, частина містить перше випадкове число, часову інформацію другого пристрою і перше перевірене повідомлення,

(г) перевірка першим пристроєм дійсності сертифіката другого пристрою та визначення, чи перебуває часова інформація другого пристрою в заздалегідь визначеному діапазоні часової інформації першого пристрою,

(д) посилення першим пристроєм другому пристрою другого повідомлення, яке зашифроване ключем загального користування другого пристрою, причому друге повідомлення містить друге випадкове число, вироблене першим пристроєм, друге перевірене повідомлення, вироблене першим пристроєм, перевірене повідомлення, вироблене другим пристроєм, і часову інформацію першого пристрою,

(е) формування першим пристроєм ключа сеансу зв'язку із комбінації першого випадкового числа та другого випадкового числа,

(є) перевірка другим пристроєм першого перевіреного повідомлення, формування ключа сеансу

зв'язку з комбінації першого випадкового числа та другого випадкового числа і визначення, чи перебуває часова інформація першого пристрою в заздалегідь визначеному діапазоні часової інформації другого пристрою,

(ж) посилення другим пристроєм першому пристрою оповіщення, зашифрованого ключем сеансу зв'язку, причому оповіщення містить друге перевірене повідомлення, та

(з) розшифрування, першим пристроєм оповіщення та перевірка другого повідомлення

39 Спосіб за п 38, який відрізняється тим, що в ньому перший пристрій приєднано до електронної грошової системи з мережним сервером, крок (а) містить кроки посилення першим пристроєм мережному серверу повідомлення, що містить сертифікат першого пристрою, який зашифровано за допомогою симетричного ключа, та розшифрування мережним сервером повідомлення та посилення сертифіката першого пристрою другому пристрою

40 Спосіб за п 38, який відрізняється тим, що в ньому кожний сертифікат містить унікальний ідентифікатор, який є унікальним для кожного пристрою, який додатково містить кроки визначення другим пристроєм того, чи міститься унікальний ідентифікатор першого пристрою в першому списку, який зберігається в другому пристрої, і визначення першим пристроєм того, чи міститься унікальний ідентифікатор другого пристрою в другому списку, який зберігається в першому пристрої, причому перший і другий списки є списками унікальних ідентифікаторів для невірних пристроїв

41 Спосіб за п 40, який відрізняється тим, що в ньому кожний пристрій є пристроєм одного з декількох типів, кожний з означених типів зв'язаний з унікальним діапазоном змінної типів, та в якому унікальний ідентифікатор даного пристрою відображає значення змінної типів в межах унікального діапазону, приписаного типу даного пристрою відповідно до механізму відображення, що безпечно зберігаються в кожному пристрої, в якому крок (б) містить кроки відображення унікального ідентифікатора першого пристрою в змінну типів першого пристрою та визначення того, чи відповідає змінна типів першого пристрою очікуваному типу першого пристрою, і в якому крок (г) містить кроки відображення унікального ідентифікатора другого пристрою в змінну типів другого пристрою та визначення того, чи відповідає змінна типів другого пристрою очікуваному типу другого пристрою

42 Спосіб передачі електронних банкнот заданої сумарної грошової вартості від грошового модуля відправника до грошового модуля одержувача, який містить наступні стадії

(а) вибір грошовим модулем відправника однієї або кількох електронних банкнот, які утворюють задану сумарну грошову вартість,

(б) створення грошовим модулем відправника однієї або кількох призначених для передачі електронних банкнот шляхом приєднання відповідного запису трансферту та цифрового підпису грошового модуля відправника до кожної з числа однієї або кількох електронних банкнот, для кожної з яких відповідний запис трансферту вказує, пере-

дається уся грошова вартість однієї або кількох електронних банкнот чи якась її частина,

(в) посилення грошовим модулем відправника однієї або кількох призначених для передачі електронних банкнот до грошового модуля одержувача,

(г) перевірку грошовим модулем одержувача дійсності однієї або кількох переданих електронних банкнот,

(д) зберігання грошовим модулем одержувача інформації для кожної з числа однієї або кількох таких переданих електронних банкнот, при цьому стадія (г) для кожної банкноти, що передається, з числа однієї або кількох таких банкнот передбачає перевірку інформації, що стосується банкноти, яка зберігається у грошовому модулі одержувача і містить відомості про інші банкноти, що раніше були передані до грошового модуля одержувача або грошовим модулем одержувача, на збіг з переданою банкнотою та перевірку на дублювання банкноти шляхом аналізу відомостей, що містяться в дереві передачі банкноти, заснованого на збігах, які ідентифіковані для переданої банкноти

43 Спосіб за п. 42, який **відрізняється** тим, що в ньому запис передачі містить порядковий ідентифікаційний номер, в якому для кожної з однієї або більше електронних банкнот порядковий ідентифікаційний номер відрізняє всі електронні банкноти передачі, утворені з неї

44 Спосіб за п. 42, який **відрізняється** тим, що в ньому для кожної електронної банкноти передачі з однієї або більше електронних банкнот передачі крок (г) містить крок перевірки запису передачі та всіх інших записів передачі, доданих іншими грошовими модулями сторони, що передає, для підтвердження того, що для кожної передачі була передана грошова вартість, яка не перевищує грошову вартість, передану при безпосередньо попередній передачі

45 Спосіб за п. 42, який **відрізняється** тим, що в ньому кожна електронна банкнота передачі з однієї або більше електронних банкнот передачі містить цифрові підписи та сертифікати кожного грошового модуля сторони, що передає, за всю історію електронної банкноти передачі, в якому крок (г) додатково містить крок перевірки дійсності кожного цифрового підпису та сертифіката

46 Спосіб за п. 42, який **відрізняється** тим, що в ньому кожна з однієї або більше електронних банкнот передачі містить дату закінчення терміну дії, та в якому грошовий модуль приймальної сторони є транзакційним грошовим модулем, крок (г) додатково містить крок перевірки грошовим модулем приймальної сторони дати закінчення терміну дії кожної електронної банкноти

47 Спосіб за п. 42, який **відрізняється** тим, що в ньому електронна банкнота є електронним поданням готівкових грошей, яке має дату закінчення терміну дії і грошову

вартість, в якому крок (а) містить такі кроки

(а) визначення грошовим модулем сторони, що передає, всіх можливих альтернатив для забезпечення заздалегідь визначеної сумарної грошової вартості за допомогою мінімальної кількості електронних банкнот,

(б) визначення того, який з наборів всіх можливих

альтернатив містить найменшу кількість передач, та

(в) якщо набір містить більше одного елемента, вибір елемента набору, що містить мінімальну кількість грошових одиниць-днів, підсумовану по всіх банкнотах елемента, де грошові одиниці-дні являють собою утворення числа днів, що залишилися до закінчення терміну дії електронної банкноти, і залишкової грошової вартості електронної банкноти

48 Спосіб за п. 42, який **відрізняється** тим, що в ньому крок (г) містить перевірку грошовим модулем приймальної сторони того, що передана заздалегідь визначена грошова вартість відповідає очікуваній вартості

49 Спосіб передачі електронних банкнот заздалегідь визначеної сумарної грошової вартості від грошового модуля сторони, що передає, до грошового модуля приймальної сторони, який **відрізняється** тим, що містить такі кроки

(а) вибір грошовим модулем передавальної сторони однієї або більше електронних банкнот, якими забезпечується заздалегідь визначена сумарна грошова вартість,

(б) створення грошовим модулем сторони, що передає, однієї або більше електронних банкнот передачі приєднанням відповідного запису передачі та цифрового підпису грошового модуля сторони, що передає, до кожної з однієї або більше електронних банкнот передачі відповідний запис передачі показує, чи передається увесь грошовий номінал однієї або більше електронних банкнот або ж якась його частина,

(в) посилення грошовим модулем сторони, що передає, однієї або більше електронних банкнот передачі до грошового модуля приймальної сторони,

(г) перевірка грошовим модулем приймальної сторони дійсності однієї або більше електронних банкнот передачі,

(д) збереження грошовим модулем приймальної сторони однієї або більше електронних банкнот передачі в каталозі банкнот після перевірки їх дійсності,

в якому кожна електронна банкнота передачі з однієї або більше електронних банкнот передачі містить цифрові підписи та сертифікати кожного грошового модуля сторони, що передає, за всю історію електронної банкноти передачі, кожний з сертифікатів містить унікальний ідентифікатор, що ідентифікує відповідний грошовий модуль передавальної сторони серед грошових модулів передавальної сторони за всю історію електронної банкноти передачі, та в якому запис передачі містить унікальний ідентифікатор кожного електронного модуля приймальної сторони за всю історію електронної банкноти передачі, та

в якому крок (г) додатково містить крок перевірки того, що унікальний ідентифікатор запису передачі відповідає унікальному ідентифікатору в сертифікаті для кожної успішної передачі за всю історію електронної банкноти

50 Спосіб передачі електронних банкнот від грошового модуля відправника до грошового модуля одержувача, який містить наступні стадії

(а) створення грошовим модулем відправника однієї або кількох призначених для передачі електронних банкнот шляхом приєднання відповідного запису трансферту грошового модуля відправника до кожної з числа однієї або кількох електронних банкнот,

(б) посилення грошовим модулем відправника однієї або кількох призначених для передачі електронних банкнот до грошового модуля одержувача,

(в) перевірку грошовим модулем одержувача дійсності однієї або кількох переданих електронних банкнот,

при цьому кожна електронна банкнота, що передається, з числа однієї або кількох таких електронних банкнот містить унікальний ідентифікатор для кожного грошового модуля одержувача за всю послідовність передачі електронної банкноти і, якщо грошовий модуль одержувача є грошовим модулем транзакцій, стадія (в) додатково передбачає перевірку кожного унікального ідентифікатора щодо наявності будь-якого з них у списку унікальних ідентифікаторів для несправних грошових модулів, який зберігається у грошовому модулі одержувача

51 Спосіб обміну першим абонентом електронного подання першої іноземної валюти, що зберігається в першому транзакційному модулі, на електронне подання другої іноземної валюти, що зберігається в другому транзакційному модулі, який відрізняється тим, що містить такі кроки

(а) встановлення криптографічно безпечного сеансу зв'язку між першим транзакційним модулем і другим транзакційним модулем,

(б) вибір абонентом, за допомогою першого транзакційного модуля, першої кількості першої іноземної валюти для продажу,

(в) перевірка, чи володіє перший транзакційний модуль достатніми коштами,

(г) посилення першим транзакційним модулем першої кількості другому транзакційному модулю через криптографічно безпечний сеанс зв'язку,

(д) нагадування другим транзакційним модулем своєму власнику про необхідність обрати курс обміну або другу кількість другої валюти,

(е) перевірка того, чи володіє другий транзакційний модуль достатніми коштами,

(є) посилення другим транзакційним модулем повідомлення, яке показує другу кількість або курс обміну першому транзакційному модулю через криптографічно безпечний сеанс зв'язку,

(ж) підтвердження першим абонентом другої кількості або курсу обміну,

(з) посилення першим транзакційним модулем електронного подання першої кількості першої іноземної валюти другому транзакційному модулю через криптографічно безпечний сеанс зв'язку,

(и) посилення другим транзакційним модулем електронного подання другої кількості другої іноземної валюти першому транзакційному модулю через криптографічно безпечний сеанс зв'язку,

(і) фіксація першим транзакційним модулем передачі першої іноземної валюти другому транзакційному модулю, а другим транзакційним модулем - отримання першої іноземної валюти від першого транзакційного модуля, а також фіксація другим

грошовим модулем передачі другої іноземної валюти першому транзакційному модулю, а першим транзакційним модулем - отримання другої іноземної валюти від другого транзакційного модуля, в непередбаченому порядку

52 Спосіб за п 51, який відрізняється тим, що в ньому крок (і) містить такі кроки

(а) спільне використання першим транзакційним модулем і другим транзакційним модулем загального випадкового двійкового значення, що має або перше значення, або друге значення,

(б) умовний запис до журналу першим транзакційним модулем або передачі першої іноземної валюти другому транзакційному модулю, або отримання другої іноземної валюти від другого транзакційного модуля, де загальне випадкове двійкове значення має перше значення або друге значення відповідно, так щоб можна було зробити скасування,

(в) посилення першим грошовим транзакційним модулем другому транзакційному модулю повідомлення, яке показує, що перший транзакційний модуль виконав умовний запис переносу до журналу,

(г) у відповідь на повідомлення, умовний запис до журналу другим транзакційним модулем або прийому першої іноземної валюти від першого транзакційного модуля, або передачі другої іноземної валюти першому транзакційному модулю, де загальне випадкове двійкове значення дорівнює першому значенню або другому значенню відповідно, так щоб можна було зробити скасування,

(д) посилення другим грошовим транзакційним модулем, у випадку, якщо значення загального випадкового числа дорівнює першому значенню, повідомлення про початок фіксації першому транзакційному модулю,

(е) перетворення першим транзакційним модулем, у відповідь на повідомлення про початок фіксації, умовного запису до журналу в безумовний запис до журналу та ініціалізація протоколу фіксації, в якому перший транзакційний модуль фіксує належну передачу так, що перший транзакційний модуль не може більш перервати транзакцію шляхом скасування свого стану, та в якому другий грошовий модуль фіксує передачу другої іноземної валюти і прийом першої іноземної валюти записом до журналу передачі та прийому так, що другий грошовий модуль не може більш перервати обмін іноземної валюти шляхом скасування свого стану, та

(ж) перетворення другим транзакційним модулем, якщо значення загального випадкового числа дорівнює другому значенню, умовного запису до журналу в безумовний запис до журналу та ініціалізація протоколу фіксації, в якому другий транзакційний модуль фіксує належну передачу так, що другий транзакційний модуль не може більш припинити передачу скасуванням свого стану, та в якому перший грошовий модуль фіксує передачу першої іноземної валюти та прийом другої іноземної валюти так, що перший грошовий модуль не може більш перервати обмін іноземної валюти скасуванням свого стану

53 Спосіб за п 52, який відрізняється тим, що в ньому загальне випадкове число виробляється як

ключ сеансу зв'язку під час кроку встановлення криптографічно безпечного сеансу зв'язку

54 Спосіб за п. 51, який відрізняється тим, що в ньому протокол фіксації, що ініціалізується даним грошовим модулем для будь-якої належної передачі грошей щодо другого грошового модуля, містить такі кроки

посилання даним модулем повідомлення про готовність до фіксації другому грошовому модулю, посилання другим грошовим модулем оповіщення даному грошовому модулю у відповідь на повідомлення про готовність до фіксації,

фіксація даним грошовим модулем записом до журналу будь-якої невиконаної передачі грошей так, що даний грошовий модуль не може більш перервати будь-яку невиконану передачу грошей скасуванням свого стану, та

фіксація другим грошовим модулем записом до журналу будь-якої невиконаної передачі грошей так, що другий грошовий модуль не може більш перервати будь-яку невиконану передачу грошей шляхом скасування свого стану

55 Спосіб за п. 51, який відрізняється тим, що в ньому на кроці (б) абонент обирає першу кількість першої іноземної валюти для продажу типом банкноти

56 Система передачі електронних банкнот між виконаними на процесорах електронними модулями, в якій кожний заснований на процесорі електронний модуль є одним з декількох типів модулів, яка відрізняється тим, що містить

виконані на процесорах електронні модулі, причому кожний виконаний на процесорі електронний модуль зберігає унікальний ідентифікатор і здатний створювати криптографічно безпечний канал та передавати і отримувати електронні банкноти через криптографічно безпечний канал, і де кожний електронний модуль має пам'ять для зберігання електронних банкнот,

в якій кожний з декількох типів модулів є співвідносним з унікальним діапазоном змінної типів модуля, та в якій кожний унікальний ідентифікатор відбивається в значення змінної типів в межах унікального діапазону, виділеного для типу модуля відповідно до механізму відображення, що безпечно зберігається у кожному електронному модулі

57 Система за п. 56, яка відрізняється тим, що в ній кожний унікальний ідентифікатор є унікальним цілим числом, меншим заздалегідь визначеного простого числа, та в якій значення змінної типів виробляється відповідно до піднесення первісного кореня простого числа у степінь унікального ідентифікатора в модульній арифметиці над заздалегідь визначеним простим числом, та в якій кожний з декількох електронних модулів, первинний сервер безпеки і кожний з декількох вторинних серверів безпеки зберігають первісний корінь і просте число

58 Спосіб використання абонентом транзакційного модуля для поновлення кредитної банкноти для банківського рахунка абонента в емісійному банку, що має модуль банківського касира, модуль генератора грошей та інтерактивну систему рахунків, який відрізняється тим, що містить такі кроки

(а) вибір абонентом, за допомогою транзакційного модуля, банківського рахунка, кредитну банкноту з

якого треба поновити, та кредитної суми, яка вимагається, що показує сумарну кредитну суму, що вимагається, для кредитної банкноти,

(б) встановлення транзакційним модулем першого криптографічно безпечного сеансу зв'язку з модулем банківського касира,

(в) відсилання транзакційним модулем повідомлення про витребування кредиту модулю банківського касира в першому криптографічно безпечному сеансі зв'язку, де повідомлення про витребування кредиту містить суму поновлення кредиту, відповідну чистій кредитній сумі для кредитної банкноти, та інформацію про банківський рахунок, яка відповідає банківському рахунку,

(г) перевірка інформації про банківський рахунок для підтвердження її дійсності,

(д) перевірка кредитної лінії, зв'язаної з банківським рахунком абонента, на достатність коштів для забезпечення кредитної суми, що вимагається,

(е) відсилання транзакційним модулем поточної кредитної банкноти модулю банківського касира у випадку, якщо поточна кредитна банкнота для банківського рахунка абонента існує,

(є) встановлення модулем банківського касира другого криптографічно безпечного сеансу зв'язку з модулем генератора грошей,

(ж) поновлення кредитної лінії, зв'язаної з банківським рахунком абонента, відповідно до загальної кредитної суми, що вимагається, для кредитної банкноти,

(з) відсилання модулем банківського касира запиту на створення банкноти модулю генератора грошей в другому криптографічно безпечному сеансі зв'язку, де запит на створення банкноти містить вартість, що вимагається, кредитної банкноти,

(і) вироблення модулем генератора грошей кредитної банкноти вартості, що вимагається,

(и) передавання кредитної банкноти модулю банківського касира в другому криптографічно безпечному сеансі зв'язку,

(к) передавання кредитної банкноти транзакційному модулю в першому криптографічно безпечному сеансі зв'язку,

(п) фіксація сеансу зв'язку транзакційного модуля та модуля банківського касира, та

(м) фіксація сеансу зв'язку модуля банківського касира та модуля генератора грошей

59 Спосіб за п. 58, який відрізняється тим, що в ньому, у випадку, якщо поточна кредитна банкнота існує, на кроці (в) чиста кредитна сума для кредитної банкноти становить різницю між загальною кредитною сумою, що вимагається, і поточною кредитною сумою поточної кредитної банкноти

60 Спосіб за п. 58, який відрізняється тим, що в ньому інформація про банківський рахунок містить профіль рахунка, що має номер банківського рахунка, який підписано цифровим чином модулем обслуговування клієнтів, в якому крок перевірки дійсності інформації про банківський рахунок містить крок перевірки цифрового підпису на профілі рахунка за допомогою ключа загального користування грошового модуля обслуговування клієнтів

61 Спосіб за п. 58, який відрізняється тим, що крок (є) додатково містить крок посилання транзакційним модулем грошовому модулю банківського касира будь-яких готівкових банкнот і будь-яких

кредитних банкнот, що передаються, які зберігаються в транзакційному модулі,
за кроком (е) йде крок поновлення модулем банківського касира інтерактивної системи рахунків відповідно до готівкових банкнот і кредитних банкнот, що передаються,
на кроці (і) запит на створення банкноти містить суму готівкової банкноти, що вимагається, відповідну загальній сумі готівкових банкнот і кредитних банкнот, що, передаються, які зберігаються в транзакційному модулі,
кредитування рахунка емітованих грошей в інтерактивній системі рахунків за допомогою суми, що вимагається, готівкової банкноти,
крок (к) містить крок вироблення модулем генератора грошей готівкової банкноти на суму, що вимагається, готівкової банкноти,
крок (л) містить крок передачі готівкової банкноти модулю банківського касира в другому криптографічно безпечному сеансі зв'язку, та
крок (м) містить крок передачі готівкової банкноти транзакційному модулю в першому криптографічно безпечному сеансі зв'язку
62 Спосіб зв'язку з абонентом за допомогою модуля обслуговування клієнтів, який відрізняється тим, що зв'язаний з центральним процесором, що має доступ до одного або більше банків, грошового транзакційного модуля з банківським рахунком абонента в банку, який має модуль банківського касира, модуль генератора грошей та інтерактивну систему рахунків, та який містить такі кроки
(а) доступ процесора модуля обслуговування клієнтів до інформації про банківський рахунок абонента в одному або більше банках у відповідь на одержання ідентифікаційної інформації абонента,
(б) перевірка інформації про банківський рахунок та ідентифікація абонентом банківського рахунка абонента для зв'язування з грошовим транзакційним модулем,
(в) встановлення сеансу зв'язку між транзакційним грошовим модулем і модулем обслуговування клієнтів,
(г) вироблення модулем обслуговування клієнтів профілю рахунка для банківського рахунка абонента,
(д) відсилання модулем обслуговування клієнтів повідомлення транзакційному грошовому модулю, повідомлення містить профіль рахунка та цифровий підпис профілю рахунка, зроблені приватним ключем модуля обслуговування клієнтів,
(е) перевірка транзакційним грошовим модулем цифрового підпису,
(є) приєднання транзакційним грошовим модулем сертифіката модуля обслуговування клієнтів до профілю рахунка,
(ж) збереження транзакційним грошовим модулем профілю рахунка, та
(з) фіксація сеансу зв'язку транзакційного грошового модуля і модуля обслуговування клієнтів
63 Спосіб за п. 62, який відрізняється тим, що в ньому крок (е) додатково містить крок перевірки абонентом профілю рахунка
64 Спосіб за п. 62, який відрізняється тим, що в ньому крок (з) містить крок заміни транзакційним грошовим модулем існуючого другого профілю

рахунка для банківського рахунка профілем рахунка

65 Спосіб перепідтвердження для абонента, за допомогою модуля обслуговування клієнтів, що має доступ до одного або більше банків, зв'язок транзакційного грошового модуля з банківськими рахунками абонента в банку, що має модуль банківського касира, модуль генератора грошей та інтерактивну мережу рахунків, який відрізняється тим, що містить такі кроки
(а) вибір абонентом, за допомогою транзакційного грошового модуля, банку, зв'язок з яким треба перепідтвердити,
(б) встановлення транзакційним грошовим модулем криптографічно безпечного сеансу зв'язку з модулем обслуговування клієнтів,
(в) відсилання транзакційним грошовим модулем модулю обслуговування клієнтів профілю рахунка для банківських рахунків, який зберігається в транзакційному грошовому модулі,
(г) перевірка модулем обслуговування клієнтів дійсності профілю рахунка,
(д) перевірка модулем обслуговування клієнтів за допомогою банку того, чи є активними банківські рахунки абонента, які містяться в профілі рахунка,
(е) вироблення модулем обслуговування клієнтів поновленого профілю рахунка для банківського рахунка абонента,
(є) відсилання модулем обслуговування клієнтів повідомлення транзакційному грошовому модулю, причому повідомлення містить оновлений профіль рахунка і цифровий підпис профілю рахунка, виконаний приватним ключем модуля обслуговування клієнтів,
(ж) перевірка транзакційним грошовим модулем цифрового підпису,
(з) приєднання транзакційним грошовим модулем сертифіката модуля обслуговування клієнтів до оновленого профілю рахунка, та
(і) фіксація сеансу зв'язку транзакційного грошового модуля і модуля обслуговування клієнтів
66 Спосіб за п. 65, який відрізняється тим, що в ньому профіль рахунка містить цифровий підпис конкретного модуля обслуговування клієнтів та сертифікат конкретного модуля обслуговування клієнтів, в якому крок (г) перевірки дійсності профілю рахунка містить крок перевірки цифрового підпису конкретного модуля обслуговування клієнтів і підтвердження дійсності сертифіката конкретного модуля обслуговування клієнтів
67 Електронна грошова система, яка відрізняється тим, що містить емісійний банк, що має інтерактивну систему рахунків, систему погодження емітованих грошей, електронні подання грошей, які заносяться до рахунків в інтерактивній системі рахунків, модуль генератора грошей, зв'язаний з емісійним банком, для вироблення електронних подань грошей, модуль банківського касира, зв'язаний з емісійним банком, здатний зберігати електронні подання грошей, транзакційний грошовий модуль, здатний переносити електронні подання грошей, запис передавання, який приєднується до елек-

тронних подань грошей після кожної передачі між будь-якими двома з модулів і електронні банкноти періодично передаються системі погодження емітованих грошей,

система погодження емітованих грошей має процесор для аналізу записів передачі для кожної банкноти для ідентифікації електронних подань грошей, які втрачені або дубльовані, та

в якій абонент даного транзакційного грошового модуля подає запит на втрачені гроші, що ідентифікує втрачені електронні подання грошей, до емісійного банку, а емісійний банк компенсує втрату абоненту, ґрунтуючись на запиту на втрачені гроші та на систему погодження емітованих грошей, яка підтверджує дійсність запиту на втрачені гроші для кожного втраченого електронного подання грошей

68 Електронна грошова система за п 67, яка **відрізняється** тим, що в ній кожний з транзакційних грошових модулів адаптовано для зберігання інформації, зв'язаної з електронними поданнями грошей, залученими до припинення транзакції, і в якій запит на втрачені гроші містить інформацію

69 Електронна грошова система за п 67, яка **відрізняється** тим, що в ній кожний з транзакційних грошових модулів адаптовано для зберігання запиту на втрачені гроші в незалежному пристрої зберігання та в якій запит на втрачені гроші підписується цифровим чином приватним ключем транзакційного грошового модуля

70 Електронна грошова система за п 67, яка **відрізняється** тим, що в ній запит на втрачені гроші містить інформацію, зв'язану з усіма електронними поданнями грошей, що зберігаються в транзакційному грошовому модулі

71 Спосіб для створення абонентом запиту на втрачені гроші, який відрізняється тим, що ідентифікує втрачені електронні банкноти, зв'язані з транзакційним грошовим модулем абонента, та містить такі кроки

(а) вибір абонентом, за допомогою транзакційного грошового модуля, створення запиту на втрачені банкноти,

(б) вироблення транзакційним грошовим модулем унікального порядкового номера запиту та побудова запиту на втрачені банкноти у вигляді пакета, що містить унікальний порядковий номер запиту, інформацію для всіх електронних банкнот, що передаються і які зберігаються в транзакційному грошовому модулі, інформацію про невдачу фіксації для будь-якої електронної банкноти, пов'язану з невдапою фіксацією транзакційного грошового модуля, та цифровий підпис і сертифікат транзакційного грошового модуля, та

(в) зберігання запиту на втрачені банкноти в середовищі зберігання, яке не залежить від транзакційного грошового модуля

72 Система за п 71, яка **відрізняється** тим, що в ній запит на втрачені банкноти містить

перше і друге поля даних, зашифровані за допомогою приватного ключа транзакційного грошового модуля, де перше і друге поля даних містять унікальний порядковий номер запиту, інформацію для всіх електронних банкнот, що передаються, та які зберігаються в транзакційному грошовому модулі, у тому числі поточну вартість і копію кожної з електронних банкнот, що передаються, та

інформацію про невдачу фіксації для незатребуваних невдалих фіксацій, і в якому друге поле даних містить перше поле даних, підписане цифровим чином за допомогою приватного ключа транзакційного грошового модуля, та

третє поле даних, що містить порядковий номер запиту, сумарну грошову вартість запиту на втрачені банкноти та сертифікат транзакційного грошового модуля

73 Спосіб витребування абонентом, за допомогою модуля обслуговування клієнтів, який має доступ до одного або більше емісійних банків, втрачених банкнот, зв'язаних з транзакційним грошовим модулем, шляхом використання транзакційного грошового модуля, який **відрізняється** тим, що містить такі кроки

(а) забезпечення абонентом ідентифікації для центрального процесора модуля обслуговування клієнтів,

(б) встановлення криптографічно безпечного сеансу зв'язку між транзакційним грошовим модулем і модулем обслуговування клієнтів,

(в) прийом модулем обслуговування клієнтів від центрального процесора ідентифікаційної інформації абонента,

(г) посилення транзакційним грошовим модулем модулю обслуговування клієнтів повідомлення, що містить інформацію про незатребувану невдачу фіксації, пов'язану з записами незатребуваної невдалої фіксації, що зберігаються в транзакційному грошовому модулі, та

(д) побудова модулем обслуговування клієнтів запиту з інформації про незатребувану невдачу фіксації та відсилення запиту через центральний процесор системи відслідковування емітованих грошей, зв'язаний з одним або більше емісійними банками

74 Спосіб за п 73, який **відрізняється** тим, що додатково містить крок посилення модулем обслуговування клієнтів, у відповідь на повідомлення ідентифікатора, запиту транзакційному грошовому модулю та маркування транзакційним грошовим модулем кожного із записів незатребуваної невдалої фіксації за допомогою ідентифікатора запиту

75 Спосіб за п 73, який **відрізняється** тим, що в ньому інформація про незатребувану невдачу фіксації, відіслана модулю обслуговування клієнтів на кроці (г), пов'язана тільки з незатребуваними невдалими записами, які раніше не були затребувані

76 Спосіб за п 73, який **відрізняється** тим, що до кроку (г) абонент вибирає, за допомогою транзакційного грошового модуля, записи невдалої фіксації з списку записів невдалої фіксації

77 Спосіб витребування абонентом за допомогою модуля обслуговування клієнтів, який має доступ до одного або більше емісійних банків, втрачених банкнот, зв'язаних з транзакційним грошовим модулем, за допомогою пристрою зберігання, що містить запит на втрачені банкноти від транзакційного грошового модуля, а пристрій зберігання не залежить від транзакційного грошового модуля, та який **відрізняється** тим, що містить такі кроки

(а) забезпечення абонентом ідентифікації для центрального процесора модуля обслуговування клієнтів,

(б) доступ модуля обслуговування клієнтів до запиту на втрачені банкноти, який зберігається в пристрої зберігання,

(в) прийом модулем обслуговування клієнтів запиту на втрачені банкноти від пристрою зберігання,

(г) перевірка модулем обслуговування клієнтів дійсності запиту на втрачені банкноти, та

(д) побудова модулем обслуговування клієнтів запиту з інформації про незатребувані невдалі фіксації та відсилання запиту через центральний процесор до системи відслідковування емітованих грошей, зв'язаної з одним або більше емісійними банками

78 Спосіб за п. 77, який відрізняється тим, що в ньому запит на втрачені банкноти містить сертифікат транзакційного грошового модуля та в якому крок (г) перевірки модулем обслуговування клієнтів дійсності запиту на втрачені банкноти містить перевірку дійсності сертифіката

79 Спосіб за п. 77, який відрізняється тим, що в ньому запит на втрачені банкноти містить копії втрачених банкнот, причому кожна з копій втрачених банкнот має групу полів даних сертифіката, яка містить список всіх грошових модулів передавальних сторін, які передавали оригінал копії втраченої банкноти, та містить цифровий підпис кожного грошового модуля передавальної сторони, в якому крок (г)

додатково містить крок перевіряння дійсності сертифіката та цифрового підпису кожного грошового модуля передавальної сторони

80 Спосіб за п. 77, який відрізняється тим, що в ньому запит на втрачені банкноти містить копії втрачених банкнот, причому кожна копія втраченої банкноти має поле даних запису передачі, яке містить список всіх грошових сум, переданих при кожній передачі оригіналу копії втраченої банкноти, в якому крок (г) додатково містить крок перевіряння поля даних запису передачі для підтвердження того, що для кожної передачі передавалася грошова сума, що не перевищувала грошову суму, передану при безпосередньо попередній передачі

81 Спосіб за п. 77, який відрізняється тим, що в ньому на кроці (б) встановлюється лінія зв'язку між модулем обслуговування клієнтів і центральним процесором, зв'язаним з пристроєм зберігання,

модуль обслуговування клієнтів має доступ до запиту на втрачені банкноти через лінію зв'язку

82 Заснована на електронному модулі система грошових транзакцій, яка відрізняється тим, що містить

декілька серверів безпеки, декілька захищених від несанкціонованого доступу електронних модулів, кожний з яких має унікальний сертифікат модуля, підписаний цифровим чином одним з серверів безпеки, пам'ять, в якій зберігаються електронні подання грошей, і процесор, який адаптовано для забезпечення криптографічно безпечного каналу для передачі і прийому електронних подань грошей, та

в якій сертифікат модуля підтверджується при взаємодії електронного модуля з одним з інших електронних модулів або серверів безпеки, та в якій декілька серверів безпеки вибірково віддають команду про глобальну пересертифікацію сертифікатів модуля, що потребує пересертифікації сертифіката модуля будь-якого електронного модуля, який взаємодіє з одним із серверів безпеки

83 Система за п. 1, у якій список записів трансфертів може складатися з безлічі записів

84 Система за п. 1, у якій список записів трансфертів містить безліч записів, на основі чого кожен з цих записів генерується відповідним електронним модулем відправника

85 Спосіб за п. 5, у якому електронна банкнота до приєднання запису трансферту містить інший запис трансферту з іншим порядковим номером, який відповідає електронній банкноті, переданій раніше до електронного модуля відправника

86 Спосіб за п. 50, у якому грошовий модуль одержувача є грошовим модулем транзакцій

87 Спосіб за п. 50, у якому стадія створення грошовим модулем відправника однієї або кількох призначених для передачі електронних банкнот передбачає приєднання відповідного цифрового підпису грошового модуля відправника до кожної з числа однієї або кількох електронних банкнот

88 Спосіб за п. 50, у якому відповідний запис трансферту для кожної з числа однієї або кількох призначених для передачі електронних банкнот вказує, передавалася уся грошова сума однієї або кількох електронних банкнот чи деяка частина цієї суми

Дана заявка є частковим продовженням спільно розглянутої заявки на патент США 08/234461, яка подана 28 квітня 1994р

Галузь техніки, якої стосується винахід

Даний винахід стосується електронної грошової системи для реалізації електронних грошових транзакцій як засобу, який альтернативний до економічного обміну готівки, чеків, кредитних і дебетових карток та електронного переміщення капіталів

Існуючий рівень техніки

У наш час щорічно відбувається біля 350 мільярдів грошових транзакцій між приватними особа-

ми та установами. Екстенсивне використання транзакцій монетами і паперовими грошима обмежило автоматизацію окремих транзакцій, таких як покупки, плата за проїзд, внесення грошей на банківський рахунок і зняття грошей з банківського рахунка. Окремі транзакції з використанням готових грошей ускладнені необхідністю мати потрібну кількість грошей або забезпечити здачу. Більш того, поводження з паперовими грошима та монетами і управління ними (включаючи охорону) незручне, коштове та забирає багато часу як для приватних осіб, так і для фінансових установ. За оцінками, тільки в Сполучених Штатах щорічно 60

мільярдів доларів витрачається фінансистами на те, щоб просто переміщувати гроші. Крім того, безпека паперових грошей серйозно загрожує відносною простотою їх підробки за допомогою, наприклад, досить поширених високоякісних кольорових копіювальних пристроїв.

Незважаючи на те, що чеки можуть випливатися на будь-яку конкретну суму аж до суми, доступної за рахунком, чеки мають дуже обмежену переміщуваність і повинні постачатися з фізичного опису. Паперові чекові системи не дають істотного полегшення від обмежень транзакцій з готівкою, поділяючи багато незручностей поводження з паперовими грошима та додаючи власні затримки, пов'язані з обробкою чеків. У цьому випадку економічний обмін борюється за більшу зручність при менших витратах, у той же час вимагаючи більшої безпеки.

Автоматизація досягла деяких з цих властивостей для великих транзакцій через системи автоматизованого електронного руху капіталів (ЕРК). Електронний рух капіталів є по суті процесом обміну вартостей, які відбуваються шляхом централізованих комп'ютерних транзакцій банківської системи. Послугами ЕРК є переведення платежів за допомогою електронних чеків, які спочатку використовувались великими комерційними організаціями.

Системи автоматизованого пункту розрахунків (АПР) і пункту продажу (ППР) є прикладами систем електронного руху капіталів, які за останні роки стали використовуватися торговими та комерційними організаціями на реальній основі. Однак платежі, що проводяться через ці типи систем ЕРК, обмежені тим, що вони не можуть виконуватися без банківської системи. Крім того, транзакції АПР звичайно не можуть виконуватися в неробочий час.

Послуги внутрішньодержавних банківських платежів за рахунками є прикладами системи електронного руху капіталів, яка використовується приватними особами для здійснення платежів. На поточний момент ініціативи внутрішньодержавних банківських платежів знайшли мало клієнтів. Менше одного відсотка клієнтів банків, які пропонують послуги з платежів, по переведенню рахунків та інформації за телефонними лініями за допомогою персональних комп'ютерів, користуються цією послугою. Однією з причин, через які внутрішньодержавні банківські платежі не стали успішним продуктом, є те, що клієнт не може класти гроші на рахунок і знімати їх, як вимагає того система такого типу.

Сучасні системи ЕРК, кредитні або дебетові картки, що використовуються разом з оперативними системами для переведення грошей між рахунками, наприклад, між рахунком продавця та рахунком покупця, не можуть задовольнити потребу в автоматизованій системі транзакцій, яка забезпечує рух універсально акцептованої вартості поза банківською системою. Крім того, системи кредитних і дебетових карток звичайно не захищені від шахрайства і не забезпечують адекватної секретності.

Для реалізації автоматизованої, ще зручнішої системи транзакцій, яка не вимагає банківської

системи для посередництва при переведенні та має можливість розподіляти будь-яку форму економічної вартості, з'явилася тенденція до автономного електронного руху капіталів. Приміром, було запропоновано багато ідей деякої форми "електронних грошей", які можуть використовуватися в транзакціях з безготівковими платежами як альтернатива традиційним грошовим і чековим платіжним системам. Див. патент США № 4977595, який має назву "Спосіб і пристрій для втілення електронної готівки" та патент США № 4305059, озаглавлений як "Модульна система руху капіталів".

Найбільш відомі методи містять картки з магнітною смугою, що купуються за певну суму, з яких сплачена сума може зніматися на конкретні потреби. Після витрати економічної вартості картки викидаються. Іншими прикладами є картки з пам'яттю або так звані інтелектуальні картки, які здатні багаторазово запам'ятовувати інформацію, яка становить суму, зняту таким же чином на певні потреби.

Однак ці системи страждають від нездатності повністю розпізнати значення банківських депозитів як грошей та їх необхідності субсидювати будь-яку форму універсально акцептованих грошових подань, які можуть бути емітовані. У цих системах подання економічної вартості, електронні або паперові, емітуються без субсидювання рівноцінних пасивів як дублікатів їх активів.

Жодна з цих запропонованих систем безпаперових платежів не є достатньо всебічною для впровадження багатоцільової електронної грошової системи, що містить не тільки автоматизовані пристрої, що дозволяють клієнтам переводити електронні капітали або гроші між ними без будь-якої системи посередників, але також і такої, що стосується та містить цілу банківську систему для вироблення вартості, представленої електронними грошима, і для безготівкових розрахунків і укладення угод по електронно-грошових рахунках банків і фінансових установ для підтримання грошового балансу в системі.

Таким чином, існує потреба в системі, що забезпечує звичайний економічний обмін між платником і одержувачем платежу без посередництва банківської системи, а також такої, що передає управління процесом платежу приватній особі. Крім того, існує потреба в системі економічного обміну, яка може використовуватися великими організаціями для комерційних платежів будь-якого розміру, що не має обмежень теперішніх систем ЕРК.

У патентній заявці США № 07/794112 з відкритою ліцензією, яка заявлена 15 листопада 1991 р., що включена до данного винаходу як посилання, описана електронна грошова система (ЕГС), яка переборює описані вище та інші обмеження прототипу та забезпечує повну електронно-грошову систему, що використовує електронні гроші, які можуть обмінюватися на традиційні готівкові та універсально приймаються. Винайдена ЕГС забезпечує спосіб і систему для безпечного і надійного переведення економічної вартості, у тому числі грошей і кредитів, між клієнтами, між фінансовими установами, а також між клієнтами та фінансовими установами. ЕГС забезпечує також

електронні гроші у вигляді безлічі валют. Проте, першочергова важливість безпеки та надійності породжує потребу в подальших вдосконаленнях ЕГС.

Відповідно, метою даного винаходу є забезпечення вдосконаленої ЕГС і відповідних способів економічного обміну, безпечних від повторного використання, дублювання та підробки.

Ще однією метою даного винаходу є забезпечення системи та процесу витребування втрачених грошей.

Ще однією метою даного винаходу є забезпечення дружніх щодо користувача системи та способу електронних платежів, які можуть надійно та безпечно використовуватися для переміщення грошей в реальному часі від покупця до продавця в обмін на товари.

Вищезазначені цілі та переваги даного винаходу ілюструють ті цілі та переваги, які можуть досягатися за допомогою даного винаходу, і не призначені для вичерпання або обмеження можливих переваг. Таким чином, ці та інші цілі та переваги даного винаходу стануть очевидні з опису або можуть бути виявлені в процесі впровадження винаходу, як реалізовані тут, так і змінені при розгляді будь-яких варіантів, що можуть стати очевидними для фахівців. Відповідно, даний винахід полягає в нових способах, пристроях, комбінаціях і вдосконаленнях, показаних і описаних тут.

Стислий опис винаходу

Для досягнення вищезазначених та інших цілей, спосіб та пристрій за даним винаходом використовують переважно виконаними у вигляді електронно-грошової системи, що має (1) банки або фінансові установи, підключені до пристрою грошового генератора для вироблення та емісії електронних грошей для клієнтів, що підписалися, у тому числі електронної валюти, яка підкріплена депозитами до вимоги та електронними кредитними санкціями, (2) кореспондентські банки, що приймають і розподіляють електронні гроші, (3) безпечні пристрої транзакції, які використовуються передплатниками для зберігання електронних грошей, для виконання грошових транзакцій з інтерактивними системами банків-учасників або для обміну електронних грошей з іншими подібними пристроями транзакції в автономних транзакціях, (4) пристрої видачі грошей, зв'язані з емісійними та кореспондентськими банками, для сполучення пристроїв транзакцій з емісійними та кореспондентськими банками, а також для взаємодії між самими емісійними та кореспондентськими банками, (5) кліринговий банк для підтримання балансу електронно-грошових рахунків різних емісійних банків, (6) мережу обміну даними для забезпечення комунікаційних послуг всім компонентам системи, і (7) установку безпеки для підтримання цілісності системи та для виявлення шахрайства у системі.

У переважному виконанні функції пристроїв, що виробляють гроші, пристроїв транзакцій і пристроїв видачі грошей будуть виконуватися комбінацією захищених від шахрайства модулів з комп'ютерного обладнання і прикладних програм, що можуть пов'язуватися в мережу. Інформація передається у зашифрованому вигляді для забезпе-

чення захисту від несанкційованого перегляду. Електронні гроші передаються з цифровими підписами для забезпечення підтвердження справжності та захисту від зміни або підроблення.

Електронні гроші, що обмінюються цими пристроями, можуть бути електронним поданням готових грошей або кредиту. Важливим аспектом електронних готових грошей є те, що вони еквівалентні банкнотам та можуть обмінюватися на звичайні паперові гроші через затребування депозитів в емісійному банку, але можуть і зніматися з рахунка або вноситися на рахунок як в емісійному, так і в кореспондентському банку. Однак тільки емісійні банки можуть виробляти електронну валюту та будуть нести відповідальність за її погашення.

Пізніше емісійні банки використовують процеси міжбанківського клірингу та врегулювання для підтримання грошового балансу в банківській системі, як це практикується в сучасній банківській індустрії.

Подання електронних грошей є родовими, універсально акцептованими та такими, що незаперечно погашаються з боку емісійних банків, тобто мають характеристики грошових транзакцій. Для підтримання цілісності електронної грошової системи кожний обмін електронних грошей містить, разом з іншою інформацією, ще й дані, що ідентифікують грошову одиницю кредиту або валюти (тобто долари, ієни тощо), суму в одиницях кредиту або валюти, банк, що емігував електронний кредит або електронну валюту, і декілька цифрових підписів.

Відповідно до широкого аспекту даного винаходу електронна грошова система забезпечує транзакції, що використовують електронні гроші, у тому числі електронні готові гроші, що субсидуються депозитами до вимоги в банку, замість транзакцій з готівкою, та підтвердження дійсності електронних кредитів. У виконанні даного винаходу ЕГС містить грошовий модуль для вироблення електронних грошей, грошовий модуль для емісії, розподілу та прийому електронних грошей і грошовий модуль для прийому, зберігання та перенесення електронних грошей між іншими приймаючими грошовими модулями та між приймаючим грошовим модулем і емісійним грошовим модулем.

У відповідності з додатковим аспектом даного винаходу електронна грошова система забезпечує реалізацію та підтримання електронних грошей, які містять в собі електронну валюту, яка може взаємно обмінюватися зі звичайними грошима шляхом затребування депозитів у банку та підтвердження дійсності електронних кредитів.

У виконанні даного винаходу система містить безліч емісійних банків, генераторний модуль для створення електронних грошей, модулі банківських касирів, зв'язані з генераторними модулями для виконання транзакцій банківських касирів і для взаємодії з іншими модулями банківських касирів, причому такі транзакції включають в себе прийом і розподіл електронних грошей, систему безпеки для забезпечення загальної цілісності електронної грошової системи, кліринговий і договірний процес для підтримання балансу рахунків електронних грошей окремих емісійних банків і для клірингу.

електронних грошей, емітованих емісійними банками, а також безліч транзакційних модулів, що напежать уповноваженим користувачам, для переміщення електронних грошей між транзакційними модулями та між транзакційними модулями і модулями банківських касирів, і модуль обслуговування клієнтів, який обробляє вимоги втрачених грошей і зв'язує рахунки з грошовими модулями для забезпечення банківського доступу

У відповідності з ще одним аспектом даного винаходу функції генераторних модулів, транзакційних модулів, модулів банківських касирів і модулів обслуговування клієнтів будуть виконуватися комбінацією захищених від шахрайства комп'ютерного обладнання та прикладного програмного забезпечення, що можуть бути поєднані мережею

Електронні гроші, що обмінюються даними модулями, які можуть бути електронними поданнями валюти, яка субсидюється депозитними рахунками до вимоги в емісійному банку або підтвердженнями дійсності кредитів, можуть передаватися з цифровими підписами для забезпечення захисту від несанкціонованої зміни або підробки. У виконанні, якому надається перевага, захист від підробки та втручання забезпечується також шляхом вимоги періодичного поновлення модулів та індивідуальних одиниць електронних грошей. Більш прийнятне, коли перенесення банкноти між модулями містить порядковий ідентифікаційний номер для спрощення погодження послідовності перенесення банкноти. Модулі-порушники або підроблені електронні гроші можуть вилучатися з обороту, як тільки вони виявлені.

Крім того відповідно до додаткового аспекту даного винаходу забезпечується процес витребування втрачених грошей, за допомогою якого власник/утримувач транзакційного модуля може подавати банківській системі вимоги через модуль обслуговування клієнтів, і після погодження банківською системою послідовності перенесення банкноти власник/ утримувач може повернути втрачені банкноти, які вимагаються.

Додатковий аспект даного винаходу забезпечує для транзакційного модуля процес поновлення кредиту так, щоб у грошовому модулі існувала тільки одна кредитна банкнота для кожного кредитного рахунка.

Крім того у відповідності з переважним виконанням даного винаходу для власника/утримувача транзакційного модуля забезпечується процес безпечної і надійної купівлі товарів у продавця.

Стислий опис креслень

Додаткові аспекти, ознаки і переваги даного винаходу стануть зрозуміли і більш очевидними при розгляді винаходу в світлі наступного опису разом із супутніми кресленнями, на яких

Фіг. 1А є схемою, яка показує ієрархію безпеки ЕГС.

Фіг. 1Б є схемою, яка показує повідомлення мережі безпеки між первинним сервером безпеки і звичайним сервером безпеки.

Фіг. 2 є схемою, яка показує структуру мережі безпеки для ЕГС.

Фіг. 3А ілюструє функціональні компоненти

серверу безпеки.

Фіг. 3Б ілюструє функціональні компоненти мережаного серверу.

Фіг. 4А ілюструє функціональні компоненти модуля обслуговування клієнтів.

Фіг. 4Б ілюструє функціональні компоненти первинного серверу безпеки.

Фіг. 5 показує огляд процедури входження у мережу.

Фіг. 6А - 6К ілюструють протокол входження у мережу.

Фіг. 7А - 7Д ілюструють протокол встановлення сеансу зв'язку в ЕГС.

Фіг. 8А - 8Б ілюструють протокол передачі банкнот.

Фіг. 9А - 9Г ілюструють протокол обміну іноземної валюти.

Фіг. 10 ілюструє протокол завершення для модулей в ЕГС.

Фіг. 11А - 11Б ілюструють протокол припинення транзакції для модулів в ЕГС.

Фіг. 12А - 12В ілюструють протокол платежу в пункті продажу (ППр).

Фіг. 13А - 13Б ілюструють протокол поновлення кредиту від емісійного банку.

Фіг. 14 ілюструє протокол видачі кредиту.

Фіг. 15А - 15Б ілюструють протокол запиту кредиту.

Фіг. 16 показує приклад послідовності передачі банкноти.

Фіг. 17 ілюструє дерево передачі банкноти.

Фіг. 18А - 18В ілюструють протокол зв'язку грошового модуля з банківським(и) рахунком(ами) для банківського доступу.

Фіг. 19А - 19В ілюструють протокол перепевірки вірогідності зв'язку грошового модуля з банківським(и) рахунком(ами).

Фіг. 20 ілюструє протокол вірогідного номера рахунка.

Фіг. 21А - 21Б ілюструють протокол створення вимоги на втрачені банкноти.

Фіг. 22А - 22Д ілюструють протокол витребування втрачених банкнот.

Докладний опис винаходу

Даний винахід забезпечує вдосконалену грошову систему, що використовує електронне середовище для безпечного та надійного обміну економічних вартостей. Ця система може бути реалізована інтегруванням нових систем обробки даних з іншими процедурами, які можуть бути реалізовані сучасними світовими банківськими системами. Відповідно з даним винаходом представлено декілька типів вдосконалень для Електронної Грошової Системи, яка описана в патентній заявці США № 07/794112 з відкритою ліцензією, поданою 15 листопада 1991 р., що включено до даного винаходу як посилання. Ці вдосконалення включають набір вдосконалень безпеки, у тому числі вдосконалені процеси обміну іноземної валюти (ОВ) і процеси транзакції передачі банкнот, процес витребування втрачених грошей, процес зв'язування грошових модулів для банківського доступу, процес платежу в пункті продажу та процес поновлення кредиту.

Безпека

Ефективна безпека для грошової системи має

три характеристики перешкодження шахраям, викриття шахраїв і подавлення шахраїв. Описувана ЕГС сконструйована таким чином, щоб вона містила компоненти, які виявляють всі три ці характеристики.

Для перешкодження шахраям грошові модулі сполучаються один з одним з використанням симетричного і асиметричного криптографічних ключів. Жодне повідомлення не передається в явному вигляді. Протоколи модуля також фізично захищені за допомогою апаратури, захищеної від несанкційованого доступу.

Шахрайство виявляється за допомогою процесів погодження банкнот. Загальносистемні тимчасові протоколи (наприклад, термін закінчення дії банкноти) змушують електронні банкноти проходити регулярне погодження. Електронні банкноти також поновлюються (тобто замінюються новими банкнотами з новим терміном дії) при виконанні банківських транзакцій.

Грошові модулі блокуються (наприклад, заносяться до списку невірних ідентифікаторів), якщо з ними зв'язані дубльовані або підроблені банкноти. Крім того банкноти, що пройшли через ці модулі, не будуть дозволені для передачі. Передача дубльованих або підроблених банкнот буде подальша, оскільки у банкнот закінчується термін дії або вони будуть зрештою вкладені в банк. Більш того у випадку виникнення серйозних проблем з безпекою системи, ЕГС може викликати глобальну пересертифікацію, вимагаючи тим самим пересертифікації всіх модулів, в тому числі грошових транзакційних модулів, як тільки вони в наступний раз увійдуть до мережі ЕГС.

Наступний список вдосконалень спрямований на захист всієї інформації від підслуховування транзакційних модулів. Вся інформація приховується - навіть ключі для загального користування та ідентифікатори модулів. Список вдосконалених ознак безпеки містить наступне:

(1) Захист входу в мережу так, щоб ніхто не міг обманути грошовий модуль або перехопити будь-яку його інформацію у явному вигляді, як описано нижче з посиланням на фіг. 5.

(2) Створення способу привласнення ідентифікаторів серверу безпеки, генератора грошей і банківського касира (див. "Схему нумерації модулів"). Ці ідентифікатори перевіряються при:

а) встановленні сеансу зв'язку (див. фіг. 7),

б) передачі банкнот - перевірки записів про передачу (див. фіг. 8).

(3) Реалізацію двох'ярусної структури серверу безпеки (див. "Ієрархію безпеки" і "Мережу безпеки"), що містить первинний сервер безпеки, в якому всі модулі мають ключі загального користування первинного серверу безпеки, і сервер безпеки, що сертифікує всі інші модулі.

(4) Вдосконалення передачі банкнот для перевірки списку невірних ідентифікаторів по всіх передачах перед прийняттям банкнот в платежі або обміні іноземної валюти (ОВ) і для перевірки на дубльовані банкноти (див. фіг. 8).

(5) Шифрування всіх сертифікатів за допомогою приватних ключів серверу безпеки (див. "Структуру та перевірку вірогідності сертифікату").

(6) Динамічне варіювання розмірів ключів за-

гального користування (див. "Мережу безпеки" та фіг. 6).

(7) Зміну протоколу завершення так, щоб помилка не тягнула дублювання грошей (див. фіг. 10).

(8) Зміну ОВ так, щоб жодна з сторін не могла з певністю перервати завершення з метою шахрайства, отримавши гроші і не відправивши грошей (див. фіг. 9).

(9) Зміну реєстраційної інформації про припинення транзакції при невдалому завершенні, якщо платник завершує, але отримувач припиняє транзакцію (див. фіг. 11).

(10) Дозвіл, у випадку необхідності, глобальної пересертифікації (див. "Мережу безпеки" та фіг. 6).

Наведений вище список вдосконалень безпеки висвічує деякі з ознак безпеки, які забезпечуються вдосконаленою системою безпеки за даним винаходом. Ці та інші вдосконалення можуть стати зрозумілими з наступного докладного опису альтернативного переважного виконання системи безпеки для ЕГС.

Ієрархія безпеки

Відповідно до даного винаходу ще одне виконання безпеки системи ЕГС може забезпечуватися наступним чином. Як показано на фіг. 1А, ЕГС буде мати два типи серверів безпеки: первинний 1182 та звичайний 1184. Первинні сервери 1182 безпеки сертифікують (звичайні) сервери 1184 безпеки. Сервери 1184 безпеки сертифікують всі інші модулі в системі (транзакційні грошові модулі 1186, грошові модулі 1188 банківських касирів, модулі 1190 генератора грошей та модулі 1192 обслуговування клієнтів).

Первинні сервери 1182 взаємодіють тільки з іншими первинними серверами 1182 або серверами 1184 безпеки. Як показано на фіг. 2, первинні сервери 1182 безпеки розміщуються в надійному об'єкті та сполучені один з одним за допомогою ЛОМ (локальної обчислювальної мережі) 1194 безпеки. ЛОМ 1194 зв'язана через безпечний шлюз з мережею 1196 безпеки. Цією мережею пов'язуються тільки сервери безпеки. Усі сервери безпеки є фізично захищеними пристроями.

Сервери 1184 безпеки також пов'язані з мережею 1198 ЕГС (електронної грошової системи) і локальними банківськими мережами 1200.

Припускається, що сервери безпеки можуть наражатися на певний ризик, і вони перевіряються після кожної взаємодії з іншим модулем.

Сертифікати мають тільки сервери 1184 безпеки та модулі. Ці пристрої мають ключі загального користування первинного серверу безпеки. Існує два типи сертифікатів: сертифікат серверу безпеки і сертифікат модуля.

Структура і перевірка вірогідності сертифіката

Сертифікат має наступну структуру:

Серт (СБ) = $E_{\text{ПСБ}}[(\text{ІД}) \text{ СБ} \quad (\text{КЗК}) \text{ СБ} \quad \text{термін дії}]$

дії

$\sigma_{\text{ПСБ}(X)} [(\text{ІД}) \text{ ПСБ} \text{ Виключ} \text{ АБО С}]$
-----X-----

Серт (М) = $E_{\text{СБ}} [(\text{ІД}) \text{ М} \quad (\text{КЗК}) \text{ М} \quad \text{термін дії}]$

$\sigma_{\text{СБ}}(Y)$

Серт (СБ)

-----Y-----

Протоколами підтвердження сертифіката є наступні

1) Перевірити вірогідність Серт (СБ)

а) (ід) ПСБ = [(ід) ПСБ Виключ АБО С] Виключ АБО С,

б) $D_{\text{ПСБ}}(E_{\text{ПСБ}}(X \cdot \sigma_{\text{ПСБ}}(X))) = X \cdot \sigma_{\text{ПСБ}}(X)$,

в) перевірити, чи справжній (ід)СБ (див схему нумерації модулів),

г) перевірити, чи дійсна дата,

д) перевірити, чи виконується $D_{\text{ПСБ}}(\sigma_{\text{ПСБ}}(X)) = h(X)$

2) Перевірити вірогідність Серт (М)

а) перевірити вірогідність Серт (СБ),

б) $D_{\text{СБ}}(E_{\text{СБ}}(Y \cdot \sigma_{\text{СБ}}(Y))) = Y \cdot \sigma_{\text{СБ}}(Y)$,

в) перевірити, чи справжній (ід)М ((див схему нумерації модулів),

г) перевірити, чи дійсна дата,

д) перевірити, чи виконується $D_{\text{СБ}}(\sigma_{\text{СБ}}(Y)) = h(Y)$,

де

ПСБ означає первинний сервер безпеки,

СБ означає сервер безпеки,

М означає модуль,

σ означає знак конкатенації,

ід означає ідентифікаційний номер,

h означає функцію хешування,

С означає постійне випадкове число, яке використовується всіма модулями спільно,

D означає алгоритм з ключем загального користування, що використовується для розшифрування та перевірки цифрового підпису,

КЗК означає ключ загального користування (включаючи довжину ключа),

σ означає цифровий підпис = $E \cdot h$,

Серт означає сертифікат,

E означає алгоритм з приватним ключем, що використовується для шифрування і створення цифрового підпису

Слід відзначити, що E і D можуть також використовуватися відповідно для розшифрування та шифрування при застосуванні до інших додатків

Схема нумерації модулів

Первинні сервери 1182 безпеки, сервери 1184 безпеки, грошові модулі 1188 банківських касирів, модулі 1190 генератора грошей, модулі 1192 обслуговування клієнтів і транзакційні грошові модулі 1186 одержують ідентифікаційні номери (ід), щоб номери можна було перевіряти на дійсність Генерується 48-розрядний первинний номер "р", і у процесі забезпечення безпеки перебуває первинний корінь "а" по модулю р (де $a^n \neq 1 \pmod{p}$ для всіх $1 \leq n < p - 1$) Обидві величини а і р таємно завантажуються до всіх модулів у системі в процесі їхнього виробництва первинними серверами безпеки
Схема працює наступним чином

Якщо $a^n \neq 1 \pmod{p}$ і

(1) $1 \leq m \leq 99999$, то n призначається як (ід) первинного серверу безпеки,

(2) $100000 \leq m \leq 999999$, то n призначається як (ід) серверу безпеки,

(3) $1000000 \leq m \leq 6999999$, то n призначається

як (ід) модуля банківського касира,

(4) $7000000 \leq m \leq 9999999$, то n призначається

як (ід) модуля генератора грошей,

(5) $10000000 \leq m \leq 11999999$, то n призначається як (ід) модуля обслуговування клієнтів,

(6) $m \geq 12000000$, то n призначається як (ід) грошового транзакційного модуля

Якщо модуль або сервер підтверджує вірогідність сертифікату, то цей модуль або сервер перевіряє дійсність ідентифікаційного номера n (наприклад, (ід)М, (ід)СБ або (ід)ПСБ) розрахунком $an = m(p)$, а після цього перевіряє, чи перебуває m у потрібному діапазоні

Мережа безпеки

Як показано на фіг. 2, мережа 1196 безпеки та ЛОМ 1194 безпеки зв'язують сервери 1184 безпеки з первинними серверами 1182 безпеки Сервери 1184 безпеки спочатку сертифікують грошові модулі та модулі 1192 обслуговування клієнтів при їх виробництві Такі сервери безпеки можуть бути зв'язані ЛОМ 1202 виробництва модулів Вони передають модулям інформацію про безпеку, таку як список невірних ідентифікаторів і список первинних серверів безпеки та їх ключів загального користування Список невірних ідентифікаторів містить ідентифікатори грошових модулів, модулів обслуговування клієнтів і серверів безпеки, які заблоковані від транзакцій Пересертифікація цих модулів описана нижче з посиланням на блок-схему алгоритму входження у мережу

Сервери 1184 безпеки спочатку сертифікують первинними серверами 1182 безпеки при виробництві Такі первинні сервери 1182 безпеки можуть бути з'єднані ЛОМ 1204 виробництва серверів безпеки Як показано на фіг. 1Б, сервери 1184 безпеки одержують різноманітну інформацію про безпеку, яку вони передають іншим модулям Сервери безпеки забезпечують безпечне обслуговування мережі 1198 ЕГС і банківських ЛОМ 1200, таке як входження у мережу, коли сервери передають поновлену інформацію про безпеку Сервери 1184 безпеки одержують цю інформацію від первинних серверів 1182 безпеки по мережі 1196 безпеки Транзакційні грошові модулі 1186 зв'язуються з мережею 1198 ЕГС через мережані сервери 1206 (МС) Банки, що беруть участь у системі, мають грошові модулі 1188 банківських касирів, а також, можливо, грошовий(і) генератор(и) 1190, з'єднані зі своїми ЛОМ 1200

Мережа 1196 безпеки є мережею з зашифрованими лініями зв'язку Крім того первинні сервери безпеки та сервери безпеки спільно використовують загальний симетричний ключ (ключ шифрування мережі безпеки) Цей ключ періодично змінюється певним первинним сервером 1182 за допомогою функції "Ключ загального користування"

Список невірних ідентифікаторів контролюється призначеним первинним сервером 1182 Цей список поповнюється при взаємодії з банками-учасниками, органами забезпечення правопорядку та абонентами системи

Довжина ключів загального користування для серверів безпеки і модулів буде періодично змінюватися Довжина ключа звичайно буде збільшуватися для підтримання високого рівня безпеки Нові призначені довжини ключів будуть передава-

тися на первинні сервери безпеки призначеним первинним сервером. Нові довжини будуть передаватися на сервери безпеки первинними серверами, коли посилюються нові списки невірних ідентифікаторів або після пересертифікації. У випадку виникнення небезпеки "злому" системи первинний сервер безпеки може викликати глобальну пересертифікацію.

Довжина ключа загального користування для кожного первинного серверу не буде змінюватися. Буде створюватися тимчасова таблиця, яка буде планувати введення і припинення експлуатації первинних серверів безпеки. Нові сервери найбільш певно будуть мати довші ключі, окрім випадків, коли вони впроваджуються із-за обсягу транзакцій, що збільшилися. Список ключів загального користування активного ПСБ створюється первинним сервером безпеки та підписується цим сервером за допомогою його приватного ключа. Потім список передається іншим серверам безпеки.

На фіг. 3А показано функціональні компоненти серверу 1184 безпеки. Функція 1208 "Зовнішній інтерфейс" забезпечує комунікаційний рівень для мережаної взаємодії. Функція 1210 "Менеджер сеансу зв'язку" управляє аспектами безпеки транзакційного сеансу зв'язку. Функція 1212 "Вхід до мережі" управляє функціями безпеки для входження у мережу. Функція 1214 "Створення сертифікату" створює сертифікат для будь-якого грошового модуля (в первинному сервері безпеки ця функція сертифікує сервери безпеки). Функція 1218 "Розподіл сертифікаційних ключів" розподіляє список дійсних ключів загального користування первинного серверу безпеки сертифікаційного агентства серед грошових модулів (первинний сервер безпеки також розповсюджує глобальне пересертифікаційне повідомлення). Функція 1220 "Управління списком невірних ідентифікаторів" веде список невірних ідентифікаторів і розповсюджує його. Функція 1222 "Синхронізація дати/часу" підтримує служби годинника/таймера грошового модуля синхронізованими за системним часом. Функції 1224 "Годинник/таймер" і 1226 "Криптографія" ідентичні цим же функціям у грошових модулях.

На фіг. 3Б показані функціональні компоненти мережаного серверу 1206. Функція 1226 "Зовнішній інтерфейс" забезпечує комунікаційний рівень для мережаної взаємодії. Функція 1230 "Менеджер зв'язку" управляє сеансом зв'язку між грошовими модулями та між грошовим модулем і сервером безпеки. Функція 1232 "Вхід до мережі" управляє процесом входження грошового модуля у мережу. Функція 1234 "Повідомлення маршруту" забезпечує послуги по пересиланню повідомлень, управління пересиланням повідомлень під час входження у систему та під час сеансу зв'язку грошового модуля. Функція 1236 "Прямий зв'язок" з банківськими службами забезпечує надання інформації про послуги, які надаються банками-учасниками. Функція 1238 "Криптографія" забезпечує функцію 1240 "Симетричний ключ" і функцію 1242 "Генератор випадкових чисел". Функція 1240 "Симетричний ключ" шифрує повідомлення між мережаним сервером 1206 і модулями, що мають доступ до мережі, а також між мережаним сервером

1206 і серверами 1184 безпеки. Функція 1242 "Генератор випадкових чисел" створює випадкові числа для шифрування ключів і перевірочних повідомлень.

У відповідності з даним винаходом перевага надається використанню ще одного безпечного процесингового компонента, модуля обслуговування клієнтів (МОК) 1192. МОК є захищеним від несанкційованого доступу пристроєм, що використовується для створення і поновлення профілів рахунків. МОК містить унікальний сертифікат, подібний сертифікатам, що містяться в грошових модулях і серверах безпеки. МОК можуть встановлювати безпечні сеанси зв'язку з іншими модулями (наприклад, з серверами безпеки). МОК вимагає центрального процесора для взаємодії з представником клієнтської служби та з інтерактивними банківськими системами.

МОК має дві основні функції. По-перше, МОК створює профілі рахунків, щоб грошовий модуль міг мати доступ до банківських рахунків, перепідтверджувати зв'язок грошового модуля з банківськими рахунками і підтверджувати номери рахунків. Ці транзакції найбільш повно описані нижче з посиланням на фіг. 18 - 20. По-друге, МОК витребує втрачені банкноти у відповідь на запит від представника клієнтської служби центрального процесора, що описано більш докладно за фіг. 21 і 22. МОК має ті ж функції безпеки, що і грошовий модуль, а також спеціальний діапазон чисел для свого ідентифікатора (див. "Схему нумерації модулів"). Виконання цих функцій модулем обслуговування клієнтів спрощує процес підтвердження номера рахунка для модуля банківського касира.

Відповідно до одного з виконань ЕГС, що використовує МОК, структура профілю рахунка для кожного банку замінюється на

```
Дата закінчення чинності (ід) М (ід) В LA
μ мок(Х) Серт (МОК)
-----X-----
де
(ід)М - ідентифікатор модуля
(ід)В - ідентифікатор банку
LA - список номерів рахунків і тип рахунка (де-
позит або позика)
М мок - підпис МОК
- конкатенація
```

Процедура підтвердження для такого профілю описана нижче з посиланням на фіг. 20.

Фіг. 4А показує функціональні компоненти модуля 1192 обслуговування клієнтів (МОК). Зовнішній інтерфейс 3000 зв'язує МОК з іншими обробляючими і комунікативними засобами в центральному процесорі модуля обслуговування клієнтів (ЦПМОК), менеджер 3001 сеансу зв'язку діє для управління транзакцією та завершення (тобто закінчення) або припинення транзакційного сеансу зв'язку між МОК і транзакційним грошовим модулем або представником клієнтської служби. Функція 3002 "Створення профілю рахунка" будує за інформацією про рахунок клієнта профіль рахунка, що дозволяє грошовому модулю мати доступ до різних банківських рахунків абонента. Функція "Ключ загального користування"

сертифікує та підписує профіль банківського рахунка. Оскільки МОК вимагає центрального процесора для взаємодії з представником клієнтської служби і інтерактивними банківськими системами, функція 3006 "Зв'язок з центральним процесором" є посередником при розподілі функцій між додатками МОК і додатками центрального процесора. Функція 3008 "Витребування втрачених банкнот" відповідає на вимоги втрачених банкнот абонента, які МОК перевіряє і розподіляє серед емісійних банків. Функція 3004 "Підтримання безпеки" веде список скомпрометованих грошових модулів, застосовується для сертифікатів, синхронізує тактування та управляє створенням нових цифрових ключів. Функції 3012 "Годинник/таймер" і 3010 "Криптографія" ідентичні таким же функціям у грошових модулях.

Фіг. 4Б показує функціональні компоненти первинного серверу 1182 безпеки. Функція 3020 "Зовнішній інтерфейс" забезпечує комунікаційний рівень для мережаної взаємодії. Функція 3002 "Менеджер сеансу зв'язку" управляє аспектами безпеки сеансу зв'язку з серверами безпеки, що розглядаються так, наче вони можуть бути скомпрометовані, і з іншими первинними серверами безпеки. Функція 3024 "Створення сертифікату" створює сертифікат для будь-якого з серверів безпеки. Функція 3026 "Розподіл сертифікаційних ключів" розподіляє серед серверів безпеки список дійсних ключів загального користування первинного серверу безпеки, складений сертифікаційним агентством. Функція 3032 "Розподіл ключів мережі безпеки" управляє ключами мережі безпеки та розподіляє їх серед первинних серверів безпеки та серверів безпеки. Функція 3030 "Встановлення глобальної пересертифікації" визначає, чи вимагається глобальна пересертифікація (наприклад, через небезпечне порушення безпеки), і, якщо це представляється необхідним, викликає глобальну пересертифікацію. Функція 3028 "Розподіл списку невірних ідентифікаторів" управляє списком невірних ідентифікаторів і розподіляє його. Функції 3034 "Годинник/таймер" і 3036 "Криптографія" ідентичні тим же функціям у грошових модулях.

Входження у мережу

Загальний огляд процедури входження у мережу описаний з посиланнями на фіг. 5. Протокол входження до системи описує ситуацію, коли модулю 1243 вимагається доступ до мережі 1198 ЕГС для пересертифікації, депонування грошей, зняття грошей або з будь-яких інших причин. Модуль 1243 може бути транзакційним грошовим модулем 1186, грошовим модулем 1188 банківського касира, модулем 1190 генератора грошей або модулем 1192 обслуговування клієнтів.

(а) Встановити зв'язок між модулем 1243 і мережним сервером 1206.

(б) Передати сертифікат модуля мережному серверу 1206.

(в) Мережаний сервер 1206 вироблює випадкове перевірочне число V і випадковий ключ K , потім мережаний сервер передає сертифікат модуля, V і K серверу 1184 безпеки (зашифрованими за допомогою ключа зв'язку мережного серверу з сервером безпеки (МС/СБ)).

(г) Модуль 1243 і сервер 1184 безпеки встано-

влюють безпечний сеанс зв'язку (за допомогою ключа зв'язку грошового модуля з сервером безпеки (ГМ/СБ)).

(д) Сервер 1184 безпеки передає час/дату, поновлений список невірних ідентифікаторів, поновлений список ключів загального користування первинного серверу безпеки, довжину ключа загального користування, глобальну пересертифікацію (якщо необхідно), і пересертифікований сертифікат модуля (якщо необхідно).

(е) Закінчити сеанс зв'язку з модулем 1243 і надіслати V і K модулю 1243.

(є) Зашифрувати V за допомогою K і надіслати мережному серверу 1206.

(ж) Мережаний сервер 1206 підтверджує модулю 1243 входження у мережу.

(з) Модуль 1243 інформує після цього мережаний сервер 1206 про адресата (якщо він є), з яким він хотів би зв'язатися.

(і) Мережаний сервер 1206 встановлює зв'язок з цим адресатом.

Вхід до мережі побудований таким чином, щоб ніхто не міг "обманути" модуль 1243 або перехопити в явному вигляді яку-небудь його інформацію. На фіг. 6 подано докладний процес входження у мережу.

Функція "Зв'язку А" встановлює зв'язок з мережею 1198 ЕГС (крок 1244). Функція "Підтримання безпеки А" надсилає мережному серверу 1206 свій сертифікат (крок 1246). Функція "Вхід до мережі МС" приймає сертифікат (крок 1248). Функція "Генератор випадкових чисел МС" виробляє випадковий ключ K і випадкове перевірочне число V (крок 1250). Функція "Симетричний ключ МС" шифрує сертифікат модуля, V і K за допомогою ключа МС/СБ (крок 1252). Ключі МС/СБ є локальними симетричними ключами, які встановлюються на мережних серверах 1206 і серверах 1184 безпеки, які пов'язуються для входження у мережу. Функція "Вхід до мережі МС" надсилає сертифікат, V і K серверу 1184 безпеки, а функція "Вхід до мережі СБ" приймає це повідомлення, а функція "Симетричний ключ СБ" дешифрує це повідомлення (кроки 1254-1258). Функція "Вхід до мережі СБ" зберігає K і V , а потім надсилає сертифікат модуля функції "Ключ загального користування СБ" для підтвердження (кроки 1260-1264). Щоб припустити можливість пересертифікації, функція "Ключ загального користування СБ" не передбачає закінчення терміну дії при визначенні дійсності сертифіката модуля.

Якщо сертифікат модуля недійсний, то функція "Вхід до мережі СБ" створює повідомлення для заборони доступу для передачі мережному серверу 1206 і модулю 1243 (крок 1266). Функція "Ключ загального користування СБ" шифрує повідомлення для модуля 1243 за допомогою ключа загального користування модуля, а функція "Менеджер сеансу зв'язку СБ" надсилає ці повідомлення мережному серверу (кроки 1268 - 1270). Функція "Вхід до мережі МС" приймає ці повідомлення та відзначає, що доступ заборонений. Зашифроване повідомлення після цього відсилається модулю, а мережаний сервер відключається (крок 1272). Функція "Менеджер сеансу зв'язку А" приймає повідомлення, функція "Ключ загального

користування А" розшифровує повідомлення, а функція "Менеджер сеансу зв'язку А" відзначає, що входження у систему було заборонене (кроки 1274 - 1278) Якщо пристрій, що запитує входження у систему, було транзакційним грошовим модулем, то функція "Зв'язок з абонентом А" інформує абонента (кроки 1280-1282) В інших випадках функція "Зв'язок з банком А" інформує банк (крок 1284)

Якщо ж, з іншого боку, сертифікат модуля дійсний, то функція "Управління списком невірних ідентифікаторів СБ" перевіряє, чи є ідентифікатор модуля в списку невірних ідентифікаторів (кроки 1286 - 1288) Якщо ідентифікатор є в цьому списку, то доступ до мережі забороняється В іншому випадку функція "Генератор випадкових чисел СБ" створює випадкове число R і перевіряє повідомлення (крок 1290) Функція "Вхід до мережі СБ" збирає R і перевіряє повідомлення в одне повідомлення, що шифрується за допомогою ключа загального користування А функцією "Ключ загального користування СБ" Функція "Ключ загального користування А" також доповнює це зашифроване повідомлення, приєднуючи до нього сертифікат серверу безпеки (кроки 1292 - 1294) Це повідомлення відсилається до А, де функція "Ключ загального користування А" розшифровує це повідомлення та перевіряє сертифікат серверу безпеки (крок 1298)

Якщо сертифікат недійсний, то А записує, що сеанс зв'язку був перерваний, та інформує абонента або банк (кроки 1304 - 1306) Якщо ж сертифікат дійсний, то функція "Підтримання безпеки А" перевіряє, чи є ідентифікатор серверу безпеки у списку невірних ідентифікаторів (кроки 1308 - 1310) Якщо ідентифікатор перебуває в цьому списку, то сеанс зв'язку переривається (кроки 1300 - 1306) Якщо ідентифікатора немає в списку, то функція "Генератор випадкових чисел А" створює випадкове число R(A) (крок 1312) Функція "Підтримання безпеки А" формує ключ (MC/СБ) сеансу зв'язку за допомогою операції Виключаюче АБО над R(A) і R і потім зберігає цей ключ сеансу зв'язку (крок 1314)

Повідомлення, що містить перевіряюче повідомлення і R (A), компонується та шифрується за допомогою ключа загального користування серверу безпеки (крок 1316) Функція "Менеджер сеансу зв'язку А" відсилає це повідомлення функції "Вхід до мережі СБ", а функція "Ключ загального користування СБ" розшифровує це повідомлення (кроки 1318 - 1322)

Функція "Вхід до мережі СБ" перевіряє, що перевіряюче повідомлення є одним з тих, які були створені нею (кроки 1324 - 1326) Якщо це не так, то сервер безпеки забороняє доступ до мережі Якщо перевіряюче повідомлення вірне, то функція "Симетричний ключ СБ" формує ключ (MC/СБ) сеансу зв'язку шляхом виконання операції Виключаюче АБО над R(A) і R (крок 1328) Функція "Менеджер сеансу зв'язку СБ" відзначає початок сеансу зв'язку та надсилає до А підтвердження про прийом за допомогою підпрограми "Посилка повідомлення" (кроки 1330 - 1332) Функція "Менеджер сеансу зв'язку А" одержує підтвердження про прийом і відзначає початок сеансу зв'язку (крок

1334)

Функція "Годинник/таймер А" відсилає значення часу і дати функції "Менеджер сеансу зв'язку", яка відправляє їх серверу безпеки (кроки 1336 - 1340) Функція "Синхронізація дати/часу СБ" приймає дату та час і перевіряє, чи знаходяться вони в межах параметру (кроки 1342 - 1344) Якщо вони поза параметром, то функція "Синхронізація дати/часу СБ" надсилає нові значення дати та часу функції "Менеджер сеансу зв'язку А" (кроки 1346 - 1350) Потім функція "Годинник/таймера А" настраює дату і час (крок 1352) Після цього А знову надсилає свої дату та час серверу безпеки для повторної перевірки Якщо спроба синхронізації годинників здійснюється більше встановленої кількості разів, то про несправність годинника повідомляється абоненту або банку, які після цього при необхідності можуть ще раз здійснити цю спробу (кроки 1354 - 1362)

Якщо ж, однак, час і дата перебувають в межах параметра, то функція "Вхід до мережі СБ" компонує повідомлення, що має список невірних ідентифікаторів, новий список ключів загального користування первинного серверу безпеки (який беруть у функції "Розповсюдження сертифікаційних ключів") і довжину ключа загального користування (розмір ключів загального користування періодично змінюється) (крок 1364) Функція "Створення сертифіката СБ" перевіряє, чи була призначена глобальна пересертифікація, та встановлює, що період часу для глобальної пересертифікації ще не вичерпано (кроки 1366 - 1368) Такий період часу повинен бути достатнім, щоб кожний сертифікат був пересертифікований або прострочений Ця функція повинна також перевіряти, коли модуль був останній раз пересертифікований, оскільки якщо він був сертифікований у період глобальної пересертифікації, то не буде потреби пересертифікувати його знов

При необхідності пересертифікації функція "Створення сертифіката СБ" додає до попереднього повідомлення "модуль потрібно пересертифікувати" (крок 1370) Після цього, незалежно від того, викликана пересертифікація чи ні, функція "Ключ загального користування СБ" підписує повідомлення (крок 1372) Повідомлення відсилається до А, де функція "Ключ загального користування А" перевіряє цифровий підпис на повідомленні (кроки 1374 - 1378) Якщо підпис недійсний, то сеанс зв'язку переривається Функція "Підтримання безпеки А" після цього поновлює свій список невірних ідентифікаторів, список ключів загального користування та довжину ключа (крок 1382)

Після цього модуль А перевіряє, чи вимагається пересертифікація його сертифіката (або внаслідок команди щодо глобальної пересертифікації, або внаслідок того, що сертифікат прострочено) (кроки 1384 - 1386) Якщо потрібний новий сертифікат, то функція "Підтримання безпеки А" ініціює створення нового сертифіката (крок 1388) Функція "Ключ загального користування А" виробляє нові ключі та підписує новий ключ загального користування своїм старим приватним ключем (крок 1390) Функція "Менеджер сеансу зв'язку А" надсилає підписаний новий ключ до функції

"Створення сертифіката СБ" (кроки 1392 - 1396) Після цього функція "Ключ загального користування СБ" перевіряє підпис на новому ключі загального користування (кроки 1398 - 1400) Якщо підпис недійсний, сервер безпеки забороняє доступ до мережі Якщо підпис дійсний, то функція "Ключ загального користування СБ" підписує новий сертифікат модуля і відсилає його модулю (крок 1402) Функція "Менеджер сеансу зв'язку А" приймає сертифікат, функція "Підтримання безпеки А" перевіряє сертифікат, а функція "Ключ загального користування А" перевіряє підпис (кроки 1404 - 1410)

Якщо сертифікат недійсний, то функція "Менеджер сеансу зв'язку А" надсилає серверу безпеки повідомлення "Сертифікат недійсний" та сертифікат за допомогою функції "Посилка повідомлення" (кроки 1412 - 1413)

Функція "Вхід до мережі СБ" приймає повідомлення, а функція "Ключ загального користування СБ" перевіряє підпис (кроки 1414 - 1418) Якщо сервер безпеки відзначає, що сертифікат насправді дійсний, то він забороняє модулю доступ до мережі Якщо ж, однак, сертифікат недійсний, то функція "Менеджер сеансу зв'язку СБ" інформує мережаний сервер про те, що він відключиться від мережі (крок 1420) Функція "Вхід до мережі МС" інформує модуль про несправність (крок 1422) Після цього модуль надсилає запит абоненту або банку на повтор спроби (кроки 1424 - 1432)

Якщо ж, з іншого боку, модуль відзначає, що його новий сертифікат дійсний, то функція "Менеджер сеансу зв'язку А" надсилає підтвердження про прийом серверу безпеки (крок 1434) Аналогічно до цього, якщо не вимагався новий сертифікат, функція "Підтримання безпеки А" надсилає підтверджувальне повідомлення серверу безпеки (кроки 1436 - 1438) У будь-якому випадку функція "Менеджер сеансу зв'язку СБ" приймає підтвердження про прийом і відмічає кінець свого сеансу зв'язку з модулем (крок 1440) Потім функція "Вхід до мережі СБ" надсилає К та V до А (кроки 1442 - 1444) Функція "Менеджер сеансу зв'язку А" приймає це повідомлення, а функція "Симетричний ключ А" шифрує V та адресата за допомогою К і надсилає це повідомлення мережаному серверу (кроки 1446 - 1448) Функція "Вхід до мережі МС" приймає повідомлення, а функція "Симетричний ключ МС" розшифровує це повідомлення та перевіряє, чи є V тим же самим V, що було сформоване раніше (кроки 1450 - 1454)

Якщо V невірне, то функція "Вхід до мережі МС" відсилає до А повідомлення про відмову входження у систему і після цього роз'єднується (кроки 1456 - 1458) Якщо V правильне, то функція "Вхід до мережі МС" встановлює зв'язок з адресатом і надсилає до А підтвердження прийому (крок 1460) І, зрештою, функція "Менеджер сеансу зв'язку А" приймає підтвердження про прийом і відмічає, що А увійшов у мережу 1198 ЕГС (крок 1462)

Встановлення сеансу зв'язку

На фіг 7 показано протокол встановлення сеансу зв'язку Функція "Підтримання безпеки А" надсилає сертифікат модуля менеджеру сеансу зв'язку, а функція "Менеджер

сеансу зв'язку А" приймає сертифікат і переві-

ряє, чи з'єднаний з мережею грошовий модуль А (кроки 1464 - 1466) Якщо грошовий модуль А не підключено до мережі, то функція "Менеджер сеансу зв'язку А" відсилає сертифікат, отриманий від функції "Підтримання безпеки А", адресату В (крок 1476)

Альтернативно, якщо грошовий модуль А підключено до мережі, то функція "Симетричний ключ А" шифрує сертифікат за допомогою К, а функція "Менеджер сеансу зв'язку А" надсилає зашифрований сертифікат мережаному серверу (кроки 1468 - 1472) Мережаний сервер розшифровує сертифікат за допомогою К і надсилає сертифікат адресату В

Незалежно від того, чи був сертифікат відправлений мережним сервером або менеджером сеансу зв'язку А, функція "Менеджер сеансу зв'язку В" приймає сертифікат, а функція "Підтримання безпеки В" (якщо В є сервером безпеки, то ця функція реалізується менеджером сеансу зв'язку) перевіряє дійсність сертифіката (кроки 1480 - 1484) Якщо сертифікат недійсний, то функція "Менеджер сеансу зв'язку В" відзначає, що сеанс зв'язку перервано, та інформує абонента або банк (кроки 1486 - 1492) (якщо В є сервером безпеки, то В просто відзначає, що транзакцію перервано)

Якщо сертифікат дійсний, то функція "Підтримання безпеки В" перевіряє, чи перебуває А в списку невірних ідентифікаторів (кроки 1494 - 1496) Якщо А перебуває в цьому списку, то сеанс зв'язку переривається Якщо А немає в списку, то функція "Генератор випадкових чисел В" створює випадкове число R(B) і перевіряє повідомлення В (крок 1498) Функція "Годинник/Таймер В" запрошує дату та час (крок 1500) Функція "Підтримання безпеки В" компонує в одне повідомлення R(B), перевіряє повідомлення В, час і дату (крок 1502) Функція "Ключ загального користування В" шифрує це повідомлення за допомогою ключа загального користування А, а функція "Менеджер сеансу зв'язку В" приєднує до зашифрованого повідомлення сертифікат В і надсилає це повідомлення до А (кроки 1504 - 1506)

Функція "Менеджер сеансу зв'язку А" приймає це повідомлення, функція "Ключ загального користування А" розшифровує зашифровану частину повідомлення, а функція "Підтримання безпеки А" перевіряє сертифікат В (кроки 1508 - 1514) Якщо сертифікат недійсний, то функція "Менеджер сеансу зв'язку А" відзначає, що сеанс зв'язку перерваний, і інформує абонента або банк (кроки 1516 - 1522) Якщо сертифікат дійсний, то функція "Підтримання безпеки А" перевіряє, чи перебуває В у списку невірних ідентифікаторів (кроки 1524 - 1526) Якщо В перебуває в цьому списку, то сеанс зв'язку переривається Якщо В немає в списку, то функція "Підтримання безпеки А" затребує дату та час і порівнює їх з датою та часом В (кроки 1528 - 1530) Якщо дата та час перебувають поза діапазоном, то сеанс зв'язку переривається

Якщо ж дата та час перебувають у встановлених межах, то функція "Генератор

випадкових чисел А" створює випадкове число R (A) і перевіряє повідомлення А (крок 1532) Функція "Підтримання безпеки А" після цього формує ключ сеансу зв'язку за допомогою операції

Виключаюче АБО над R(A) та R(B) (крок 1534) Перевірочне повідомлення A, перевірочне повідомлення B, час, дата та R(A) компонуються в одне повідомлення та шифруються за допомогою ключа загального користування B (крок 1536) Це повідомлення надсилається до B функцією "Менеджер сеансу зв'язку A" (крок 1538) Функція "Менеджер сеансу зв'язку B" приймає це повідомлення, функція "Ключ загального користування B" розшифровує повідомлення, а функція "Підтримання безпеки B" перевіряє перевірочне повідомлення B (кроки 1540 - 1546) Якщо перевірочне повідомлення B невірне, то сеанс зв'язку переривається Якщо перевірочне повідомлення B вірне, то функція "Підтримання безпеки B" формує ключ сеансу зв'язку за допомогою операції Виключаюче АБО над R(A) і R(B) (крок 1548) Після цього затребуються значення часу та дати, які порівнюються з часом і датою A для перевірки того, чи знаходяться вони один відносно одного в заздалегідь заданому діапазоні (крок 1550) Якщо час і дата поза цим діапазоном, сеанс зв'язку переривається Якщо час і дата в цьому діапазоні, то функція "Менеджер сеансу зв'язку B" відмічає початок сеансу зв'язку (крок 1552)

Після цього функція "Менеджер сеансу зв'язку B" надсилає до A підтвердження про прийом і перевірочне повідомлення A (кроки 1554 - 1556) Функція "Менеджер сеансу зв'язку A" приймає повідомлення, а функція "Підтримання безпеки A" перевіряє перевірочне повідомлення A (кроки 1558 - 1562) Якщо перевірочне повідомлення невірне, то сеанс зв'язку переривається Якщо же перевірочне повідомлення вірне, то функція "Менеджер сеансу зв'язку A" відмічає початок сеансу зв'язку (крок 1564)

Передача банкнот

На фіг. 8 показано протокол передачі банкнот Функція "Каталог банкнот X" вибирає банкноту(и) і суми для передачі, поновлює суми та порядкові номери банкнот, а після цього надсилає повідомлення функції "Банкноти" (крок 1566) Можливими завданнями у виборі банкнот для передачі можуть бути, наприклад (1) мінімізація кількості цифрових підписів (які вимагають певного часу на обробку), (2) мінімізація розміру пакета, (3) максимізація придатності електронних банкнот, що залишилися у абонента, який передає (тобто передача банкнот, до закінчення терміну дії яких залишилися найменша кількість часу) Ці завдання можуть бути вирішені за допомогою наступного алгоритму передачі банкнот (1) визначити всі можливі альтернативи, що містять мінімальну кількість банкнот, (2) визначити, які з цих альтернатив мають найменше число передач, (3) якщо з кроку 2 виходить більше одного вибору, то обрати той, в якому найменше число банкнотоднів "Банкнотодні" є остаточною значенням банкноти, що передається, помноженим на кількість днів, що залишилися до терміну закінчення дії банкноти, просумоване за всіма банкнотами у пакеті

Функція "Банкноти X" після одержання повідомлення від функції "Каталог банкнот X"

створює трансферт, доданий до кожної банкноти, що передається (крок 1568) Функція "Ключ загального користування X" створює підписи для

банкнот(и) (крок 1570) Функція "Менеджер пакета X" потім komponує банкноти та їх нові трансферти та підписи в пакет і надсилає пакет до Y (кроки 1572 - 1574) Функція "Менеджер пакета Y" приймає пакет і розбирає його (крок 1576)

Функція "Перевірка Y" перевіряє справжність всіх сертифікатів в банкнот(ах) (наприклад, сертифікат генератора грошей і всі сертифікати трансфертів) Після цього функція "Перевірка Y" перевіряє, щоб всі ідентифікаційні номери в трансфертній групі збігалися з ідентифікаційними номерами сертифікатів модуля в групі підписів і сертифікатів протягом усієї історії електронної банкноти Підтверджується також відповідність трансфертних сум для кожної банкноти встановленням того, що протягом всієї історії електронної банкноти сума, передана при кожній наступній передачі, є меншою від суми при передачі, що безпосередньо їй передувало Крім того, перевіряється відповідність переданої суми очікуваній сумі (кроки 1578 - 1580) Якщо такої відповідності немає, то транзакція переривається (крок 1582)

Якщо відповідність є, а Y є транзакційним грошовим модулем, то функція "Перевірка Y" перевіряє терміни дії банкнот(и) (кроки 1584 - 1588) Якщо будь-яка з банкнот є простроченою, то транзакція припиняється Якщо ж жодна не прострочена, то функція "Перевірка Y" звіряє кожний ідентифікатор з трансфертів банкноти зі списком невірних ідентифікаторів (кроки 1590 - 1592) Якщо хоча б один з ідентифікаторів трансфертів перебуває в списку невірних ідентифікаторів, то транзакція переривається

Якщо ідентифікаторів трансфертів немає в списку невірних ідентифікаторів (або Y не є транзакційним грошовим модулем), то функція "Ключ загального користування Y" перевіряє дійсність підписів банкнот(и) (кроки 1594 - 1596) Якщо будь-який з підписів недійсний, то транзакція припиняється Якщо підписи дійсні, то функція "Перевірка Y" перевіряє, чи збігаються тіла банкнот з тілами банкнот, що зберігаються в додатку "Банкноти" або розміщеними в "Журналі транзакцій" (кроки 1598 - 1600) Для кожного тіла банкноти, що збігається, створюється дерево передач банкноти для того, щоб визначити, чи відбувалося дублювання банкноти (кроки 1602 - 1604) Якщо будь-яка з банкнот була дубльована, транзакція припиняється Ця перевірка на дублювання (тобто кроки 1598 - 1604) зокрема спрямована проти тих, хто намагається створювати гроші шляхом передач банкнот самим собі за допомогою скомпрометованого грошового модуля

Якщо дублювань немає або якщо не було ідентифіковано збігу тіл банкнот, функція "Банкноти Y" вмищує банкноту(и) до утримувача грошей (крок 1606) І, нарешті, функція "Каталог банкнот X" поновлює місцезнаходження та значення банкнот, а також ініціалізує порядковий номер(и) (крок 1608)

Зрозуміло, що процес передачі банкнот містить кроки поновлення та ініціалізації

порядкового номера для спрощення узгодження банкноти (див. "Узгодження емітованих грошей"), перевірки, чи не перебуває приймаюча сторона в списку невірних ідентифікаторів, і перевірки на дублювання банкнот Ці додаткові ознаки та

кроки ускладнюють уведення та обіг дубльованих банкнот і підвищують здатність фіксувати дубльовані банкноти, які перебувають в обігу

Обмін іноземної валюти

На фіг 9 показано протокол транзакції для обміну іноземної валюти на прикладі доларів і фунтів. Початкове A дає згоду B обміняти долари (\$)

на фунти (\pounds) за обмінним курсом $\$/\pounds$ (крок 1602). Після цього A і B входять до своїх грошових модулів, і модулі запрошують своїх абонентів увести тип транзакції (кроки 1604 - 1610). A обирає покупку іноземної валюти, а B обирає відповідно продаж (кроки 1612 - 1614). Після цього A і B встановлюють безпечний транзакційний сеанс зв'язку (кроки 1616 - 1620).

Функція "Зв'язок з абонентом A " запитує власника/утримувача A про суму в доларах, яку він бажає обміняти (крок 1622). Функція "Платіж/обмін A " приймає суму, а функція "Каталог банкнот A " перевіряє, чи має A достатньо коштів (кроки 1624 - 1628). Якщо коштів недостатньо, то функція "Зв'язок з абонентом A " запитує нову суму, яка знов зв'язується з наявними коштами (кроки 1630 - 1632). Якщо нова сума не задана, то транзакція переривається (крок 1634).

Якщо коштів достатньо, то функція "Платіж/обмін A " надсилає суму в доларах до B (кроки 1636 - 1638). Функція "Зв'язок з абонентом B " пропонує власнику/утримувачу B обрати або суму в фунтах, яку він хоче обміняти на долари, або просто обмінний курс для доларів (крок 1640). Функція "Каталог банкнот B " перевіряє наявність достатніх коштів (кроки 1642 - 1644). Якщо коштів недостатньо, то функція "Зв'язок з абонентом B " запитує новий курс і знову зв'язує наявність коштів (кроки 1646 - 1648). Якщо ж, однак, не обрано жодного нового курсу, то функція "Платіж/обмін B " інформує A про нестачу коштів (кроки 1650 - 1652). Після цього A може вибрати нову суму для обміну або припинити транзакцію (кроки 1630 - 1634).

Якщо B має достатньо коштів для транзакції, то функція "Платіж/обмін B " надсилає до A повідомлення та суму в фунтах для обміну (також надсилається еквівалентний курс) (кроки 1654 - 1656). Функція "Зв'язок з абонентом A " пропонує перевірити суму в фунтах та курс (кроки 1658 - 1660). Якщо сума і курс невірні, то функція "Платіж/обмін A " інформує B , що сума і курс невірні (кроки 1662 - 1664). Після цього функція "Зв'язок з абонентом B " запитує новий курс (кроки 1666 - 1668). Якщо не обрано жодного нового курсу, то транзакція припиняється (крок 1670).

Якщо ж, однак, A упевнений у вірності суми та курсу, то функція "Платіж/обмін A " передає суму в доларах утримувачу грошей (крок 1672). Після цього доларові банкноти передаються від A до B (крок 1674). Функція "Платіж/обмін B " передає суму в фунтах своєму утримувачу грошей (крок 1676). Після цього фунтові банкноти передаються від B до A (крок 1678).

У цей момент транзакції як A , так і B умовно мають вірні суми іноземних банкнот. Кожний з A і B узяв участь у двох трансфертах: трансферти A (1) A передав долари B , (2) A прийняв фунти від B , трансферти B (1) B передав фунти A , (2) B прийняв

як долари від A . Для завершення транзакції обміну валюти A в цей момент повинен зафіксувати (тобто закінчити і записати постійно в своєму журналі транзакцій) обидва своїх трансферти. Так само B повинен зафіксувати обидва своїх трансферти. Слід відзначити, що A може здійснювати трансферти обміну валюти $A \rightarrow B$ (долари від A до B) і $B \rightarrow A$ (фунти від B до A) окремо. Так само і B може здійснювати трансферти обміну валюти $A \rightarrow B$ і $B \rightarrow A$ окремо.

Наступна частина протоколу обміну валюти побудована так, щоб жодна з сторін не знала про порядок, за яким грошові модулі будуть фіксувати транзакцію. Така невизначеність перешкодить навмисним спробам будь-якої з сторін здійснити шахрайство. За основу береться функція $S(X)$, яка визначається як $S(0) = A$ і $S(1) = B$, де A і B відповідають грошовим модулям A і B . Таким чином, якщо X обирається випадково з 0 і 1, то випадково позначаються грошові модулі A і B .

Наступна процедура використовується з тією метою, щоб дозволити A і B спільно встановити випадковий X . $R(A)$ і $R(B)$ є випадковими числами, виробленими A і B відповідно під час підпрограми "Встановлення сеансу зв'язку". Визначається парність операції Виключаюче АБО від $R(A)$ і $R(B)$ (за допомогою виконання операції Виключаюче АБО для всіх розрядів " $R(A)$ Виключаюче АБО $R(B)$ ").

Ця парність є випадковим числом X . $\overline{X^*}$ є доповненням $X(\overline{X^*} = X$ Виключаюче АБО 1).

Як показано на фіг 9, функція "Журнал транзакцій A " умовно оновлює свій Журнал транзакцій

для запису трансферту $S(X)$ в $S(\overline{X^*})$ (крок 1680). Якщо X розраховується як 0, то умовно записується трансферт A в B (тобто передача доларів). Якщо X розраховується як 1, то умовно записується трансферт B в A (тобто передача фунтів). Оскільки записи умовні, то журнал може бути повернутий до вихідний стану у випадку, якщо грошовий модуль A припинить транзакцію. Зміни в журналі стають постійними, як тільки зміни будуть проголошені безумовними (або відповідно до того, як явно показано на блок-схемі алгоритму, або неявно під час фіксації). Після цього функція "Менеджер сеансу зв'язку A " надсилає до B повідомлення "Журнал поновлено" (кроки 1682 - 1684). У відповідь функція "Журнал транзакцій B " також умовно поновлює свій журнал для запису транс-

ферту $S(X)$ в $S(\overline{X^*})$ (крок 1686).

Якщо $X = 1$, то функція "Журнал транзакцій B " оголошує зміни в журналі безумовними (кроки 1688 - 1690). Таким чином, у цей момент B здійснив свій трансферт передачі фунтів A . Далі B дотримується протоколу фіксації (крок 1692), описаному нижче з посиланням на фіг 41. У цій ситуації A здійснить обидва своїх трансферти (тобто передачу доларів і отримання фунтів), а B здійснить один свій невиконаний (незафіксований) трансферт, а саме отримання доларів.

Якщо ж, однак, $X = 0$ (крок 1688), то функція "Менеджер сеансу зв'язку B " надсилає до A повідомлення "Розпочати фіксацію" (кроки 1694 - 1696). Після цього функція "Журнал транзакцій A " оголо-

шує зміни в своєму журналі безумовними (крок 1698), фіксує таким чином свій трансферт передачі доларів. Після цього викликається протокол фіксації за фіг. 41 (крок 1700). Під час виконання цього протоколу (описаного нижче), В фіксує обидва свої трансферти (тобто передачу фунтів і отримання доларів), а А фіксує один свій невиконаний трансферт, а саме отримання фунтів.

Як можна побачити, при транзакції "Обмін іноземної валюти" фіксується кожна передача банкнот, завдяки цьому банкноти охороняються від дублювання, що могло б відбутися у випадку тільки однієї фіксації. Протокол обміну валюти гарантує, що жодна з сторін не знає, чий трансферт (передача доларів до А або передача фунтів до В) буде зафіксовано першим. Це зменшує стимул будь-якої з сторін до шахрайства. Кожна передача фіксується окремо, але порядок фіксацій обирається двома модулями випадковим чином. Сторона, що намагається втрутитися в транзакцію, має шанси 50-50 втратити гроші. Немає також сенсу втручатися до процесу фіксації, оскільки втрачені гроші можуть бути витребовані (див. "Витребування втрачених грошей").

Фіксація

На фіг. 10 показано протокол фіксації для модулей. Функція "Менеджер сеансу зв'язку Х" надсилає до У повідомлення "Готовий до фіксації" (кроки 1702 - 1704). Це повідомлення зобов'язує модуль, який його прийняв, зафіксувати транзакцію. У звичайному процесі передачі грошей така технологія передачі обов'язку фіксації першим використовується для гарантії того, що сторона, яка передає гроші, фіксує транзакцію першою, тим самим виключаючи можливість дублювання грошей.

Після цього функція "Менеджер сеансу зв'язку У" надсилає до Х підтвердження про прийом (кроки 1706 - 1708) і фіксує всі невиконані транзакції поновленням свого журналу транзакцій (крок 1710). Крім того, якщо У є грошовим модулем транзакцій, то функція "Зв'язок з абонентом У" повідомляє абоненту про успішну транзакцію (кроки 1712 - 1714). Після цього функція "Менеджер сеансу зв'язку У" записує кінець сеансу зв'язку (крок 1716).

Функція "Журнал транзакцій Х" приймає підтвердження про прийом від У і поновлює свій журнал транзакцій, фіксуючи таким чином всі невиконані трансферти. Х завершує свою фіксацію таким же чином, що і У (кроки 1718 - 1724).

Переривання транзакції

На фіг. 11 показано протокол "Переривання транзакції" для модулей. Функція "Менеджер сеансу зв'язку Х" скасовує зміни і відзначає, що транзакцію перервано (крок 1726). Після цього функція "Менеджер сеансу зв'язку Х" перевіряє, чи було відправлено повідомлення "Готовий до фіксації" (кроки 1728 - 1730). Якщо повідомлення було відправлено, то Х поновлює свій журнал транзакцій (крок 1732), записуючи, що Х перервав транзакцію після відправлення повідомлення про готовність до фіксації, та записуючи ідентифікатори банкнот і номінали всіх банкнот, отриманих протягом протоколу передачі банкнот. Таким чином, протокол переривання реєструє інформацію, коли протягом

невдалого виконання підпрограми фіксації викликається підпрограма "Припинення".

Якщо Х є транзакційним грошовим модулем 1186 і було відправлено повідомлення про готовність до фіксації, то функція "Зв'язок з абонентом Х" інформує свого абонента, що транзакція була перервана і що могла бути помилка передачі грошей (кроки 1734 - 1738).

Якщо Х є грошовим модулем 1188 банківського касира, то функція "Зв'язок з банком Х" інформує банк, що він повинен скасувати свої транзакції, пов'язані з веденням рахунків (за допомогою відповідних дебетів і кредитів) (кроки 1740 - 1742). Якщо Х є транзакційним грошовим модулем 1186 і не було відіслано повідомлення про готовність до фіксації, то функція "Зв'язок з абонентом Х" інформує абонента, що транзакція була перервана (крок 1744).

У будь-якому випадку функція "Менеджер сеансу зв'язку Х" надсилає до У повідомлення про те, що транзакція не може бути завершена (кроки 1746 - 1748). Функція "Менеджер сеансу зв'язку У" скасовує свої зміни і відзначає, що транзакція перервана (крок 1750). Після цього У інформує свого абонента, що транзакція перервана (кроки 1752 - 1754), або інформує банк про необхідність скасувати транзакції, пов'язані з веденням рахунків (кроки 1756 - 1758).

Як описано вище, якщо транзакція переривається під час протоколу фіксації, то виникає можливість втрати банкнот. Якщо це відбувається, то одержувач припинить транзакцію, а той, хто передає, виконає передачу банкнот. У цьому випадку грошовий модуль одержувача записує інформацію про банкноти, які він повинен був отримати, і повідомляє абоненту, що існує потенційна проблема (тобто що він не отримав банкноти, відіслані від А). Необхідно відзначити, що в цих умовах до тих пір, поки грошовий модуль того, хто передає, є задіяним, він правильно передає банкноти.

Абонент грошового модуля одержувача може після цього подати вимогу про гроші до сертифікаційного агентства. Вимога буде містити журнальний запис невдалої транзакції. Після цього сертифікаційне агентство може перевірити за допомогою банків-емітентів, чи були банкноти узгоджені. Через деякий час, якщо банкноти не були узгоджені, абонент може знов затребувати свої гроші.

Платіж у пункті продажу

На фіг. 12 показано протокол "Платіж у пункті продажу". Протокол "Платіж у пункті продажу" застосовується для спрощення платежів, що виконуються між грошовим модулем 1186 транзакцій покупця та грошовим модулем 1186 транзакцій продавця. Грошовий модуль 1186 транзакцій продавця може бути, наприклад, розміщений у касовому апараті супермаркету.

Спочатку А дає згоду на придбання товарів або послуг у В (крок 1760). Власник/утримувач грошового модуля А транзакцій ставить підпис на своєму грошовому модулі (крок 1762). Функція "Зв'язок з абонентом А" запитує у власника/користувача транзакцію, а А обирає виконання платежу в пункті продажу (кроки 1764 - 1766). У той же час продавець визначає загальну ціну по-

купки (крок 1768) Функція "Зв'язок з абонентом В" запитує транзакцію, а В обирає отримання платежу в пункті продажу (кроки 1770 - 1772) Після цього А і В встановлюють безпечний сеанс зв'язку (кроки 1774 - 1776)

Функція "Зв'язок з абонентом В" повідомляє суму платежу, а функція "Платіж/обмін В" приймає суму і надсилає її до А (кроки 1778 - 1782) Після цього функція "Зв'язок з абонентом А" надсилає запит своєму абоненту перевірити необхідну суму (кроки 1784 - 1786) Більш того, абонента просять обрати банкноти, якими він буде платити (наприклад, готівкою або в кредит) та їхню кількість, щоб підсумок дорівнював необхідній сумі Якщо сума, що вимагається, невірна, то функція "Платіж/обмін А" надсилає В повідомлення, яке вказує на те, що потрібна сума є невірною (кроки 1788 - 1790) Після цього функція "Зв'язок з абонентом В" запитує у свого господаря нову суму (кроки 1792 - 1794) Якщо нова сума не обрана, то транзакція переривається (крок 1796)

Якщо потрібна сума вірна, то функція "Платіж/обмін А" приймає суми в залежності від типів банкнот (крок 1798) Після цього функція "Управління банкнотами А" перевіряє наявність достатніх коштів (кроки 1800 - 1802) Якщо коштів недостатньо, то функція "Зв'язок з абонентом А" запитує нові суми в залежності від типів банкнот (кроки 1804-1806) Якщо , нова сума не задана, то функція "Платіж/обмін А" надсилає до В повідомлення, що коштів А не достить (кроки 1808, 1790) Функція "Зв'язок з абонентом В" запитує у свого господаря нову суму (кроки 1792 - 1794) Якщо не обрано жодної нової суми, то транзакція переривається (кроки 1798) Якщо обрана нова сума, то транзакція платежу починається знову

Якщо коштів досить, то функція "Платіж/обмін А" передає суму утримувачу грошей (крок 1810) Після цього банкноти передаються від А до В (крок 1812) І, нарешті, грошові транзакційні модулі фіксують транзакцію (крок 1814)

Таким чином, платіж у пункті продажу спрощено для покупця, оскільки він є платежем, який ініціалізується одержувачем платежу Звичайно платіж у пункті продажу використовується для оплати продавцям за товари, у той час, як плата абонента абоненту використовується для оплати приватним особам або для оплати рахунків

Поновлення кредиту від емісійного банку

Фіг 13 показує протокол транзакції "Поновлення кредиту від емісійного банку", і, зокрема, описує, як абонент купує кредитну банкноту, що є засобом заздалегідь санкційованого кредитного платежу Абонент може мати не більше однієї кредитної банкноти для кожного кредитного рахунка, яким він володіє Слід відзначити, що кожний банк, який дозволяє абоненту одержувати оновлені кредитні банкноти, є емісійним банком для цих кредитних банкнот

Процес транзакції поновлення кредиту починається з процесу "Встановлення кредиту" між грошовим модулем А і грошовим модулем В банківського касира (крок 1854), який далі описується з посиланням на фіг 14 Встановлення кредиту

Процес "Встановлення зняття кредиту" починається, коли власник/утримувач транзакційного

грошового модуля А вирішує зробити поновлення кредиту і, таким чином, ставить підпис на своєму грошовому модулі (крок 1876) Наприклад, абонент А може мати кредитну банкноту, але бажає змінити (тобто збільшити або зменшити) суму кредиту, у тому числі зменшити суму до нуля, або може у даний момент не мати кредитної банкноти, але бажає придбати її Функція "Зв'язок з абонентом А" повідомляє власнику/утримувачу про транзакцію, а А обирає поновлення кредиту певної суми, отриманого від певного банку на певному рахунку (кроки 1878 - 1880) У даному виконанні сума поновлення кредиту, що визначається абонентом А, є загальною сумою кредиту, яку хоче мати абонент А Після цього транзакційний грошовий модуль А ініціює процедуру зв'язку з банком, який було обрано, входженням до мережі за допомогою процедури "Вхід до мережі", описаної вище (крок 1882)

Після того, як кроки підписання грошового модуля, вибору транзакції та входження до мережі виконані, А і В встановлюють безпечний сеанс зв'язку (крок 1884) Після цього транзакційний грошовий модуль А робить кредитний запит грошовому модулю В банківського касира (крок 1886), відповідно до процедури "Запит кредиту", яка повніше описана з посиланням на фіг 15

Запит кредиту

За фіг 15 буде описано процес запитування кредиту Слід відзначити, що хоча на кресленнях сторони позначені як "Х" і "У" у кроках процесу, які описано нижче, це можна застосувати до будь-якого грошового модуля, що вступає в транзакцію з грошовим модулем банківського касира

Спочатку, якщо на обраному рахунку є кредитна банкнота, функція "Каталог банкнот Х" відсилає суму цієї кредитної банкноти функції "Зв'язок з банківським касиром Х" (крок 1897) Функція "Зв'язок з банківським касиром Х" визначає різницю між загальною сумою кредиту, що запитується абонентом А, і сумою кредитної банкноти та надсилає запит на поновлення кредиту грошовому модулю банківського касира, запитуючи санкцію певної суми кредиту з певного рахунка При передачі запиту на поновлення кредиту від грошового модуля, який запитує, грошовому модулю банківського касира разом із сумою кредиту будуть передані номер рахунка та профіль рахунка (крок 1898) Це повідомлення надсилається відповідно до протоколу відправлення повідомлень (крок 1900), в якому повідомлення шифрується за допомогою описаних методів шифрування

Коли запит на зняття кредиту, а також номер рахунка і профіль рахунка передаються грошовому модулю банківського касира, ініціалізується процедура перевірки вірогідності номера рахунка (крок 1902) Функціональна схема, що показує, як перевіряється вірогідність номера рахунка, наведена на фіг 20, яка докладно описана нижче, щоб було зрозуміліше

Поряд з перевіркою вірогідності інформації про рахунок, функція "Зв'язок з банком У" перевіряє наявність достатніх кредитних засобів для задоволення суми запиту на поновлення кредиту (крок 1904) Достатні кредитні засоби підкажуть функції "Зв'язок з транзакційним модулем У" наді-

слати повідомлення до Х, який одержує повідомлення через свою прикладну функцію "Зв'язок з банківським касиром" (кроки 1908 - 1912)

Недостатня сума кредиту, однак, викличе підказку абоненту ввести нову суму для , поновлення кредиту (кроки 1914 - 1918, фіг 15Б) Уведення абонентом нової суми для поновлення кредиту дасть в результаті відправлення функцією "Зв'язок з банківським касиром" нової суми кредиту додатку "Зв'язок з банком" грошового модуля банківського касира для перевірки наявності достатніх коштів для покриття останньої запрошеної суми - (кроки 1922 - 1924), з поверненням на крок 1904 за фіг 15А Якщо абонент не запросив нову суму, транзакція переривається (крок 1926)

За фіг 14, після виходу з процесу запиту зняття кредиту, функція "Зв'язок з банківським касиром А" викликає передачу всіх наявних банкнот, кредитних банкнот, які були передані (тобто кредитних банкнот, отриманих при попередніх транзакціях) і кредитної банкноти для рахунка грошовому модулю банківського касира (крок 1888) Якщо в транзакційному грошовому модулі не було банкнот в той час, як відбувся запит зняття кредиту, додаток "Зв'язок з банківським касиром А" надсилає грошовому модулю банківського касира повідомлення, що банкноти відсутні (кроки 1892 - 1894) Якщо в транзакційному грошовому модулі були банкноти, то електронні банкноти передаються від А до банківського касира В відповідно до процедури передачі банкнот, яка описана вище з посиланням на фіг 8 (крок 1896)

За фіг 13, функція "Зв'язок з транзакційним модулем В" перевіряє, чи були передані будь-які готівкові банкноти і кредитні банкноти, що були передані (кроки 1856 - 1858), і якщо будь-які банкноти цих типів справді були передані транзакційним грошовим модулем А, то виконані з рахунками транзакції заносяться до бухгалтерської книги додатком "Зв'язок з банком В", щоб відобразити цю ситуацію (крок 1860) Як у випадку, коли грошовий модуль не передавав банкноти, так і після запису транзакцій на кроці 1860, між грошовим модулем банківського касира та модулем генератора грошей встановлюється сеанс зв'язку (крок 1862) Функція "Зв'язок з банком В" оновлює кредитну лінію додаванням суми кредитної банкноти (якщо така є) до лінії доступного кредиту для отримання сумарного доступного кредиту та відрахування кредитної суми, яка запитується, з сумарного доступного кредиту Якщо не повинні створюватися банкноти (у тому числі готівкові банкноти та кредитні банкноти),

оскільки кредитна сума, що запитувалась, дорівнювала нулю і готівкові банкноти не передавалися, то грошові модулі закінчать транзакцію відповідно до процедури фіксації, яка описана вище з посиланням на фіг 10 (кроки 1865 - 1875)

Якщо, однак, повинні створюватися які-небудь банкноти (готівкові або кредитні) через ненульову суму кредитного запиту і/або через передачу готівкових банкнот, то банкноти запитуються банківським касиром В у модуля генератора грошей відповідно до процедури запиту банкнот (кроки 1865 - 1866) Банкноти, які запитуються у модуля генератора грошей, передаються грошовому модулю В

банківського касира за допомогою описаного вище процесу передачі банкнот (див фіг 8) для передачі електронних банкнот (крок 1868) Після цього ці банкноти передаються від грошового модуля В банківського касира транзакційному грошовому модулю за допомогою того ж самого процесу передачі банкнот (крок 1870) Нарешті, для успішного завершення процедури поновлення кредиту грошові модулі закінчать транзакцію відповідно до процедури фіксації, описаної вище з посиланням на фіг 10 Процес фіксації спочатку ініціалізується транзакційним грошовим модулем, який фіксує свою транзакцію з грошовим модулем В банківського касира (крок 1872) Після цього процес фіксації виконується між грошовим модулем В банківського касира і модулем генератора грошей (крок 1874) Цим завершується процес повного поновлення кредиту від емісійного банку

Узгодження емітованих грошей

Процес узгодження банкноти перевіряє підробку та дублювання банкноти і описується з посиланням на фіг 16 і фіг 17 Система "Узгодження емітованих грошей", основана на інформації, що зберігається в файлі "Емітовані гроші", будує дерево передачі банкноти, яке моделює історію передачі банкноти

Фіг 16 схематично показує гіпотетичну серію транзакцій, створюваних між модулем генератора грошей, який має ідентифікаційний номер "1" (позначений як "Генератор 1 грошей"), грошовим модулем банківського касира, який має ідентифікатор "2" (позначений як "Модуль 2 банківського касира") та чотирма транзакційними грошовими модулями, що мають цілочисельні ідентифікатори від 3 до 6 (які позначаються як "Транзакційні модулі 3 - 6"), пов'язаними з єдиною банкнотою, виробленою генератором 1 грошей в той момент, коли параметр дата/час дорівнював 1 00 00

Відповідно до прикладу історії передачі, показаному на фіг 16, фіг 17 ілюструє, як передача електронного подання готових грошей створює деревоподібну структуру електронних подань готових грошей, яка виводиться з початкової банкноти, що вироблена модулем генератора грошей Коли окремі передачі (частина гілки дерева) банкноти розміщуються або повертаються до банківської системи відповідно до поновлення банкноти, дерево передачі банкноти на фіг 17 будується системою "Узгодження емітованих грошей" У даному прикладі генератор 1 грошей (ідентифікатори модулів містяться в підписаних

цифрами сертифікатах) виробляє електронне подання 2300 готових грошей, що має основну групу полів даних і групу полів даних передачі, які для ясності схематично показані частково На додаток, для зручності не показана група полів даних підписів і сертифікатів

Основна група полів даних містить ідентифікатор банкноти (наприклад, "№ 12"), ідентифікатор модуля генератора грошей (наприклад, "MG1"), ідентифікатор емісійного банку (наприклад, "Назва банку"), дату емісії (наприклад, 1 00 00), дату закінчення терміну придатності (наприклад, 12 00 00), суму банкноти та ідентифікатор грошової одиниці (наприклад, \$50) Інші поля даних основної групи, такі як тип банкноти, для зручності не пока-

зані. Різні поля дати в електронних банкнотах показані для ілюстрації в формі день година хвили-на. Зрозуміло, можливі й інші форми (наприклад така, що містить секунди) контролювання часу.

Група полів даних передачі містить запис передачі, що має ідентифікаційний номер приймаючої сторони, дату передачі та суму, що передається. Група передачі також переважно містить порядковий номер, який збільшується функцією "Каталог банкнот" сторони, яка передає, після кожної передачі. Звичайно дата/час і ідентифікатор передачі повинні представляти достатню інформацію для однозначного ідентифікування передачі. Однак можливо, що передача, ідентифікатор приймаючої сторони, дата/час і сума можуть дублюватися, якщо між передачами відбувалося регулювання часу і така ж сума передавалася тому ж самому модулю. Таким чином, для запобігання цієї потенційної проблеми переважно до запису передачі та функції "Каталог банкнот" додається порядковий номер, щоб однозначно ідентифікувати передачу. Порядковий номер буде збільшуватися функцією "Каталог банкнот" після кожної передачі. Якщо порядковий номер встановлено заново, то це буде зафіксоване як дублювання.

Таким чином, коли електронне подання 2300 готових грошей передається модулю 2 банківського касира, до групи передачі додається запис 2302 передачі, що містить ідентифікаційний номер приймаючої сторони (наприклад, "2"), дату передачі (наприклад, "1 00 00"), передану суму (наприклад, \$50) і порядковий номер (наприклад, "1"). Для зручності ілюстрування передачі банкноти, наведені на фіг. 17, показують тільки знов приєднану частину запису передачі банкноти, що передається. Також для зручності не показано поле даних групи передачі, яке показує загальну кількість передач.

Електронне подання 2300 готових грошей від генератора 1 грошей зберігається в грошовому модулі 2 банківського касира. Як частина зняття \$50 транзакційним модулем 3, грошовий модуль 2 банківського касира формує електронне подання готових грошей приєднанням запису 2304 передачі до копії полів даних в електронному поданні 2302 готових грошей, доповненої записом 2302 передачі. Ця банкнота після цього зберігається у транзакційному модулі 3 після завершення зняття. Зрозуміло, що кожний вузол дерева передачі банкноти показує знов приєднану частину запису передачі банкноти, що передається.

Як показано за допомогою дерева передачі банкноти, у 1 00 05 транзакційний модуль TR3 виплачує \$10 транзакційному модулю 4 за допомогою запису 2306 передачі. У 1 01 00 транзакційний модуль 3 виплачує \$10 транзакційному модулю 5 шляхом запису 2308 передачі. У 3 08 01 транзакційний модуль 3 виплачує \$25 транзакційному модулю 5 шляхом запису 2310 передачі. У 4 11 08 транзакційний модуль 3 передає \$5 транзакційному модулю 6 записом 2312 передачі.

У 2 00 01 транзакційний модуль 4 передає \$5 транзакційному модулю 6 записом 2314 передачі. У 2 01 07 транзакційний модуль 4 передає ще \$5 транзакційному модулю 6 записом 2315 передачі, а транзакційний модуль 6, у свою чергу, у 3 07 05 передає \$5 транзакційному модулю 3 записом

2321 передачі.

У 2 00 06 транзакційний модуль 5 передає транзакційному модулю 3 цілу 10-доларову банкноту записом 2316 передачі. 3 25-доларової банкноти, отриманої в 3 08 01 транзакційним модулем 5 від транзакційного модуля 3, транзакційний модуль 5 у 3 09 12 виплачує \$20 транзакційному модулю 6 записом 2318 передачі, а \$5, що залишилися, вміщує до грошового модуля 2 банківського касира у 4 12 05 записом 2320 передачі.

У 4 10 00 транзакційний модуль 6 передає \$10 транзакційному модулю 5 відповідно до запису 2322 передачі, а в 5 00 06 передає \$10, що залишилися, транзакційному модулю 3 записом 2324 передачі. Відповідно до одного з виконань даного винаходу передбачається, що після вміщення грошей транзакційного модуля до банку всі банкноти (у тому числі кредитні банкноти) у транзакційному модулі надсилаються банківській системі й оновлюються. Тому практично водночас з описаним вище депозитом модулю 2 банківського касира від транзакційного модуля 5, поданим записом 2320 передачі, автоматично з'являється додаткова і одночасна передача, подана записом 2326 передачі. Після цього нова банкнота вартістю \$5 (припустимо, що транзакційний модуль 3 не мав кредитних банкнот) виробляється грошовим модулем 1 і передається транзакційному модулю 3 через модуль 2 банківського касира з приєднанням належних записів переносу (не показано). Відповідно можна відзначити, що поновлення всіх банкнот в транзакційному грошовому модулі після транзакції (наприклад, розміщення або зняття) між транзакційним модулем 1 і модулем банківського касира спрощує процес узгодження банкноти, забезпечуючи додатковий засіб повернення банкнот до банківської системи.

У 5 00 10 транзакційний модуль 3 вміщує \$10 в модуль 2 банківського касира записом 2328 передачі. Як описано вище для депозиту транзакційного модуля 5, одночасного з депозитом транзакційного модуля 3, поданим записом 2328 передачі, відбуваються додаткові і одночасні передачі (не показано) банківській системі всіх банкнот, які мав транзакційний модуль 3, у тому числі поданих записом 2316 передачі та записом 2321 передачі. Після цього банківська система повертає транзакційному модулю 3 банкноту на суму, яка дорівнює загальній сумі банкнот, надісланих банківській системі для поновлення (наприклад, \$15).

Таким чином, у цей момент часу тільки транзакційний модуль 6 має залишки, що передаються, початкової банкноти 2300, поданими банкнотами 2312 і 2314. Якщо транзакційний модуль 6 виконує транзакцію (наприклад, занесення на рахунок або зняття з рахунка) з грошовим модулем банківського касира до передачі цих банкнот іншим транзакційним грошовим модулем, то в обороті не буде банкнот, що передаються, які відносяться до вихідної банкноти 2300, всі банкноти, що походять з передачі вихідної банкноти 2300, будуть повернуті до банківської системи, дозволяючи завершити побудову дерева передачі банкноти, показаного на фіг. 17. Дата закінчення терміну дії ефективно полегшує узгодження банкноти за рахунок обмеження часу, протягом якого банкнота може передава-

тися

З дерева передачі банкноти стає зрозуміло, що якщо банкнота була підроблена, то не буде жодної основної частини банкноти, яка б збігалася з розміщеною на депозит першою частиною. Якщо передача була дубльована, то сума нижчеподаних передач буде більшою, ніж сума передачі більш високого порядку. Наприклад, якщо транзакційний модуль 6 передав транзакційному модулю 3 \$20 в 5 00 06 замість \$10 (тобто запис 2324 передачі), то передачі нижче запису 2318 передачі (тобто SEQ1, 3 09 12, TR6, \$20) будуть мати суму \$30, яка показує, що транзакційний модуль 6 продублював передачу.

Зв'язування грошового модуля з банківським рахунком(ами) для банківського доступу

Фіг. 18 показує протокол зв'язування грошового модуля банківськими рахунками для банківського доступу. Процес починається, коли абонент ідентифікує себе представнику клієнтської служби (ПКС) і запитує ПКС зв'язати рахунок абонента з грошовим модулем (крок 1928). ПКС вводить запит до центрального процесора МОК А (ЦПМОК А) для зв'язування рахунків для ідентифікованого абонента, а ЦПМОК А одержує доступ до інформації про рахунок ідентифікованого абонента від банківських систем (кроки 1930-1934). Після цього абонент і ПКС перевіряють інформацію про рахунок, і абонент обирає, які рахунки зв'язувати з грошовим модулем (крок 1938).

Після того, як абонент запитує зв'язок свого грошового модуля В з банківськими рахунками, а ПКС через ЦПМОК А запитує, щоб МОК А зв'язався з банківськими рахунками, між грошовим модулем В абонента і МОК А встановлюється безпечний сеанс зв'язку (кроки 1938 - 1946). Після цього, у відповідь на запит від функції "Зв'язок з центральним процесором А МОК А", ЦПМОК А надсилає інформацію про рахунок до МОК А, який приймає інформацію про рахунок і будує на її основі профіль рахунка (кроки 1948 - 1952). Функція "Ключ загального користування А" після цього підписує профіль рахунка, а функція "Створення профілю рахунка" створює повідомлення з профілю рахунка та підпису і надсилає це повідомлення грошовому модулю В (кроки 1954 - 1958). Функція "Підтримання безпеки В" приймає це повідомлення, а функція "Ключ загального користування В" перевіряє цифровий підпис на повідомленні (кроки 1958 - 1962). Якщо підпис недійсний, то сеанс зв'язку переривається (крок 1966).

Якщо підпис дійсний, то функція "Зв'язок з абонентом В" надсилає профіль центральному процесору для того, щоб абонент перевіряв профіль рахунка. Якщо абонент не підтверджує профіль рахунка, то транзакція переривається. Якщо абонент підтверджує профіль рахунка, то функція "Підтримання безпеки В" додає сертифікат МОК до профілю рахунка (крок 1968).

Функція "Зв'язок з банківським касиром В" після цього перевіряє профіль рахунка, щоб визначити, чи збережено вже профіль рахунка для банку, зв'язаного з останнім створеним ("новим") профілем рахунка. Якщо профіль рахунка для банку вже існує в додатку "Зв'язок з банківським касиром В", то він замінюється функцією "Зв'язок з банківським

касиром" на новий профіль рахунка, у протилежному разі функція "Зв'язок з банківським касиром В" додає новий профіль рахунка (кроки 1970 - 1974).

Перепідтвердження зв'язку грошового модуля з банківськими рахунками

Фіг. 19 показує протокол перепідтвердження абонентом зв'язку грошового модуля абонента з банківськими рахунками. Процес починається, коли абонент ставить підпис на своєму грошовому модулі і у відповідь на підказку про транзакції, що виробляється функцією "Зв'язок з абонентом А", абонент обирає перепідтвердження зв'язку з банківським рахунком для банку, зв'язаного з модулем обслуговування клієнтів (МОК) В (кроки 1978 - 1982). Цей грошовий модуль викликає та виконує протокол входження у мережу, описаний вище з посиланням на фіг. 6, і встановлюється безпечний сеанс зв'язку між грошовим модулем А і МОК В (крок 1986). Після цього функція "Зв'язок з банківським касиром А" надсилає профіль рахунка для банківських рахунків МОК В (кроки 1988 - 1990). Функція "Створення профілю рахунка В" приймає повідомлення, а функція "Підтримання безпеки В" підтверджує дійсність сертифіката МОК і підписи профілю рахунка (кроки 1992 - 1995). Якщо сертифікат або підпис недійсні, то МОК перериває транзакцію (крок 2000). Якщо сертифікат дійсний, то функція "Зв'язок з центральним процесором В" надсилає список рахунків з профілю рахунка центральному процесору МОК (ЦПМОК), який перевіряє за допомогою інтерактивної банківської системи, чи є кожний рахунок активним на даний момент (кроки 1996 - 2001). Якщо у якогось з рахунків скінчився термін дії, ЦПМОК надсилає МОК повідомлення про припинення (крок 2010), після цього МОК перериває транзакцію відповідно до процесу переривання (крок 2000).

Якщо всі рахунки активні, то ЦПМОК сигналізує МОК про перепідтвердження, а функція "Створення профілю рахунка В" приймає повідомлення та будує профіль рахунка з інформації про рахунок (кроки 2002 - 2004). Після цього функція "Ключ загального користування В" підписує профіль рахунка, а функція "Створення профілю рахунка В" будує повідомлення, що складається з профілю рахунка та підпису, і надсилає це повідомлення

грошовому модулю А (кроки 2006 - 2010). Функція "Ключ загального користування А" приймає це повідомлення і перевіряє цифровий підпис (крок 2012). Якщо підпис недійсний, то грошовий модуль А перериває транзакцію (крок 2018), якщо ж він дійсний, то до профілю рахунка додаються підпис профілю і сертифікат МОК (крок 2014), і грошовий модуль А фіксує транзакцію (крок 2016).

Підтвердження дійсності номера рахунка

Відповідно до виконання даного винаходу, що використовує модуль обслуговування клієнтів (МОК), описаний вище, на фіг. 20 показана блок-схема алгоритма, що показує, як підтверджується дійсність номера рахунка.

У ході цього процесу функція "Підтримання безпеки У" приймає номер рахунка і профіль рахунка, в тому числі сертифікат МОК, і перевіряє сертифікат МОК (крок 2020). Недійсний сертифікат є причиною переривання транзакції між двома гро-

шовими модулями (крок 2026)

Якщо сертифікат дійсний, функція "Підтримання безпеки У" передає профіль рахунка функції "Ключ загального користування У" для перевірки підпису МОК (крок 2022). Недійсний підпис змушує функцію "Підтримання безпеки У" інформувати функцію "Менеджер сеансу зв'язку" про те, що профіль рахунка недійсний (крок 2026), і транзакція між двома модулями переривається (крок 2028).

Якщо перевірка підпису підтверджує дійсний підпис, процедуру продовжує функція "Зв'язок з банком У", яка надсилає номер рахунка, отриманий нею, банківській комп'ютерній інтерактивній системі (крок 2024). Неактивний рахунок змусить функцію "Підтримання безпеки У" інформувати функцію "Менеджер сеансу зв'язку" про неактивний рахунок (крок 2030) і перервати транзакцію (крок 2028), активний рахунок змусить процес "Підтвердження номера рахунка" повернутися до наступного кроку послідовності дій, яка викликала процес "Підтвердження номера рахунка".

Як можна бачити, процес "Підтвердження номера рахунка" спрощено для грошового модуля банківського касира у порівнянні з варіантом виконання даного винаходу, що не містить МОК.

Витребування втрачених грошей

Як вже обговорювалося, електронні гроші можуть бути втрачені через будь-яку з декількох причин, в тому числі (1) грошовий модуль пошкоджений і більш не функціонує, (2) грошовий модуль втрачений або вкрадений, або (3) фіксування транзакції пройшло невдало. Для грошової системи важливо, щоб абонент був впевнений у безпеці своїх грошей. Таким чином, важливо, щоб приймаюча сторона була здатна затребувати гроші, втрачені в результаті системної помилки. Спроможність замінити гроші, коли грошовий модуль пошкоджений, поглинула б надійність, тому що електронна помилка більш ймовірна, ніж фізичне пошкодження паперових грошей. Заміна грошей через втрачений або вкрадений грошовий модуль проблематичніша. Вирішення таких вимог може викликати бурхливий потік вимог до системи через те, що абоненти не будуть вживати запобіжних заходів проти втрати.

У будь-якому випадку, у даному винаході реалізовано способи, які дозволять замінювати гроші, що були втрачені в будь-якому з цих випадків. У перших двох випадках (тобто у вищезгаданих випадках (1) і (2)) абонент повинен буде періодично створювати вимогу на втрачену банкноту (банкноти) (див. фіг. 21), яке могло б зберігатися поза грошовим модулем. Коли відбудеться збій, вимога, що містить ідентифікацію абонента, може бути подана до емісійного банку (див. фіг. 22). Вимога буде містити останній відомий стан грошового модуля абонента. Опис банкнот, що затребуються, може підтверджуватися і відсилатися до емісійних банків. Емісійні банки можуть замінити гроші через деякий відрізок часу, якщо банкноти, яких затребували, не були депоновані.

У випадку, коли фіксація транзакції не вдалася (тобто випадок (3)), вимога створюється інтерактивно між грошовим модулем і модулем обслуговування клієнтів, якщо грошовий модуль ще функ-

ціонує (див. фіг. 22). Ця вимога, як і у випадках (1) і (2), передається грошово-емісійній системі, що звіряє вимогу з депозитами. Емісійні банки можуть почувати себе спокійно при заміні втрачених грошей, оскільки вони можуть перевіряти гроші, що надходять, на шахрайство, а також у них є ідентифікація подавача.

Ці способи більш повно описані з посиланнями на фіг. 21 і 22.

Створення вимоги на втрачену банкноту(и) На фіг. 21А показано процес "Створення вимоги на втрачену банкноту(и)", який можна застосовувати відповідно до виконання даного винаходу. Процес починається, коли абонент входить до грошового модуля, функція "Зв'язок з абонентом А" робить підказку абоненту про транзакцію, і абонент обирає операцію "Створення вимоги на втрачену банкноту(и)" (кроки 2032 - 2036).

Після цього в декілька кроків відбувається консолідація всіх банкнот і всіх незатребуваних невдалих фіксацій (кроки 2038 - 2042). Зокрема, функція "Каталог банкнот А" створює унікальний порядковий номер вимоги (який використовується для ідентифікації вимоги) і передає копію "Каталог банкнот" разом з порядковим номером до функції "Менеджер пакета". Функція "Банкноти А" передає копію всіх банкнот з підписами і сертифікатами функції "Менеджер пакета". Після цього функція "Журнал транзакцій А" надсилає всі незатребувані транзакції, що не зробили фіксації, яких було записано до журналу під час процесу переривання транзакції, до функції "Менеджер пакета".

Далі функція "Ключ загального користування А" використовує приватний ключ грошового модуля для позначки порядкового номера вимоги, каталогу банкнот, банкнот і невдалих фіксацій, які були відправлені до функції "Менеджер пакета", а функція "Менеджер пакета" приєднує підпис до зібраних даних, видаючи в результаті зібраний пакет даних (кроки 2044 - 2046), який після цього шифрується функцією "Ключ загального користування А" (крок 2048). Після цього функція "Ключ загального користування А" приєднує до зашифрованої вимоги опис вимоги, який складається з порядкового номера вимоги, загальної суми на вимогу і сертифіката грошового модуля А (крок 2050). Функція "Зв'язок з абонентом А" надсилає цю вимогу центральному процесору грошового модуля, що приймає і зберігає вимогу за допомогою середовища, яке фізично незалежне від грошей, для використання в майбутньому (кроки 2052 - 2054).

Тому зрозуміло, що процес витребування втрачених банкнот забезпечує спосіб вироблення та захисту потенційних грошових вимог, що не руйнуються при пошкодженні або збої грошового модуля.

Затребування втрачених банкнот

Фіг. 22 показує протокол витребування втрачених банкнот, який починається, коли абонент робить запит на витребування втрачених банкнот представнику клієнтської служби (ПКС), причому абонент ідентифікує себе ПКС (крок 2056). Після цього ПКС передає ідентифікацію абонента центральному процесору модуля обслуговування клієнтів (ЦПМОК) А і перевіряє, чи подана вимога че-

рез невдалу фіксацію або через пошкодження, або втрати грошового модуля (кроки 2058 - 2060) Якщо підставою для вимоги є невдала фіксація (грошовий модуль абонента не був втрачений або пошкоджений), то після того, як абонент зробив вибір подати вимогу на втрачені банкноти, а ПКС зробив вибір прийняти від грошового модуля вимогу на втрачені банкноти, функція "Менеджер сеансу зв'язку В" грошового модуля абонента і функція "Менеджер сеансу зв'язку А" модуля обслуговування клієнтів (МОК), зв'язаного з представником клієнтської служби (через центральний процесор модуля обслуговування клієнтів (ЦПМОК)), відповідно використовуються для встановлення безпечного сеансу зв'язку між МОК А і грошовим модулем В (Кроки 2062 - 2070)

Коли встановлено безпечний сеанс зв'язку, функція "Зв'язок з центральним процесором А МОК" запитує ідентифікацію абонента, а ЦПМОК А відповідає на цей запит, надсилаючи МОК повідомлення, що містить ідентифікацію (кроки 2072 - 2074) Функція "Витребування втрачених банкнот А" приймає це повідомлення і надсилає грошовому модулю В повідомлення, яке показує, що повинна бути відправлена вимога (кроки 2076 - 2078)

Функція "Журнал транзакцій В" приймає це повідомлення і вимагає записи невдалої фіксації, які не були витребовані (крок 2080) Якщо немає записів невдалої фіксації, транзакція переривається (2083) У протилежному разі функція "Зв'язок з абонентом В" надсилає інформацію (наприклад, дату, час і суму), взяту із затребуваних записів невдалої фіксації, для перегляду абоненту (крок 2082) З цієї інформації абонент вибирає транзакції для подачі вимог (крок 2084) Наприклад, абонент не вибере невдало фіксовані транзакції, які були окремо вирішені Після цього для кожної невдало-фіксованої транзакції, обраної абонентом, функція "Журнал транзакцій В" будувє повідомлення, яке містить журнальну

інформацію для цих транзакцій, і надсилає це повідомлення МОК (кроки 2086 - 2088)

Функція "Витребування втрачених банкнот А" приймає це повідомлення і надсилає до В повідомлення, яке містить ідентифікатор вимоги (наприклад, підтверджуючий номер) для майбутніх посилань на цю вимогу (крок 2092) Функція "Журнал транзакцій В" приймає повідомлення і відмічає кожний обраний запис невдалофіксованої транзакції вимоги, поданої МОК (крок 2094) Після цього В фіксує транзакцію (крок 2098)

Після завершення процедури фіксації з прийнятого повідомлення, що містить інформацію про невдалофіксовану транзакцію, функція "Витребування втрачених банкнот А" створює вимогу, яка повинна надсилатися системі дослідження емітованих грошей (СДЕГ), яка переважно формує частину системи дослідження транзакцій Функція "Зв'язок з центральним процесором А" надсилає цю вимогу ЦПМОК А, який приймає вимогу і надсилає її далі СДЕГ (кроки 2098 - 2102)

На кроці 2060 за фіг. 22, якщо вимога ґрунтується не на невдалій фіксації (наприклад, подається через втрачений або пошкоджений грошовий модуль), абонент може вибрати подачу вимоги на втрачені банкноти з центрального процесора В,

який має доступ до всіх вимог абонента, вироблених і вивантажених з розрахункового середовища грошового модуля (наприклад, до флеш-пам'яті) відповідно до процесу створення вимоги на втрачені банкноти, який описано вище з посиланням на фіг. 21 ПКС окремо вибирає ініціалізацію процесу для отримання вимоги на втрачені банкноти від центрального процесора грошового модуля, а центральні процесори встановлюють комунікацію відповідно до будь-якого з відомих методів (кроки 2104 - 2108)

Після цього абонентський центральний процесор В надсилає вимогу, у тому числі сертифікат грошового модуля, до ЦПМОК А, який передає цю вимогу до МОК А (кроки 2108 - 2112) Функція "Витребування втрачених банкнот А" приймає вимогу і надсилає її до функції "Ключ загального користування А", яка підтверджує дійсність сертифіката грошового модуля (кроки 2114 - 2116) Якщо сертифікат грошового модуля недійсний, то функція "Зв'язок з центральним процесором А" надсилає до ЦПМОК А повідомлення, яке показує, що вимога була відхилена, а ЦПМОК А відсилає повідомлення абонентському центральному процесору В, і процес витребування втрачених банкнот переривається (кроки 2120 - 2121)

Якщо сертифікат грошового модуля дійсний, то функція "Ключ загального користування А" розшифровує вимогу та перевіряє всі сертифікати і підписи банкнот у вимозі (крок 2118) Якщо будь-які сертифікати або підписи недійсні, то транзакція переривається (кроки 2119 - 2121) Якщо сертифікати та підписи дійсні, то функція "Витребування втрачених банкнот А" перевіряє узгодженість сум передачі, щоб переконатися, що сума грошей, переданих приймаючій стороні, не перевищує суму, отриману стороною, що передає, протягом історії передачі кожної банкноти (кроки 2122 - 2123) Якщо існує неузгодженість, то транзакція буде перервана (кроки 2120 - 2121)

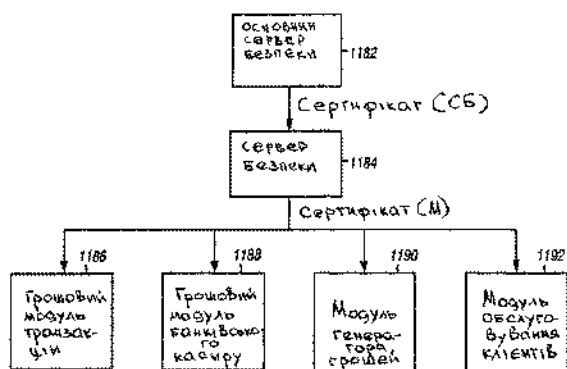
Якщо, однак, суми передачі узгоджуються для всіх банкнот, то функція "Витребування втрачених банкнот А" створює вимогу для посилки до СДЕГ, а також виробляє ідентифікатор вимоги, який зв'язується з вимогою Функція "Зв'язок з центральним процесором А" після цього надсилає створену вимогу та ідентифікатор вимоги до ЦПМОК А, який приймає вимогу та ідентифікатор вимоги і належним чином відправляє ідентифікатор вимоги абонентському центральному процесору В, а вимогу надсилає до СДЕГ (кроки 2124 - 2128), таким чином завершуючи процес витребування втрачених банкнот

Незважаючи на те, що наведений вище опис містить багато конкретних характеристик, ці подробиці не повинні сприйматися як обмеження винаходу, і для фахівців буде зрозуміло, що даний винахід може бути підданий безлічі модифікацій, адаптацій та еквівалентних реалізацій, не виходячи за рамки винаходу і без зменшення його переваг Тому даний винахід не обмежується описаними варіантами виконання і повинен визначатися відповідно до наведеної нижче формули винаходу

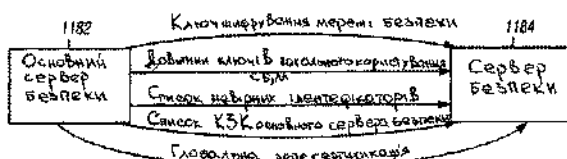
РЕФЕРАТ

Електронна грошова система, що має (1) банків або фінансові установи, які з'єднані з пристроєм

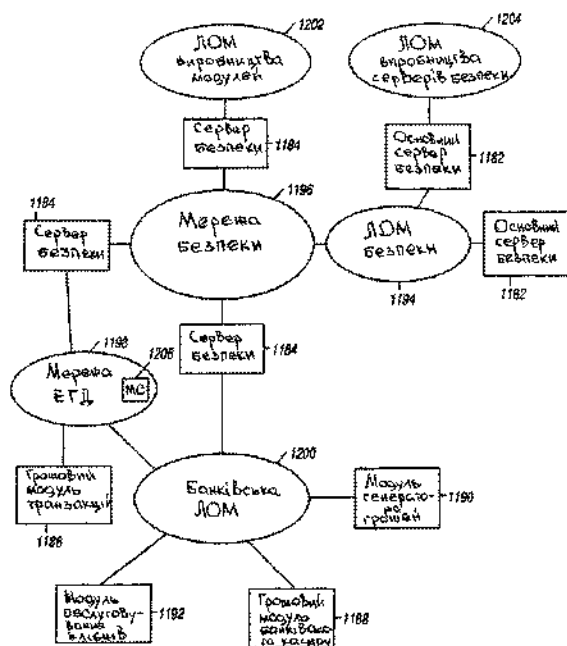
генератора грошей для вироблення та емісії для абонентів електронних грошей, у тому числі електронної готівки, субсидійованих депозитами, та електронного кредиту, (2) кореспондентські банки, які приймають і розподіляють електронні гроші, (3) декілька пристроїв транзакцій, які використовуються абонентами для зберігання електронних грошей, виконання грошових транзакцій з інтерактивними системами банків-учасників або для обміну електронними грошима з іншими такими ж пристроями транзакцій при автономних транзакціях, (4) пристрої банківських касирів, зв'язані з емісійними та кореспондентськими банками, для обслу-



Фиг. 1А

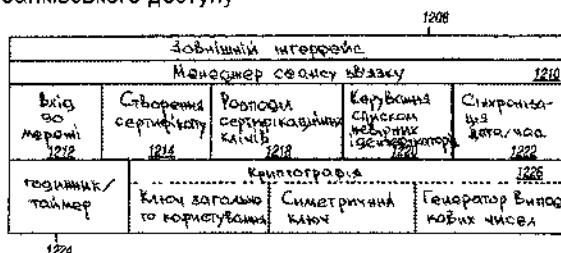


Фиг. 1Б

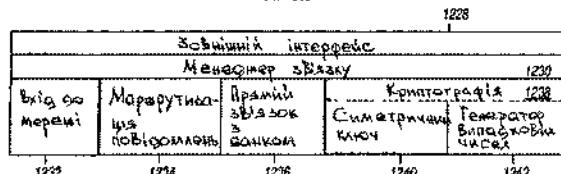


Фиг. 2

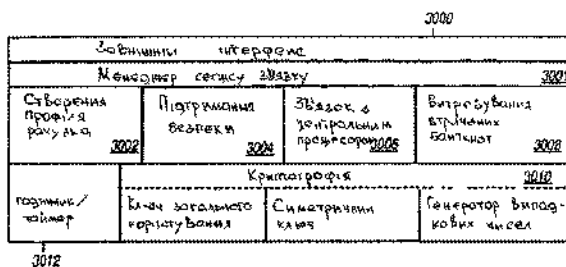
говування процесу та забезпечення взаємодії самих емісійних і кореспондентських банків, (5) кліринговий банк для зведення балансу електронно-грошових рахунків різних емісійних банків, (6) мережу обміну даними для забезпечення комунікаційних послуг всім компонентам системи, (7) систему безпеки для підтримання цілісності системи і викриття шахрайства в системі та несанкційованого доступу до системи. Виконання винаходу містить модуль обслуговування клієнтів, який обробляє запити на втрачені банкноти та зв'язує рахунки з грошовими модулями для забезпечення банківського доступу.



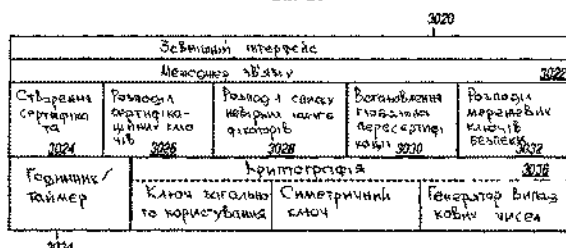
Фиг. 3А



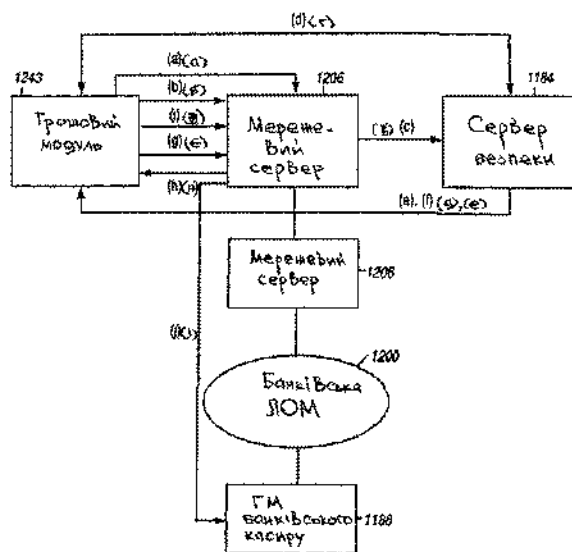
Фиг. 3Б



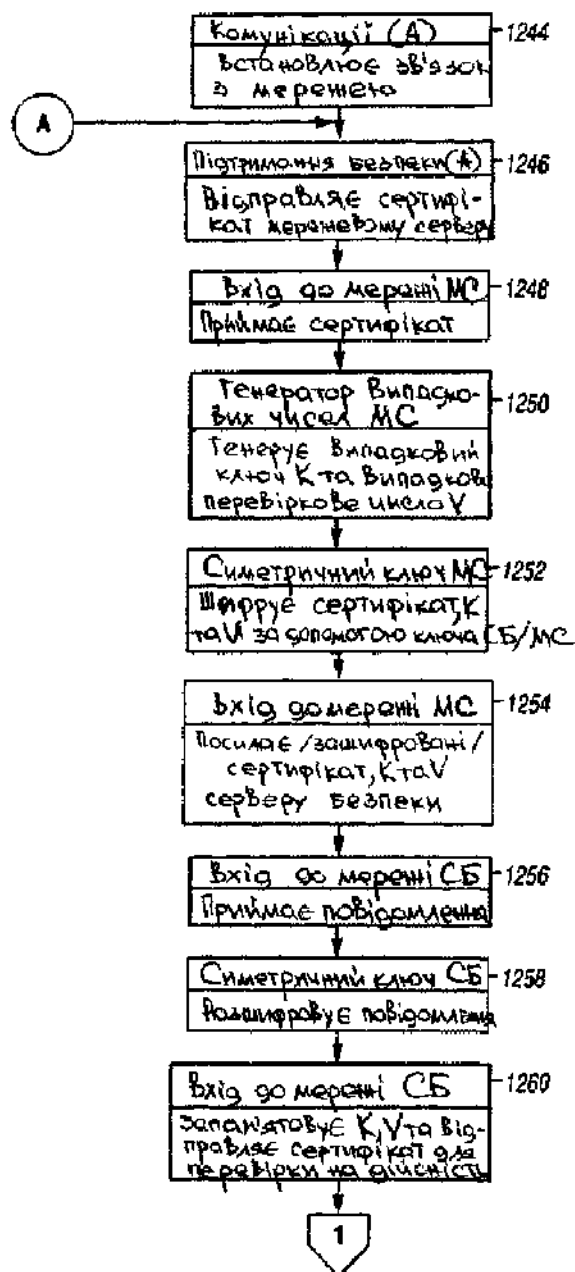
Фиг. 4А



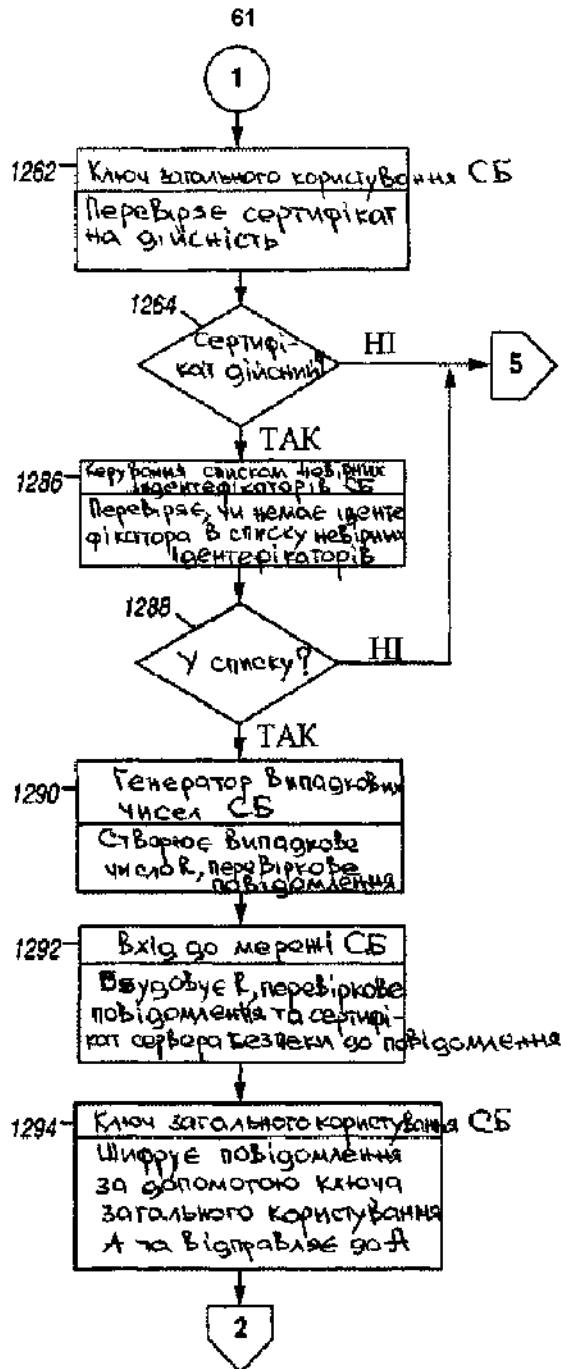
Фиг. 4Б



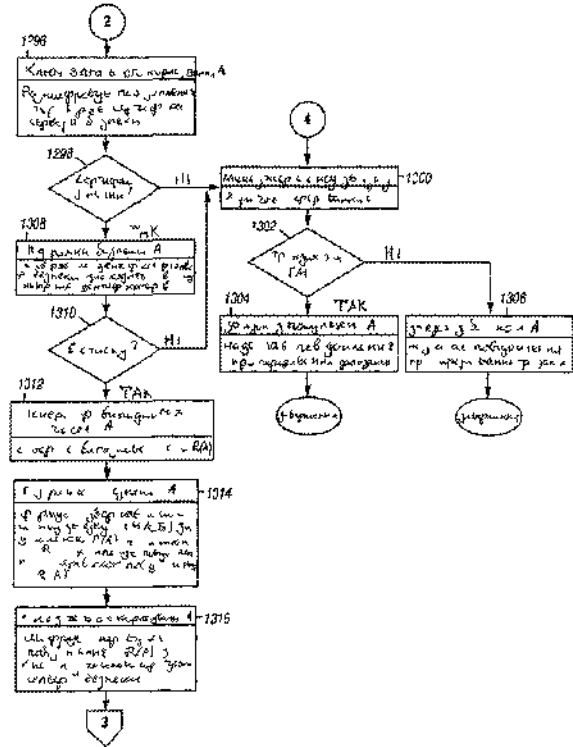
Фіг. 5



Фіг. 6А



Фіг. 6Б



Фіг. 6Б

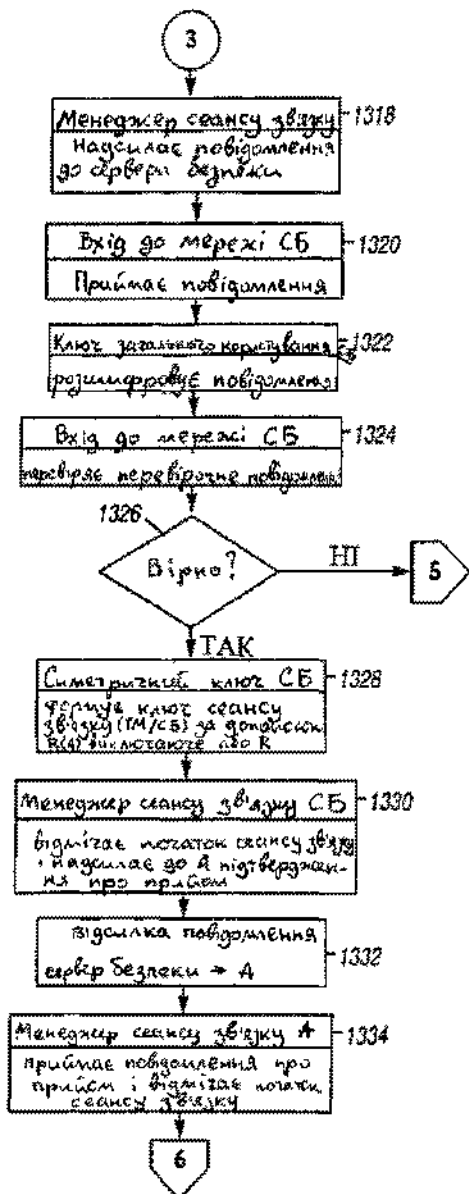


Fig. 6Г

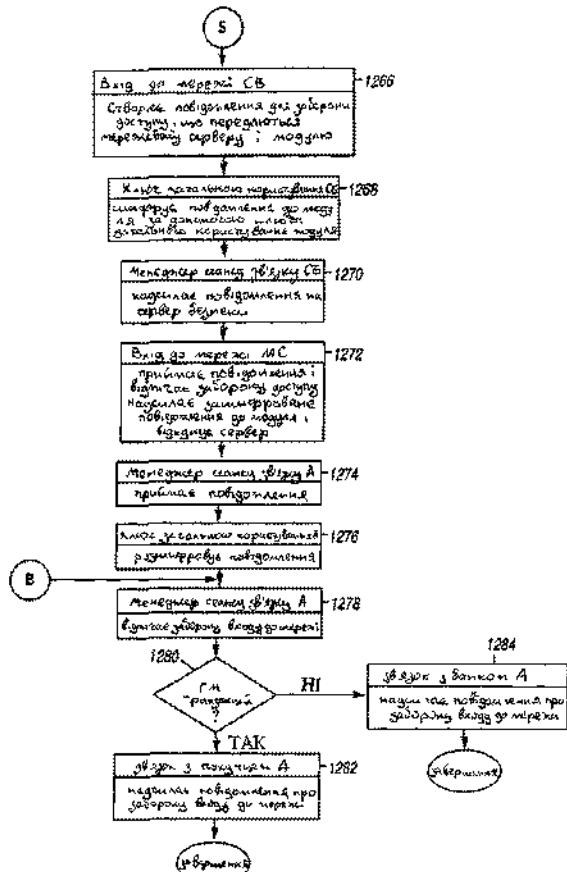
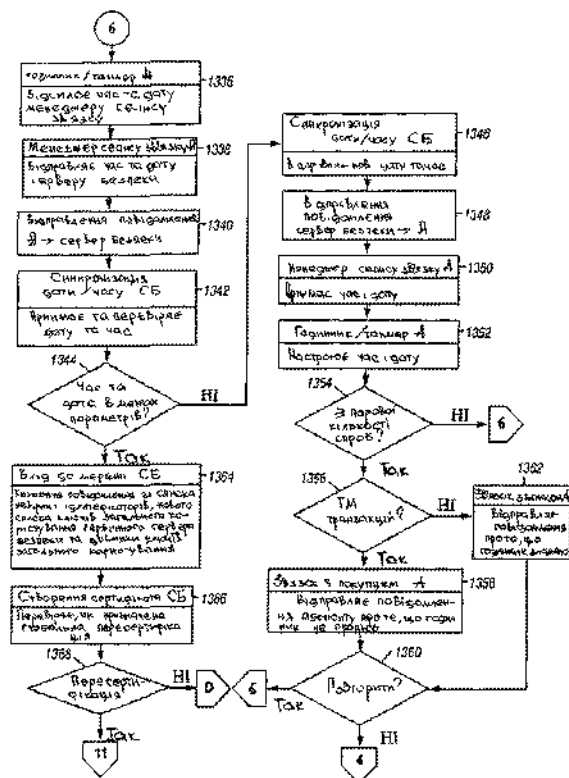
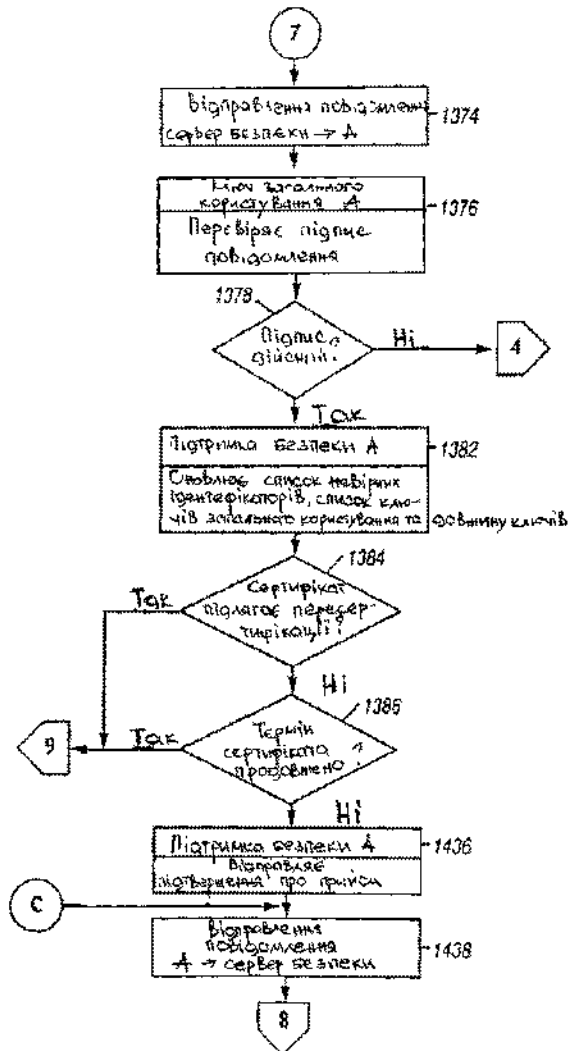


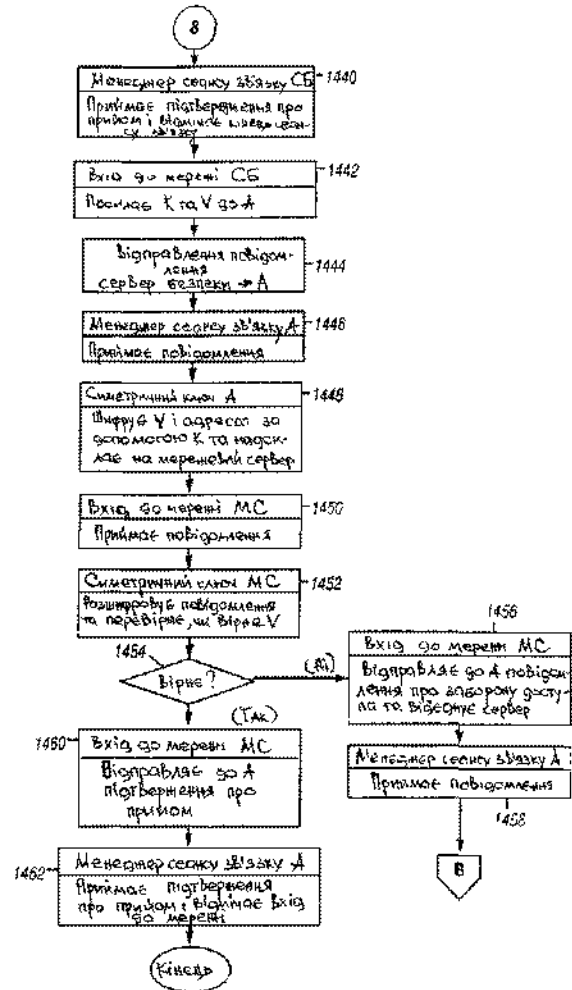
Fig. 6D



Q15. 6E



Фіг. 65



Фіг. 66

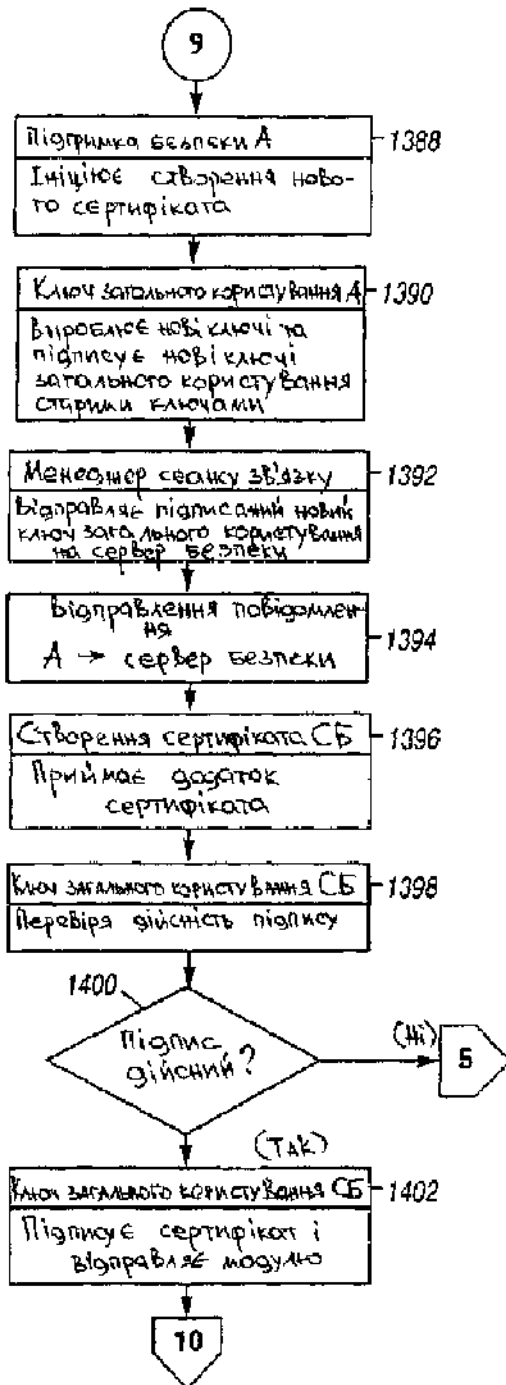


Fig. 6H

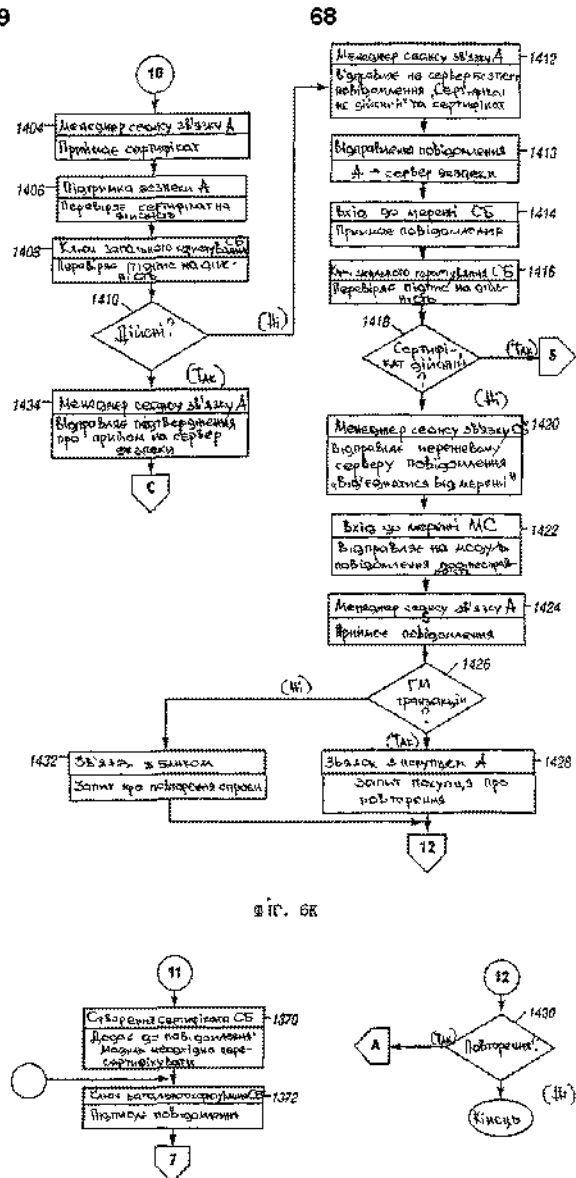
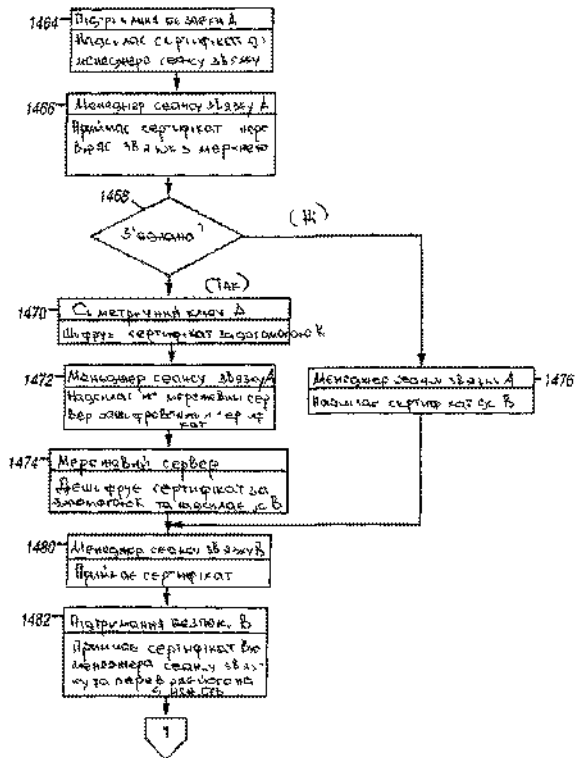
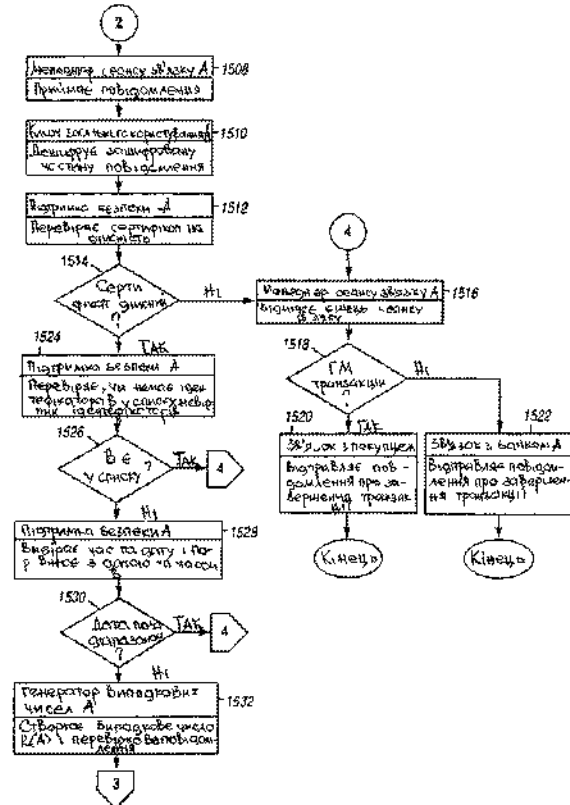


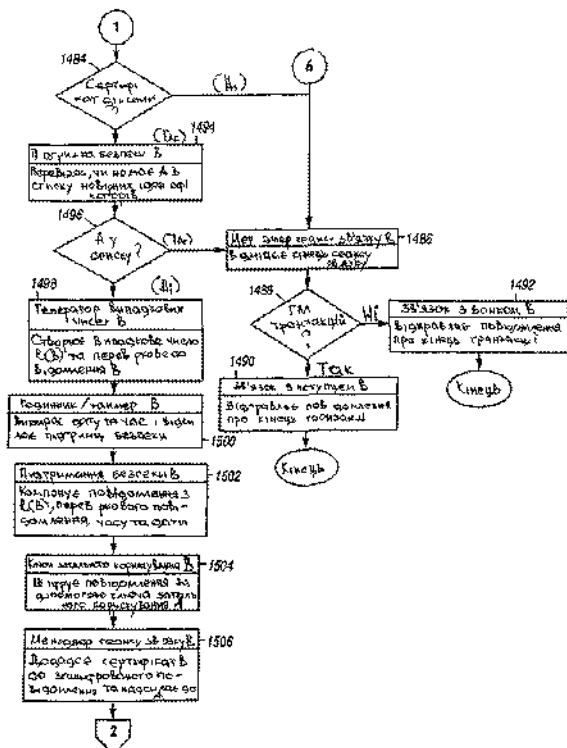
Fig. 6E



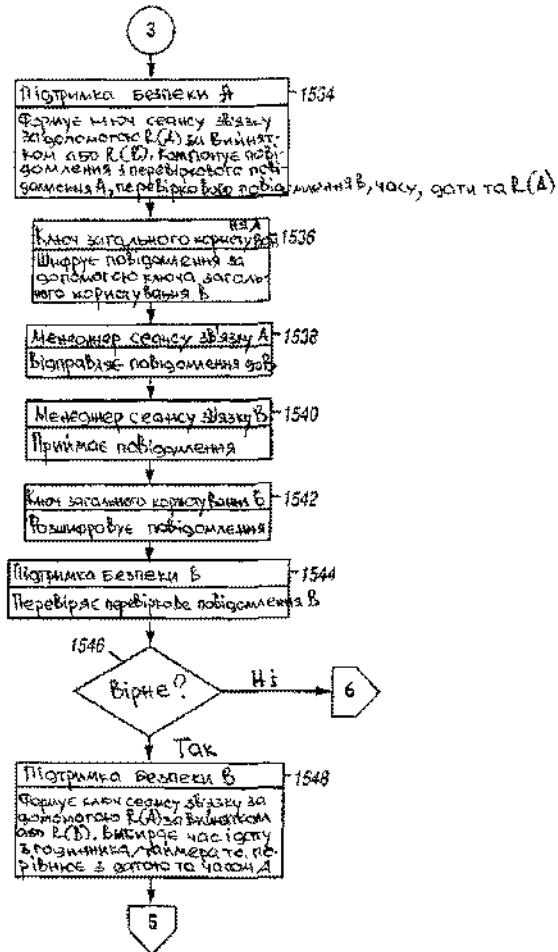
Фиг. 7А



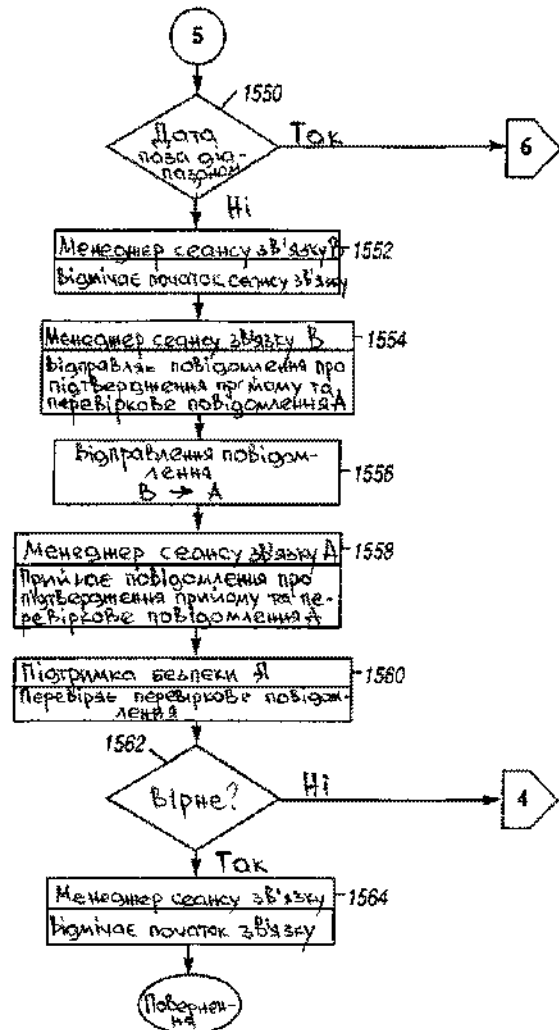
Фиг. 7Б



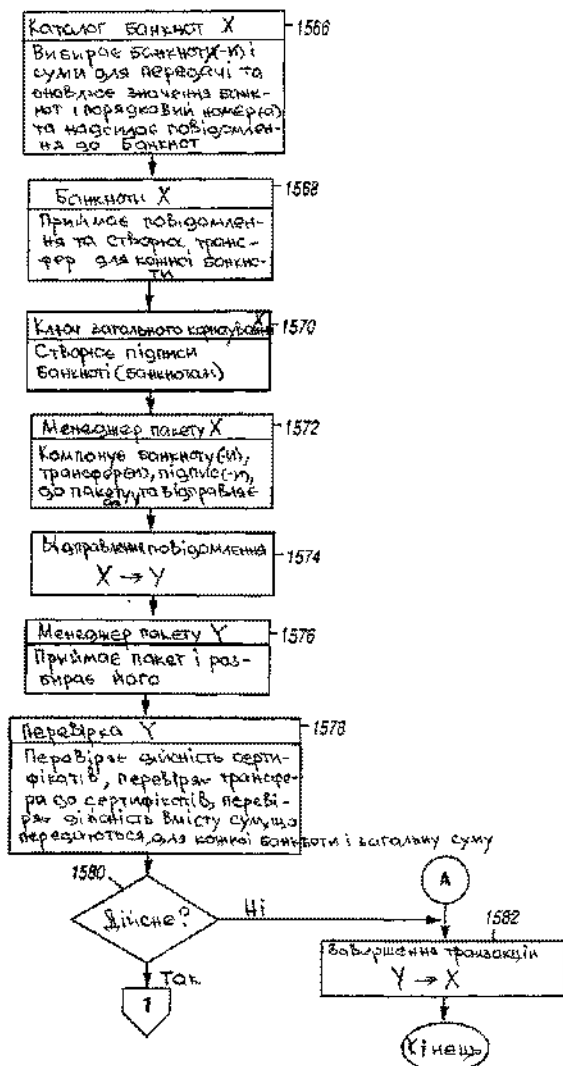
Фиг. 7Б



Фиг. 7Г



Фиг. 7Д



Sir, SA

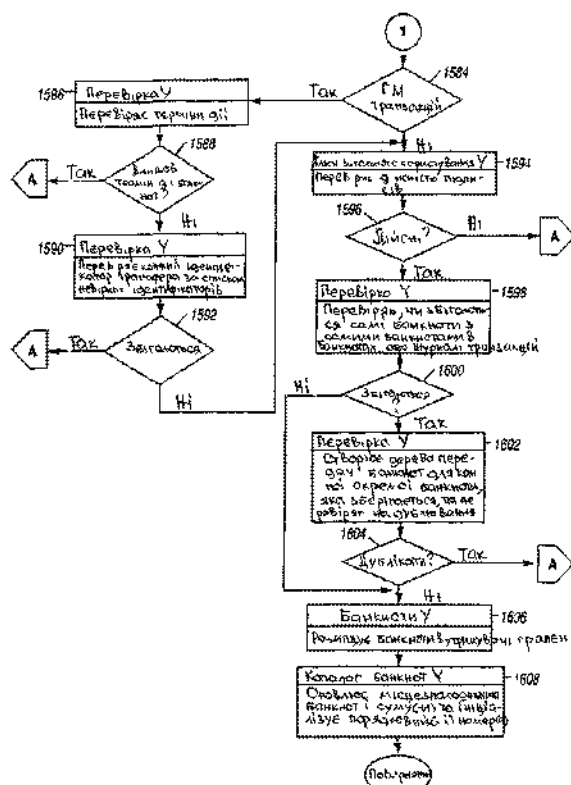
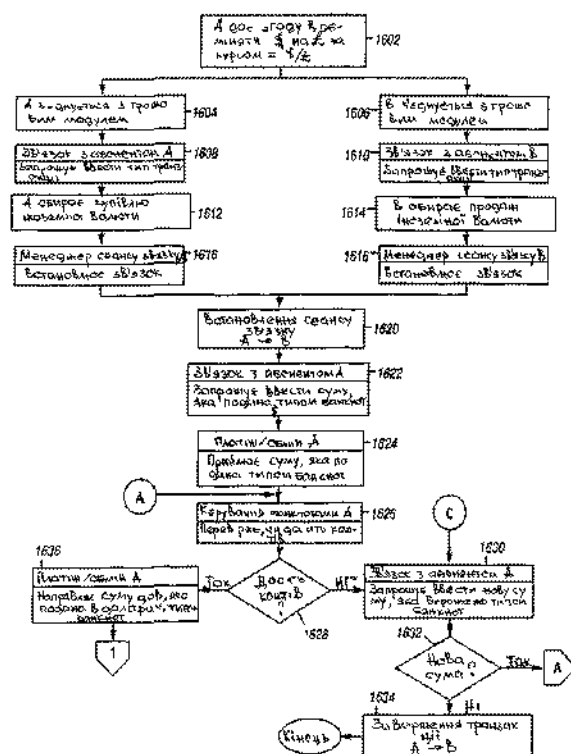
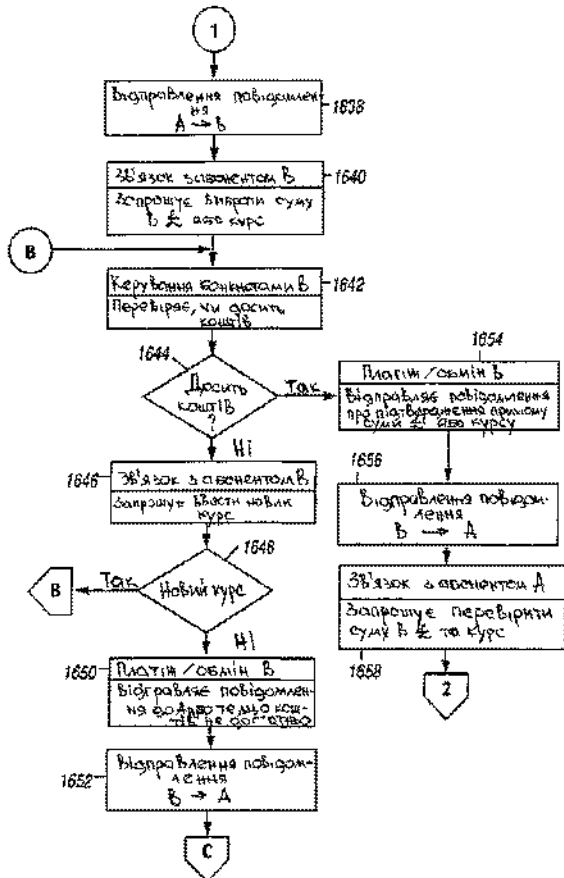
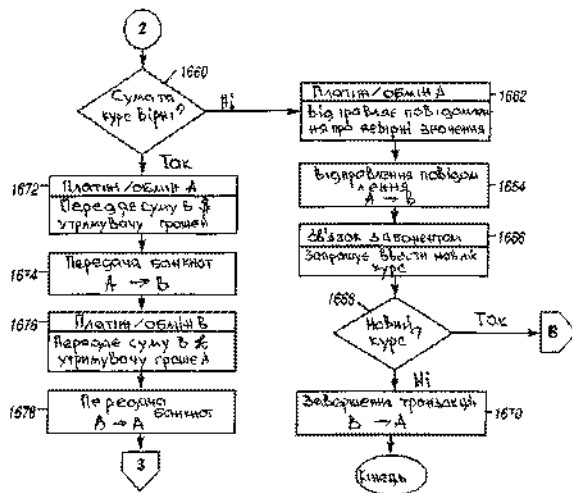


Fig. 8E

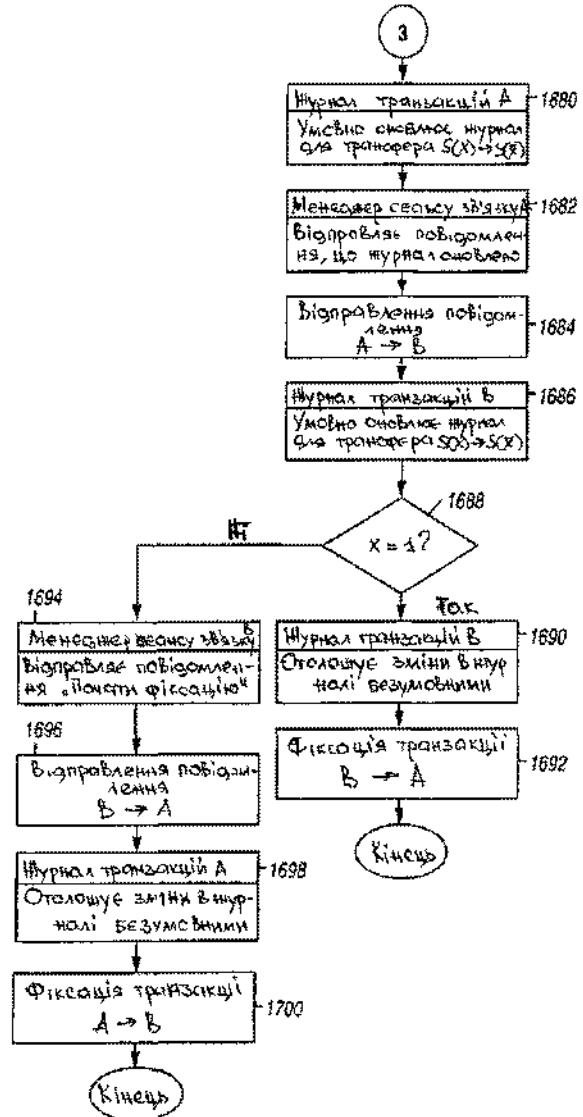
 $\Phi_{\text{tr}} = 9A$



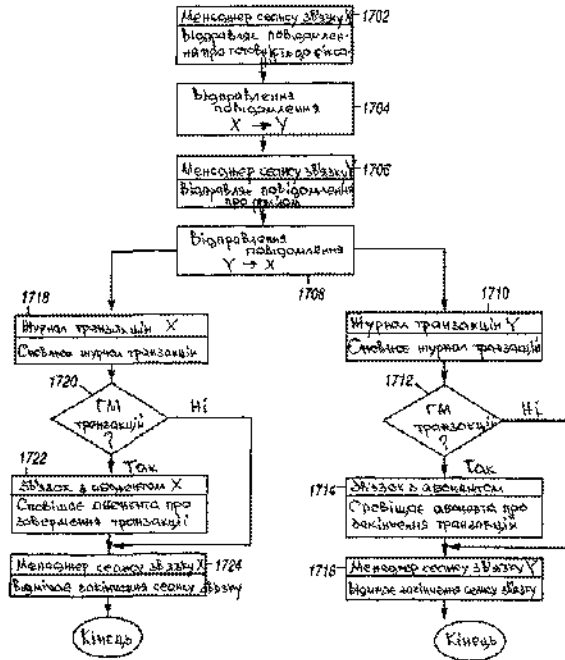
Фиг. 9Б



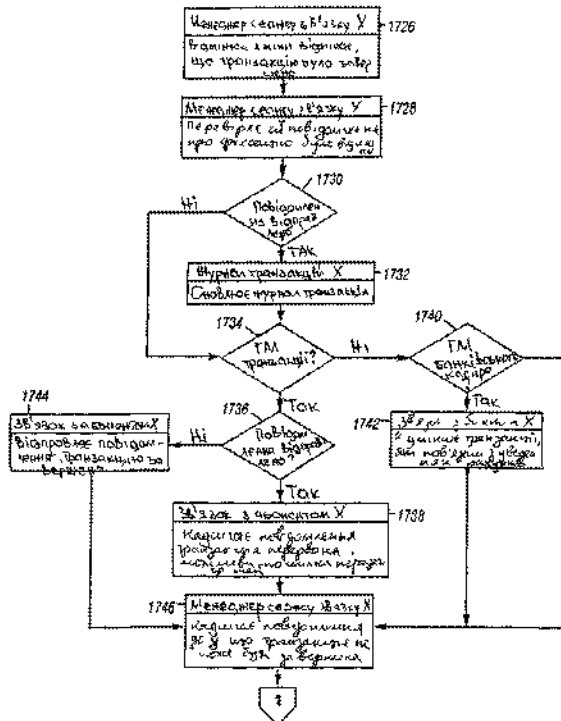
Фиг. 9В



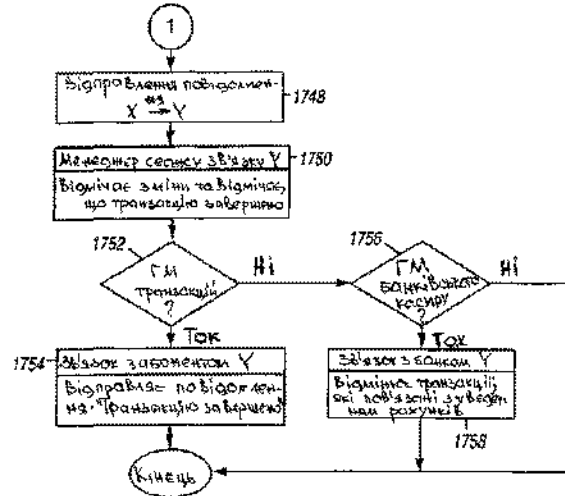
Фиг. 9Г



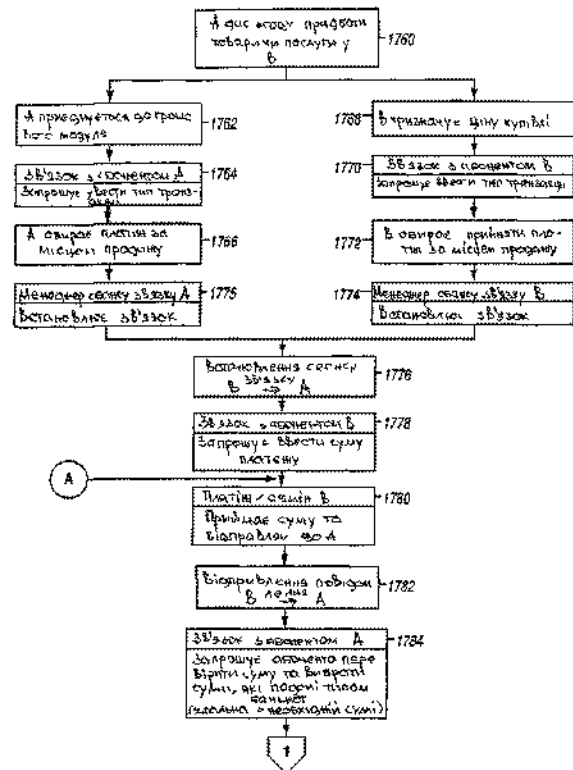
Фіг. 10



Фіг. 11A



Фіг. 11B



Фіг. 12A

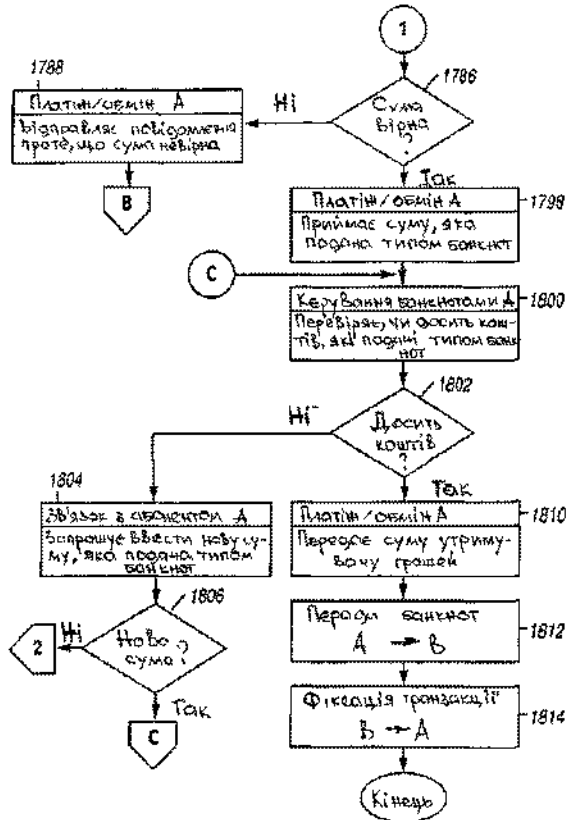


Fig. 12B

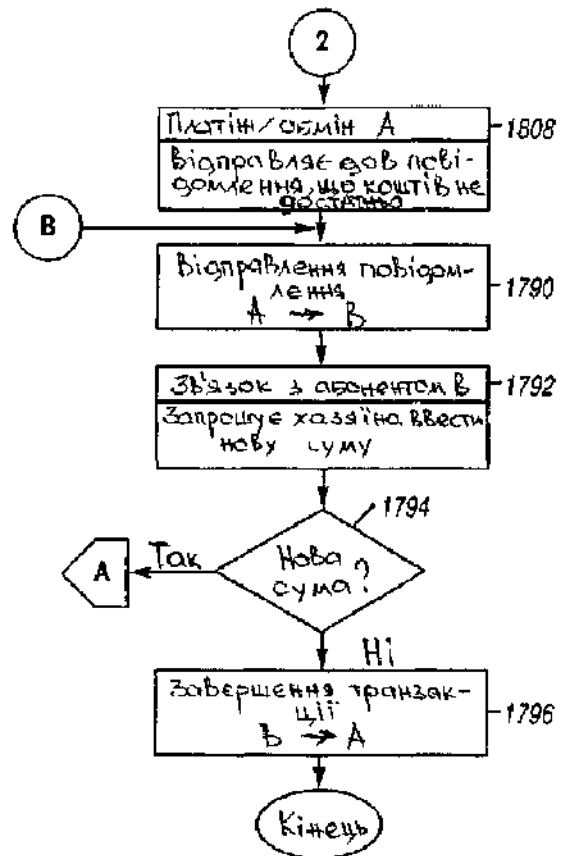
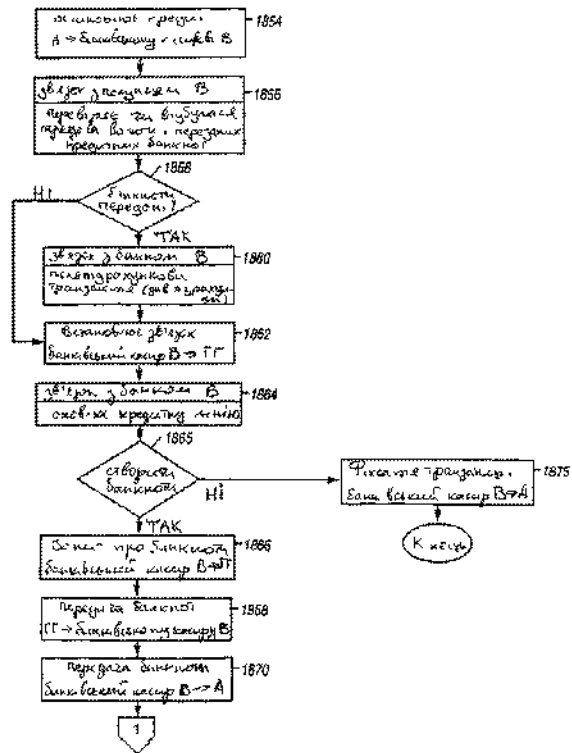


Fig. 12B

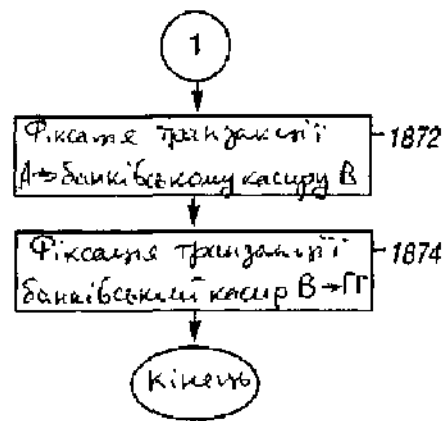
81



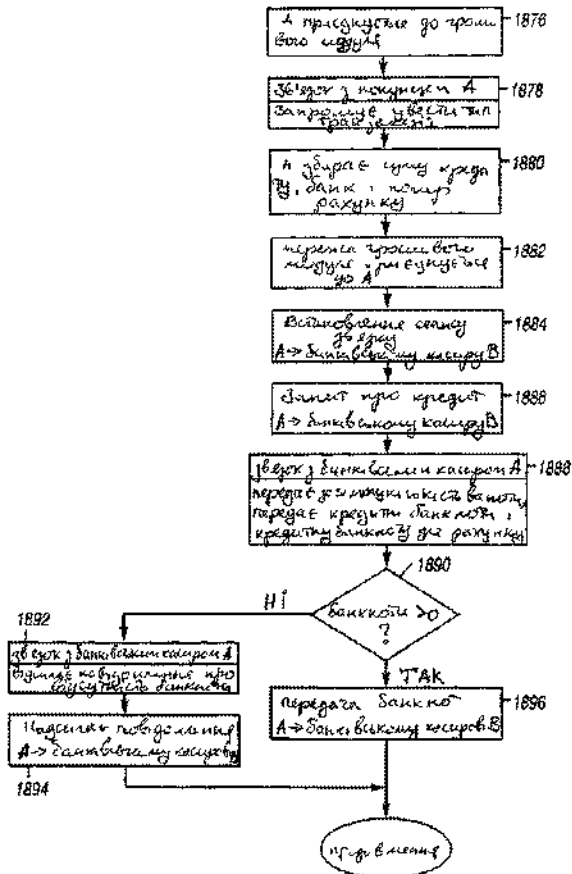
Фиг. 13А

45399

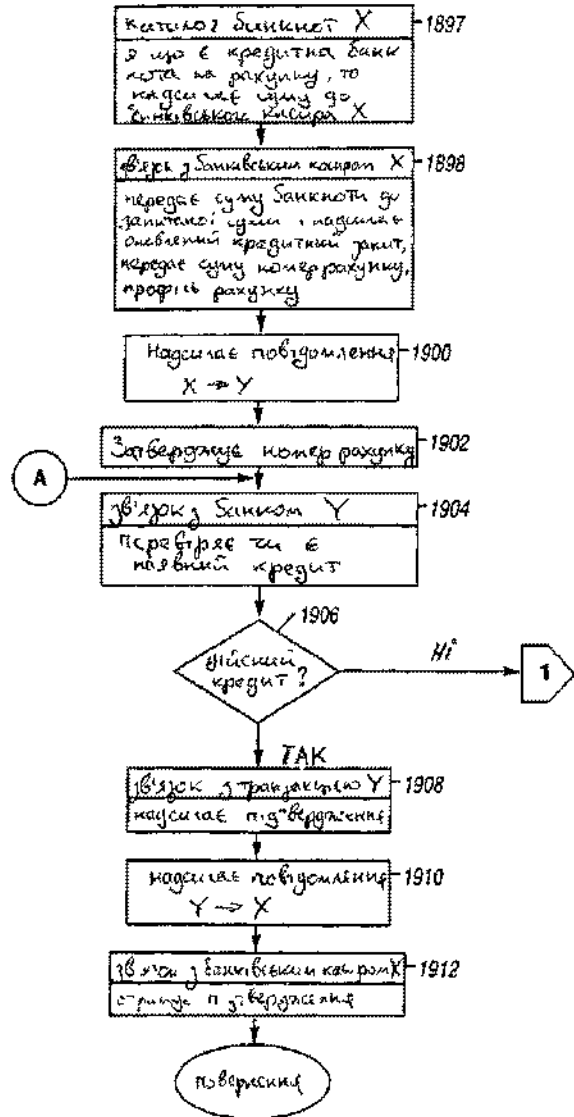
82



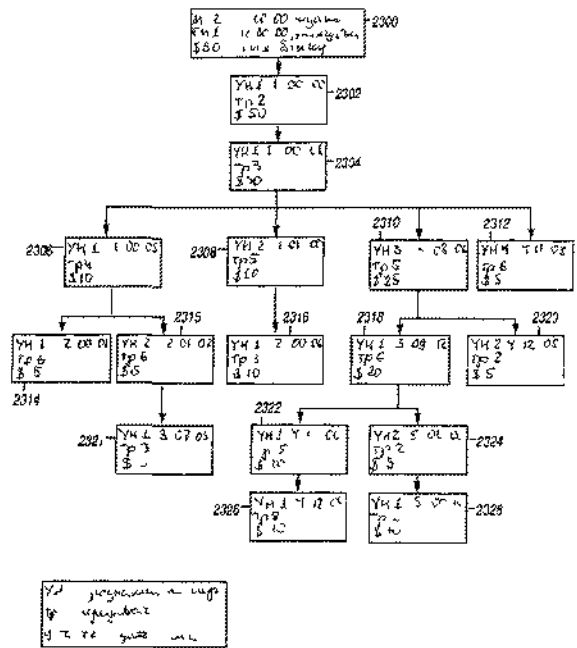
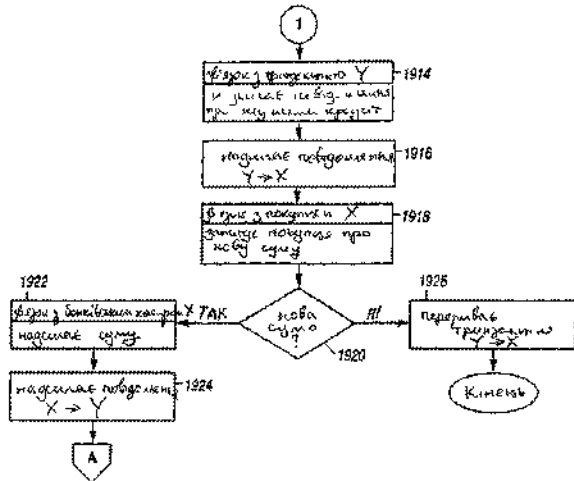
Фиг. 13Б



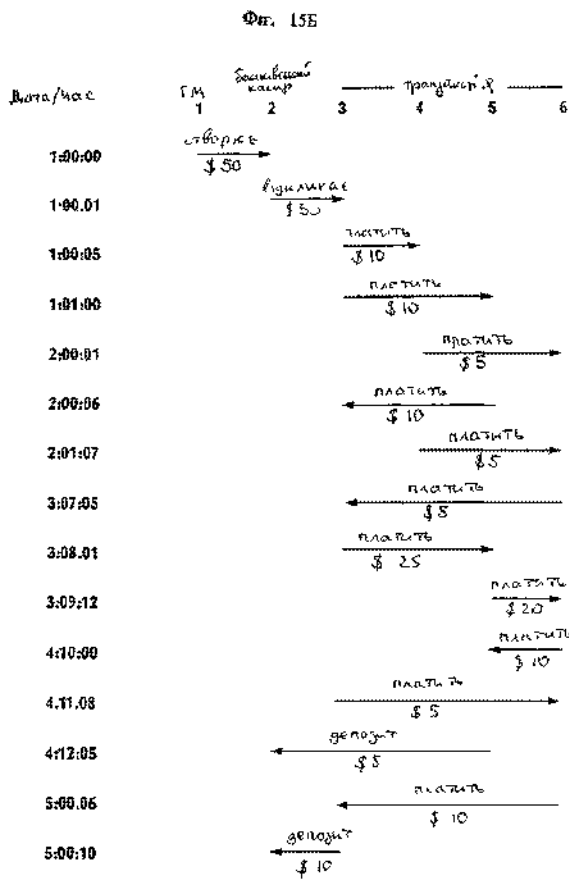
Фиг. 14



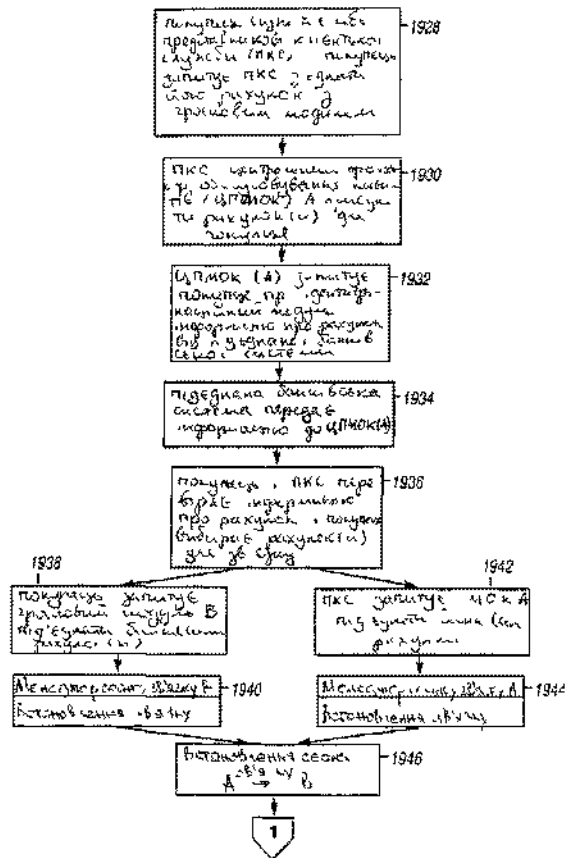
Фиг. 15A



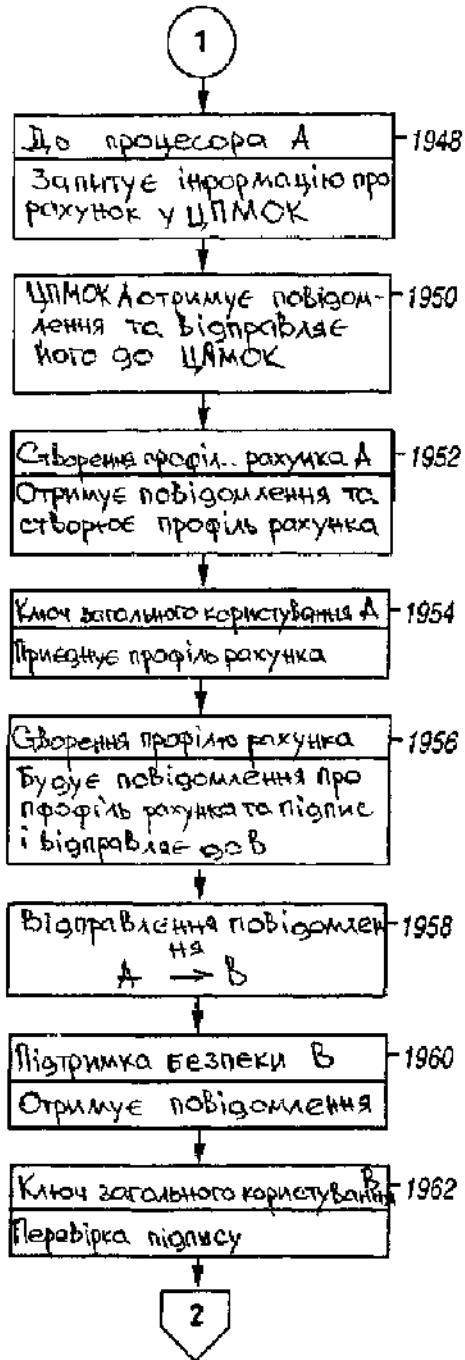
Фиг. 17



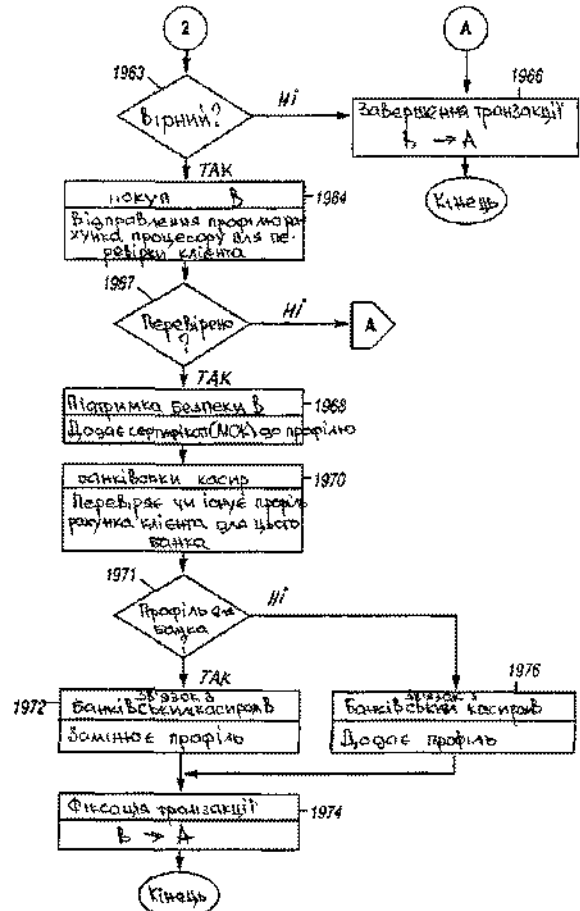
Фиг. 16



Фиг. 18А



Фіг. 18Б



Фіг. 18В

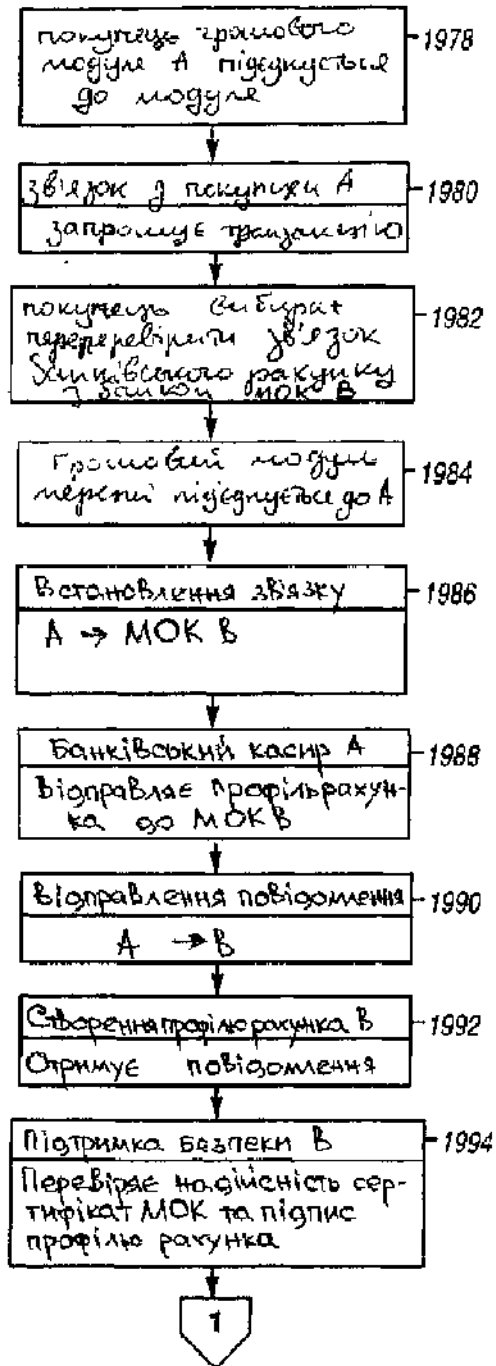


Fig. 19A

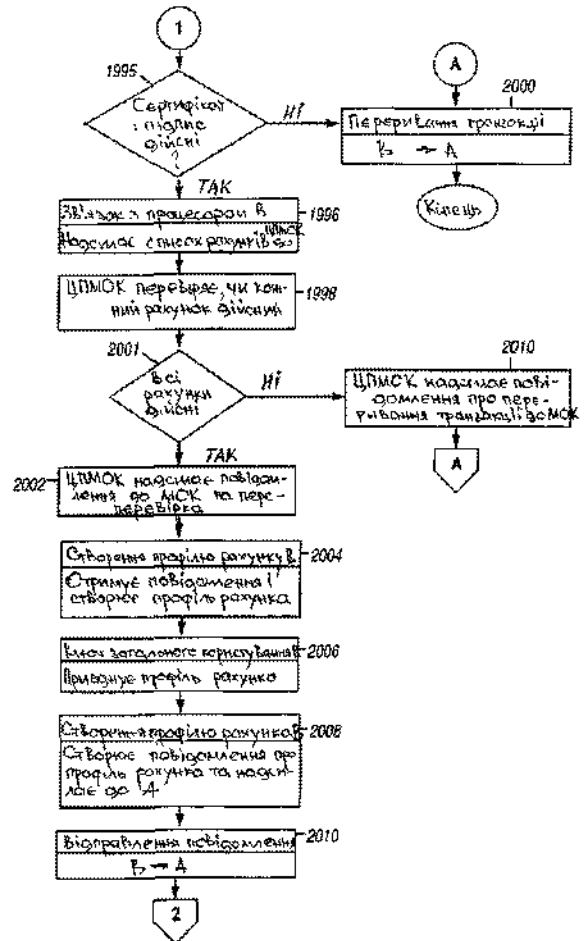
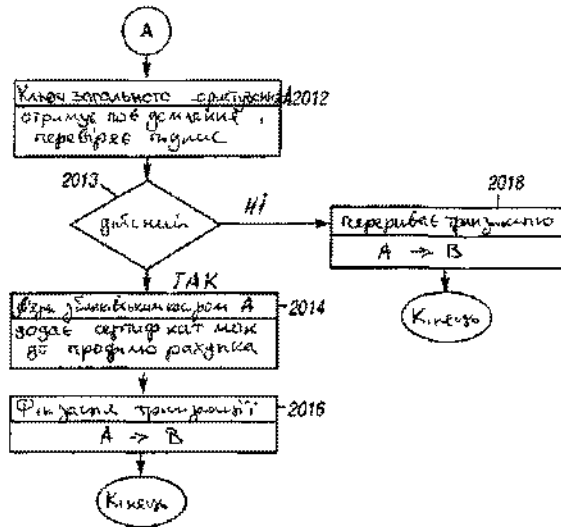
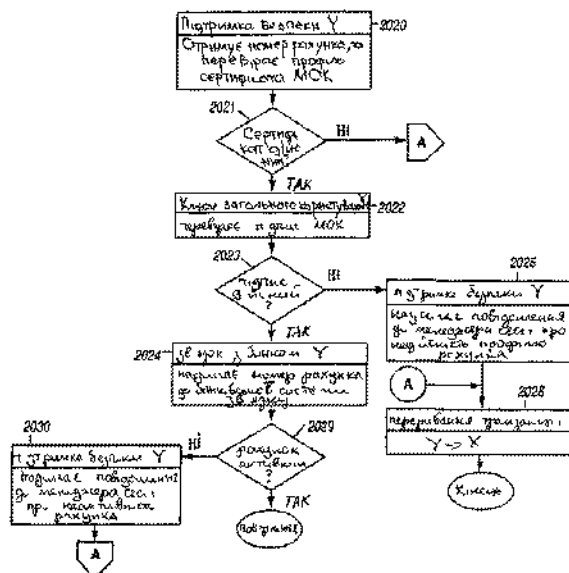


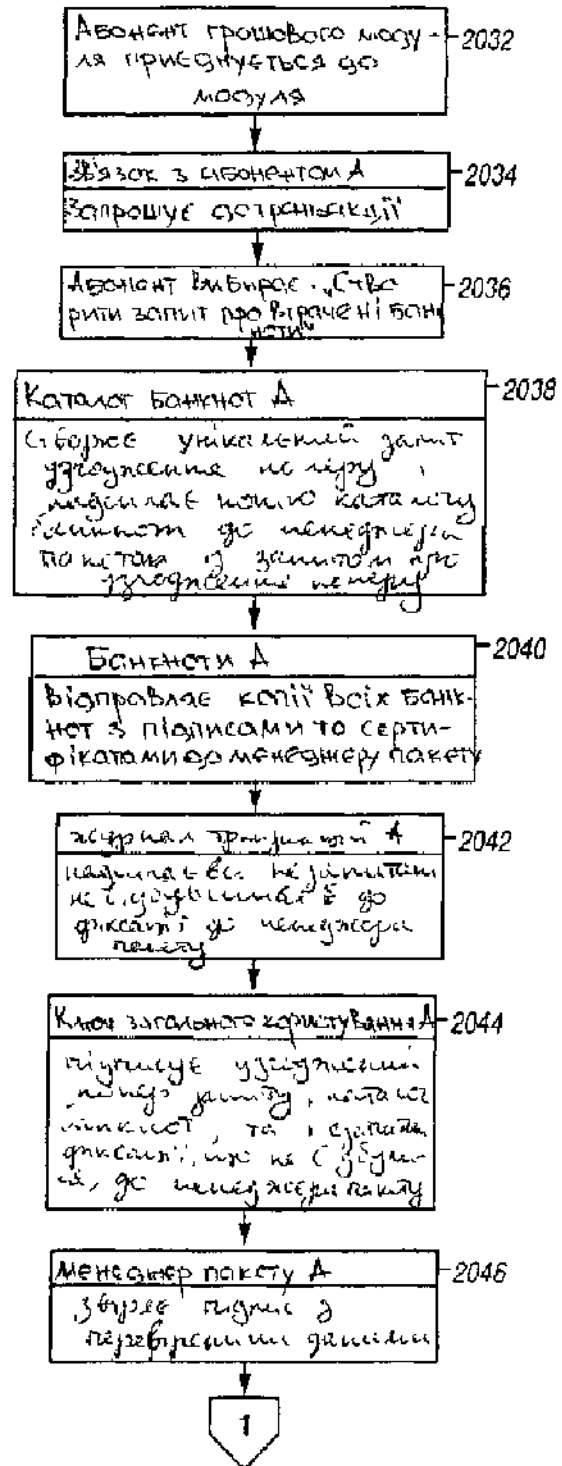
Fig. 19B



Фіг. 19B



Фіг. 20



Фіг. 21A

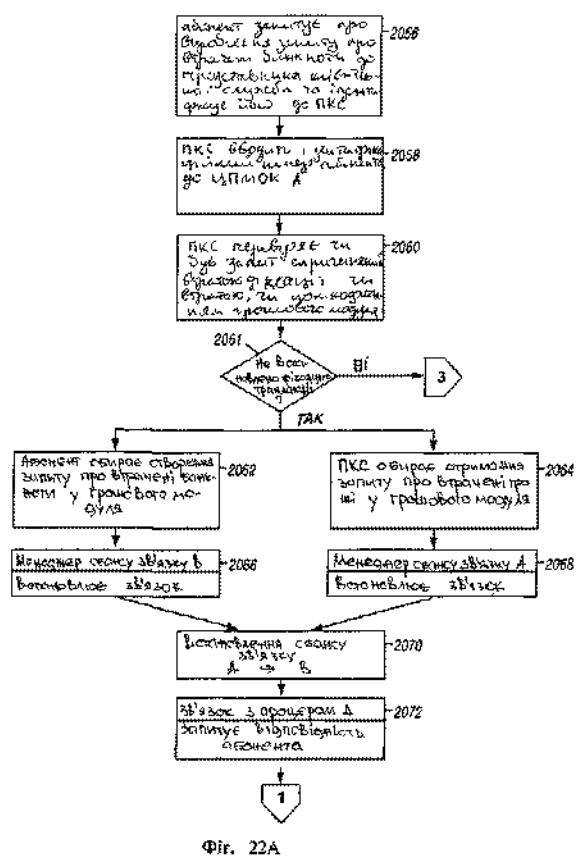
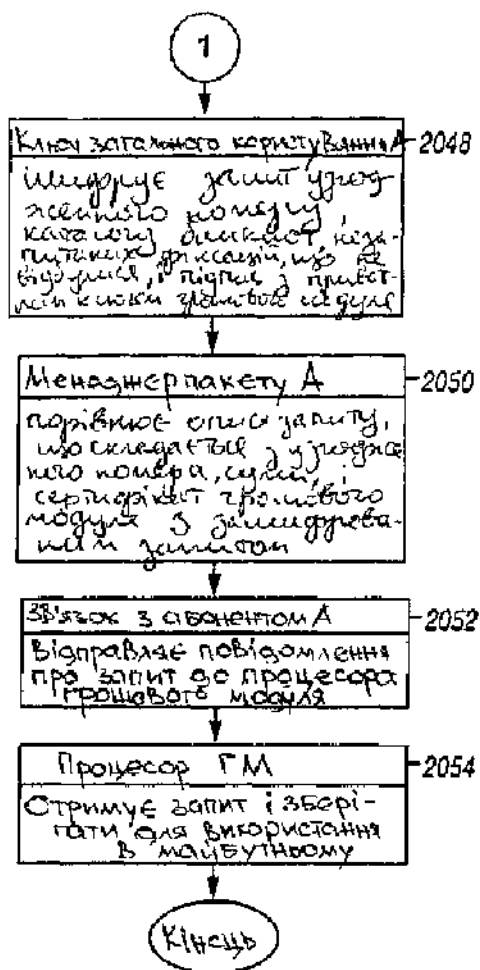
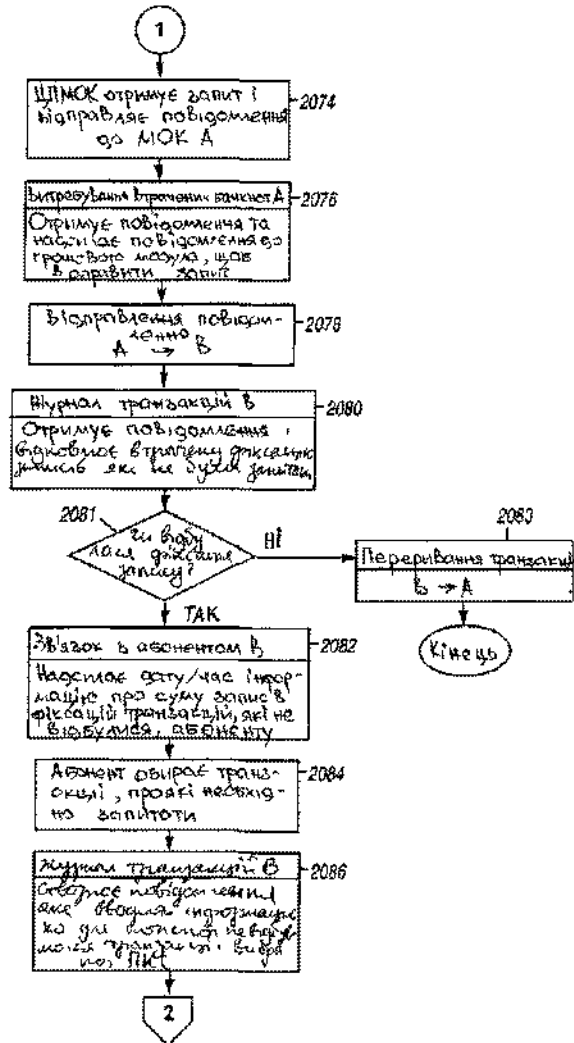
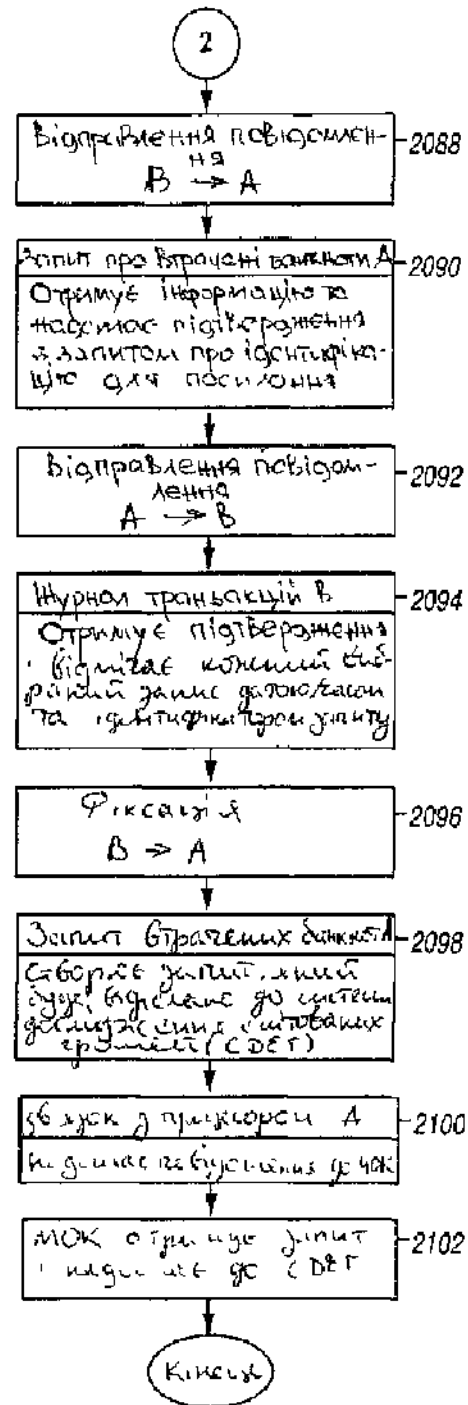


Fig. 22A

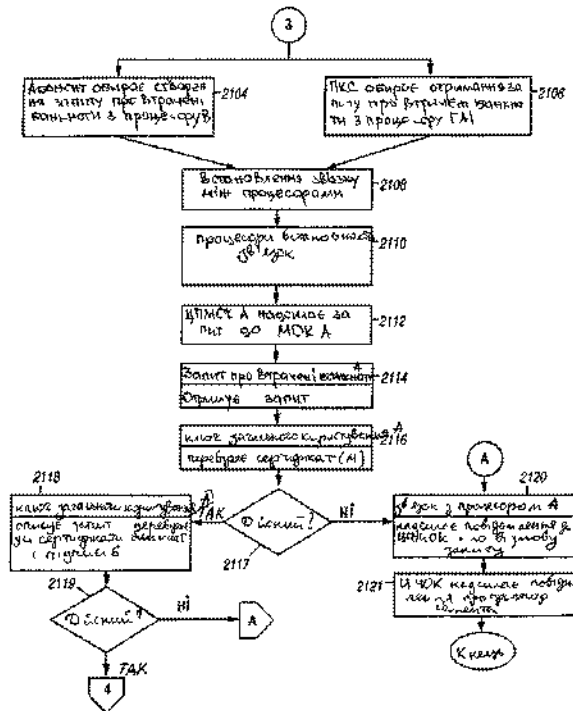
Fig. 21Б



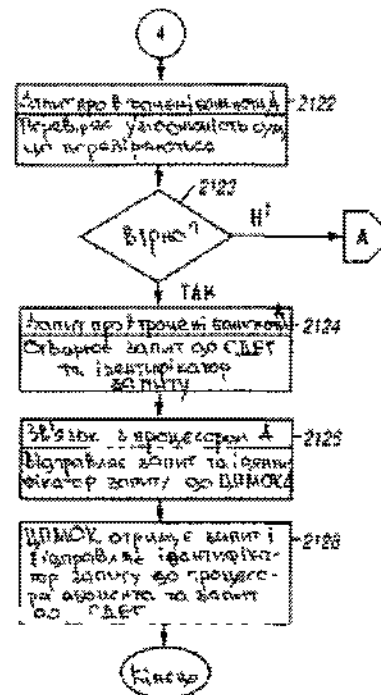
Фіг. 22Б



Фіг. 22В



Фиг. 22Г



Фиг. 22Д

ДП «Український інститут промислової власності» (Укрпатент)

вул. Сім'ї Хохлових, 15, м. Київ, 04119, Україна

(044) 456 – 20 – 90

ТОВ «Міжнародний науковий комітет»

вул. Артема, 77, м. Київ, 04050, Україна

(044) 216 – 32 – 71