



УКРАЇНА

(19) UA (11) 74766 (13) C2  
(51) МПК (2006)  
H04N 7/16  
H04N 7/167

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(54) СИСТЕМА МОВЛЕННЯ І ПРИЙМАННЯ, А ТАКОЖ СИСТЕМА УМОВНОГО ДОСТУПУ ДО НЕЇ

1

(21) 99105532  
(22) 25.04.1997  
(24) 15.02.2006  
(86) PCT/EP97/02108, 25.04.1997  
(31) 97400650.4  
(32) 21.03.1997  
(33) EP  
(46) 15.02.2006, Бюл. № 2, 2006 р.  
(72) Байасі Мулхам, FR, Де Ла Тюле, FR, Жезель Жан-Франсуа, FR  
(73) КАНАЛЬ+ СОСЬТЕ АНОНИМ, FR  
(56) WO 9414284, 23.06.1994  
US 5144663, 01.09.1992  
XP000559450: EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE - ISSN 0251-0936, Nr. 266, Page(s): 64-77, 21.12.1995  
(57) 1. Система умовного доступу для системи мовлення і приймання, яка **відрізняється** тим, що включає в себе:  
засіб генерування множини повідомлень, призначених для надання кінцевому користувачу прав на доступ до однієї або кількох передач, що видаються передавачем системи мовлення і приймання; приймач-декодер для приймання згаданих передач і згаданих повідомлень з метою надання кінцевому користувачу прав на доступ до однієї або кількох зі згаданих передач, а також для передавання у згаданий засіб генерування даних запиту на здійснення відповідного доступу; і комунікаційний сервер, підключений безпосередньо до засобу генерування; причому згаданий засіб генерування виконаний з можливістю генерування повідомлення, призначеного для надання прав, у відповідь на дані запиту, що передаються у засіб генерування приймачем-декодером через згаданий комунікаційний сервер, і з можливістю здійснення зв'язку з приймачем-декодером через згаданий комунікаційний сервер для передавання приймачу-декодеру згаданого повідомлення, призначеного для надання прав.  
2. Система умовного доступу за п.1, яка додатково включає в себе супутниковий транспондер, і в якій згаданий засіб генерування виконаний з можливістю передавання повідомлення, призначеного для надання прав, у приймач-декодер у вигляді пакета цифрових даних або через комунікаційний сервер,

2

або через супутниковий транспондер.  
3. Система умовного доступу за будь-яким з попередніх пунктів, яка **відрізняється** тим, що приймач-декодер виконаний придатним до підключення до комунікаційного сервера через модем і телефонний канал.  
4. Система мовлення і приймання, яка включає в себе систему умовного доступу за будь-яким з попередніх пунктів.  
5. Система мовлення і приймання за п.4, яка **відрізняється** тим, що згаданий комунікаційний сервер виконаний із можливістю організації спеціалізованого з'єднання між приймачем-декодером і засобом генерування.  
6. Система мовлення і приймання за п.5, яка **відрізняється** тим, що додатково включає в себе модем, причому згаданий засіб генерування підключається до цього модему через згаданий комунікаційний сервер.  
7. Система мовлення і приймання за будь-яким з пп.4-6, яка **відрізняється** тим, що згаданий приймач-декодер має засіб читання смарт-карти, що встановлюється в нього кінцевим користувачем, на якій зберігаються дані для автоматичного ініціювання передавання повідомлення від згаданого приймача-декодера у згаданий засіб генерування після встановлення смарт-карти кінцевим користувачем.  
8. Система мовлення і приймання за будь-яким з пп.4-7, яка **відрізняється** тим, що включає в себе голосовий канал для забезпечення користувачу системи мовлення і приймання можливості зв'язуватися з засобом генерування.  
9. Система мовлення і приймання за будь-яким з пп.4-8, яка **відрізняється** тим, що згаданий приймач-декодер має засіб для приймання ущільнених сигналів MPEG-типу, засіб декодування прийнятих сигналів для одержання телевізійного сигналу і засіб для спрямовування телевізійного сигналу в телевізор.  
10. Система умовного доступу для системи мовлення і приймання, призначена для забезпечення умовного доступу передплатникам, яка **відрізняється** тим, що включає в себе:  
систему управління передплатниками для зберігання даних, що стосуються передплати на дану систему мовлення і приймання; систему санкціо-

(19) UA (11) 74766 (13) C2

нування передплатників, підключену до системи управління передплатниками, для використання даних, що приймаються від системи управління передплатниками, при формуванні повідомлень, призначених для надання прав на доступ до однієї або кількох передач, що видаються передавачем системи мовлення і приймання; і комунікаційний сервер, підключений безпосередньо до системи санкціонування передплатників; причому згадана система санкціонування передплатників виконана з можливістю генерування повідомлення, призначеного для надання прав, у відповідь на дані запити на здійснення відповідного доступу, що приймаються через згаданий комунікаційний сервер.

11. Система умовного доступу за п.10, яка **відрізняється** тим, що додатково включає в себе приймач-декодер для передплатника, виконаний з можливістю підключення до згаданого комунікаційного сервера і, отже, до згаданої системи санкціонування передплатників, через модем і телефонний канал.

12. Система умовного доступу за п.11, яка **відрізняється** тим, що включає в себе супутниковий транспондер, причому згадана система санкціонування передплатників виконана з можливістю передавання повідомлення, призначеного для надання прав, у приймач-декодер у вигляді пакета цифрових даних або через комунікаційний сервер, або через супутниковий транспондер.

13. Система умовного доступу за п.11 або 12, яка **відрізняється** тим, що приймач-декодер виконаний придатним до підключення до комунікаційного сервера через модем і телефонний канал.

14. Система умовного доступу за будь-яким з пп.11-13, яка **відрізняється** тим, що повідомлення, призначені для надання прав, генеруються системою санкціонування передплатників у відповідь на команду від приймача-декодера.

15. Система умовного доступу для надання передплатнику доступу до однієї або кількох передач, що видаються передавачем системи мовлення, з використанням приймача-декодера, яка включає в себе комунікаційний сервер, виконаний з можливістю підключення до приймача-декодера передплатника, яка **відрізняється** тим, що також включає в себе: систему управління передплатниками для зберігання даних, що стосуються передплати; і систему санкціонування передплатників для генерування повідомлень, призначених для надання прав доступу, у відповідь на команди, що приймаються через комунікаційний сервер, що включає в себе: централізований сервер замовлень, підключений до комунікаційного сервера для приймання команд від приймача-декодера і даних від системи управління передплатниками; сервер санкціонування, підключений до централізованого сервера замовлень для ідентифікації і перевірки передплатника у відповідь на запит санкціонування від централізованого сервера замовлень; і генератор повідомлень, підключений до централізованого сервера замовлень, для генерування повідомлень, призначених для надання прав доступу, у відповідь на команду, прийняту від централізованого сервера замовлень; причому згаданий централізований сервер замовлень виконаний із можливістю видавання згаданої коман-

ди в генератор повідомлень у відповідь на дані про ідентифікацію і перевірку передплатника, що приймаються від згаданого сервера санкціонування, і/або даних, що стосуються передплати, що приймаються від згаданої системи управління передплатниками, і з можливістю передавання згаданих повідомлень, призначених для надання прав доступу, у приймач-декодер через комунікаційний сервер.

16. Система мовлення і приймання, яка включає в себе, із боку мовлення - систему мовлення, що включає в себе засіб для передавання шляхом мовлення запиту зворотного звертання, і з боку приймання - приймач, що включає в себе засіб для здійснення зворотного звертання до системи мовлення у відповідь на запит зворотного звертання, яка **відрізняється** тим, що вона виконана з можливістю перевірки, чи є даний приймач справжнім, за допомогою згаданого запиту зворотного звертання.

17. Система мовлення і приймання за п.16, яка **відрізняється** тим, що система мовлення має засіб для генерування контрольного повідомлення і передавання його в приймач, приймач має засіб для шифрування контрольного повідомлення і передавання його в систему мовлення, і система мовлення додатково має засіб для дешифрування контрольного повідомлення, прийнятого від приймача, і порівняння його з оригінальним контрольним повідомленням.

18. Система за п.16 або 17, яка **відрізняється** тим, що засіб мовлення виконаний з можливістю передавання шляхом мовлення запиту зворотного звертання, що містить команду, відповідно до якої зворотне звертання має бути здійснене у певний заданий час, і засіб для здійснення зворотного звертання до системи мовлення виконаний з можливістю діяти у відповідь на таку команду.

19. Система мовлення і приймання, яка включає в себе, із боку мовлення - систему мовлення, що включає в себе засіб для передавання шляхом мовлення запиту зворотного звертання, і з боку приймання - приймач, що включає в себе засіб для здійснення зворотного звертання до системи мовлення у відповідь на запит зворотного звертання, яка **відрізняється** тим, що запит зворотного звертання містить команду, відповідно до якої зворотне звертання має бути здійснене у певний заданий час, і засіб для здійснення зворотного звертання до системи мовлення виконаний з можливістю діяти у відповідь на таку команду.

20. Система за будь-яким з пп.16-19, яка **відрізняється** тим, що засіб для здійснення зворотного звертання до системи мовлення включає в себе модем, виконаний з можливістю підключення до телефонної мережі.

21. Система за будь-яким з пп.16-20, яка **відрізняється** тим, що засіб для здійснення зворотного звертання до системи мовлення виконаний з можливістю передавання в систему мовлення інформації про приймач.

22. Система по п.21, яка **відрізняється** тим, що система мовлення має засіб для зберігання згаданої інформації.

23. Система за будь-яким з пп.16-22, яка **відрізняється** тим, що засіб мовлення виконаний з мо-

жливістю мовлення як запиту зворотного звертання щонайменше одного повідомлення, призначеного для надання прав.

24. Система за будь-яким з пп.16-23, яка **відрізняється** тим, що запит зворотного звертання містить команду, що вказує задану кількість спроб і інтервали між спробами здійснення зворотного

звертання.

25. Система за будь-яким з пп.16-24, яка **відрізняється** тим, що запит зворотного звертання містить команду, що вказує щонайменше один заданий номер телефону, що має бути набраний засобом для здійснення зворотного звертання при відповіді на запит зворотного звертання.

Запропонований винахід відноситься до систем мовлення і приймання, зокрема, до систем цифрового інтерактивного супутникового телебачення, орієнтованих на масовий ринок, і систем умовного доступу для них.

Зокрема, винахід відноситься до систем мовлення для масового споживача, що має деякі або всі з вказаних нижче суттєвих особливостей (але не лише до таких систем!):

- це системи передавання інформації шляхом мовлення, у варіанті, якому віддається перевага - системи радіо- і/або телевізійного мовлення;
- це супутникові системи (хоча винахід може використовуватися для кабельного або наземного передавання);
- це цифрові системи, у яких для передавання даних/сигналів у варіанті, якому віддається перевага, використовується система ущільнення MPEG, а у варіанті, якому віддається більша перевага - MPEG-2;
- вони уможливають інтерактивність.

Більш конкретно, запропонований винахід відноситься до так званого платного телебачення (або радіо). В таких системах користувач/глядач вибирає для перегляду програму/фільм/гру, що мусить бути оплачена. Це називається сплатою за перегляд (PPV - Pay Per View, користувач сплачує за кожну переглянута передачу) або, у випадку завантаження даних - пофайловою сплатою (PPF).

У відомих PPV- і PPF-системах користувач/глядач має витратити значний час на виконання дій, необхідних для фактичного одержання доступу до вибраного продукту.

Наприклад, в одній відомій системі мають бути виконані такі кроки:

i) користувач телефонує у так звану систему управління передплатниками (SMS), що у цій відомій системі включає декілька людей-операторів, які відповідають на дзвінок передплатника і яким передплатник повідомляє інформацію про вибраний продукт, а також інформацію, що стосується фінансового стану передплатника, для так званої системи санкціонування передплатників (SAS), що включає в себе множину комунікаційних серверів, або є підключена до них;

ii) після цього оператор системи SMS повинен перевірити фінансовий стан користувача, перед тим як санкціонувати зв'язок між комунікаційними серверами і телевізором користувача для доставки продукту користувачу і подальшого перегляду продукту користувачем.

В іншій відомій системі людина-оператор замінюється автоматичним голосовим сервером, так що коли користувач телефонує до SMS, він чує

запис, що активується голосом, на який користувач повідомляє ту ж саму інформацію, що й у пункті i) вище.

В останній системі зменшується затримка, що має місце в першій з описаних систем, яка більш схильна до перевантажень у випадках, коли велика кількість користувачів бажає одночасно замовити певний продукт.

Проте навіть у другій системі користувачеві доводиться вводити значний обсяг інформації у вигляді довгої послідовності цифр, і ця операція з великою імовірністю може призводити до великого числа помилок, при цьому займаючи багато часу.

Третя відома система передбачає використання користувачем відомих екранних систем, таких як MINITEL у Франції або PRESTEL у Великобританії, що заміняє сервер, що активується голосом, згаданий вище при розгляді другої системи. Системи MINITEL і PRESTEL передбачають наявність модему із боку користувача.

В усіх цих відомих системах користувач змушений витрачати багато часу і зусиль для введення всієї тієї інформації, що необхідна системі для санкціонування передавання вибраного продукту в телевізор користувача.

У випадку системи супутникового телебачення виникає додаткова затримка фактичного приймання користувачем вибраного продукту.

У PPV- і PPF-системах ключовими елементами управління доступом користувачів до продуктів є так звані повідомлення керування доступом (EMM - Entitlement Management Messages), які повинні бути введені в систему для того, щоб надати користувачеві доступ до продукту. Більш конкретно, EMM є тим механізмом, за допомогою якого зашифровані дані, що, власне, і утворюють собою продукт, розшифровуються для конкретного окремого користувача.

У відомих системах супутникового телебачення EMM передаються в телевізори користувачів по супутниковому каналу в потоку даних MPEG-2 через однакові інтервали часу. Отже, при одержанні EMM певним конкретним користувачем може трапитися значна затримка, тривалістю до декількох хвилин, до того, як переданий наступний EMM для цього користувача надійде в телевізор даного користувача.

Ця затримка передавання додається до згаданої вище затримки, що виникає внаслідок того, що користувач змушений вводити дані в систему вручну. Накопичення цих затримок призводить до того, що для одержання доступу до вибраного продукту користувачу може знадобитися витратити, наприклад, п'ять хвилин.

Даний винахід має на меті подолання цієї проблеми.

Відповідно до першого аспекту даного винаходу пропонується система умовного доступу, яка включає в себе:

засіб для генерування множини повідомлень (у варіанті, якому віддається перевага - повідомлень умовного доступу); і

засіб для приймання згаданих повідомлень, виконаний з можливістю обміну даними зі згаданим засобом генерування через комунікаційний сервер, підключений безпосередньо до згаданого засобу генерування.

Переважно згадане повідомлення є повідомленням щодо прав, призначеним для передавання (наприклад, шляхом мовлення) у засіб приймання, причому згаданий засіб генерування виконаний з можливістю генерування повідомлень щодо прав у відповідь на дані, одержані від згаданого засобу приймання.

Засіб генерування може бути виконаний з можливістю передавання повідомлення у згаданий засіб приймання у вигляді пакета цифрових даних, або через згаданий комунікаційний сервер, або через супутниковий транспондер.

Засіб приймання може бути виконаний з можливістю підключення до згаданого комунікаційного сервера через модем і телефонний канал.

Відповідно до спорідненого аспекту даного винаходу пропонується система умовного доступу для уможливлення умовного доступу передплатників, яка включає в себе:

систему управління передплатниками; систему санкціонування передплатників, підключену до системи управління передплатниками; і комунікаційний сервер, підключений безпосередньо до системи санкціонування передплатників.

Така система може додатково включати в себе приймач-декодер для передплатника, виконаний з можливістю підключення до згаданого сервера і, отже, до згаданої системи санкціонування передплатників, через модем і телефонний канал.

Відповідно до другого аспекту даного винаходу пропонується система мовлення і приймання, яка включає в себе систему умовного доступу, описану вище.

Відповідно до третього аспекту даного винаходу пропонується систему мовлення і приймання, яка включає в себе:

засіб для генерування множини повідомлень щодо прав, які стосуються програм, що передаються шляхом мовлення;

засіб для приймання згаданих повідомлень від згаданого засобу генерування; і

засіб для з'єднання засобу приймання з засобом генерування для приймання згаданих повідомлень, причому цей засіб для з'єднання виконаний з можливістю організації спеціалізованого з'єднання між засобом приймання і засобом генерування.

Спеціалізоване з'єднання звичайно являє собою дротове з'єднання і/або мод ємне з'єднання, із можливістю організації такого з'єднання через стільникову телефонну систему. Іншими словами, спеціалізоване з'єднання утворює канал передавання інформації ("точка-точка"), на протилугу пе-

редаванню інформації шляхом мовлення через ефір або навколишнє середовище. Засіб для з'єднання, як правило, включає в себе модем з боку користувача.

Відповідно, спорідненим аспектом даного винаходу пропонується система мовлення і приймання, яка включає в себе:

засіб для генерування множини повідомлень щодо прав, які стосуються програм, що передаються шляхом мовлення;

засіб для приймання згаданих повідомлень від згаданого засобу генерування через модем; і

засіб для з'єднання згаданого модему зі згаданим засобом генерування і згаданим засобом приймання.

Розкриті вище особливості уможливають надання користувачу необхідних прав перегляду (за допомогою EMM) швидше, ніж це було можливо раніше, частково тому, що, оскільки SAS звичайно реалізується меншою кількістю програмного коду, ніж SMS, SAS може працювати більш ефективно (і в реальному часі), частково тому, що SAS може сама безпосередньо генерувати необхідне EMM, і частково тому, що EMM може передаватися користувачу або передплатнику через спеціалізований (як правило, модемний) канал.

У варіанті, якому віддається перевага, засіб генерування з'єднується із згаданим модемом через комунікаційний сервер, що у варіанті, якому віддається перевага, входить до складу згаданого засобу генерування або підключений до нього.

Засіб приймання може бути також виконаний з можливістю приймання згаданих повідомлень щодо прав через супутниковий транспондер.

Засіб приймання може являти собою приймач-декодер, що має засіб для приймання ущільненого сигналу MPEG-типу, засіб для декодування прийнятого сигналу для одержання телевізійного сигналу і засіб для спрямовування телевізійного сигналу в телевізор.

У варіанті, якому віддається перевага, засіб приймання виконаний з можливістю обміну інформацією зі згаданим засобом генерування через згаданий модем і засіб з'єднання. Засіб приймання може включати в себе засіб читання смарт-карти, що встановлюється в нього кінцевим користувачем, на якій зберігаються дані для автоматичного ініціювання передавання повідомлення від згаданого засобу приймання у згаданий засіб генерування після встановлення смарт-карти кінцевим користувачем.

Крім цього, система може додатково включати в себе голосовий канал для забезпечення користувачу системи мовлення і приймання можливості зв'язуватися з засобом генерування.

Як буде зрозуміло зі сказаного вище, даний винахід пропонує два заходи, завдяки яким скорочується час, що витрачається кінцевим користувачем для доступу до жаданого продукту. У варіанті, якому віддається перевага, для досягнення максимальної економії часу застосовуються обидва заходи, проте можливим є й незалежне застосування кожного з них.

Відповідно до ще одного аспекту даного винаходу пропонується система мовлення і приймання, яка включає в себе:

із боку мовлення - систему мовлення, що включає в себе засіб для передавання шляхом мовлення запиту зворотного звертання;

з боку приймання - приймач, що включає в себе засіб для зворотного звертання до системи мовлення у відповідь на запит зворотного звертання.

Завдяки тому, що система мовлення може запитати від приймача зворотне звертання, системі мовлення забезпечується можливість одержання інформації від приймача про стан приймача.

У варіанті, якому віддається перевага, засіб для зворотного звертання до системи мовлення включає в себе модем, виконаний з можливістю підключення до телефонної мережі. Використання зворотного модемного каналу надає простий шлях реалізації винаходу на практиці.

У варіанті, якому віддається перевага, засіб для здійснення зворотного звертання до системи мовлення виконаний з можливістю передавання в систему мовлення інформації, що стосується приймача. Це інформація може включати в себе кількість "юнітів", що залишилися, кількість попередньо замовлених сеансів тощо.

У варіанті, якому віддається перевага, система мовлення включає в себе засіб для збереження згаданої інформації для її наступної обробки в разі потреби.

У варіанті, якому віддається перевага, засіб мовлення виконаний з можливістю передавання шляхом мовлення запиту зворотного звертання, що містить команду, відповідно до якої зворотне звертання має відбутися у певний заданий час, і засіб для здійснення зворотного звертання до системи мовлення виконаний з можливістю відповідати на згадану команду. Шляхом забезпечення можливості зворотного звертання після того, як запит було отримано (тобто пізніше), забезпечується додаткова гнучкість системи.

Засіб мовлення може бути виконаний з можливістю передавання шляхом мовлення як згаданого запиту зворотного звертання одного або декількох повідомлень щодо прав.

У варіанті, якому віддається перевага, система мовлення включає в себе засіб для генерування контрольного повідомлення (наприклад, випадкового числа) і передавання його в приймач, приймач включає в себе засіб для шифрування контрольного повідомлення і його передавання в систему мовлення, і система мовлення додатково включає в себе засіб для дешифрування контрольного повідомлення, прийнятого від приймача, і порівняння його з оригінальним контрольним повідомленням. У такий спосіб можна перевірити, чи є приймач дійсним і оригінальним.

Будь-які з перерахованих вище особливостей можуть бути об'єднані в будь-якій необхідній комбінації. Вони можуть також надаватися, при необхідності, в аспектах, що стосуються способу.

Особливості даного винаходу, яким віддається перевага, будуть описані нижче, шляхом опису одного з прикладів, із посиланнями на такі фігури:

На Фіг.1 зображена загальна архітектура системи цифрового телебачення, що відповідає переважному варіанту реалізації даного винаходу;

На Фіг.2 зображена архітектура системи умов-

ного доступу системи цифрового телебачення;

На Фіг.3 зображена структура EMM, що використовується в системі умовного доступу;

Фіг.4 являє собою схематичне зображення апаратних засобів системи санкціонування передплатників (SAS) відповідно до одного варіанту реалізації даного винаходу, якому віддається перевага;

Фіг.5 являє собою схематичне зображення архітектури SAS;

Фіг.6 являє собою схематичне зображення сервера технічного управління передплатниками, що є частиною SAS;

Фіг.7 являє собою блок-схему процедури автоматичного відновлення передплат, реалізовану в SAS;

Фіг.8 являє собою схематичне зображення бітового масиву групи передплатників, що використовується в процедурі автоматичного відновлення;

На Фіг.9 зображена структура EMM, що використовується в процедурі автоматичного відновлення;

На Фіг.10 докладно зображена структура EMM;

Фіг.11 являє собою схему централізованого сервера замовлень, при його використанні для приймання команд безпосередньо через комунікаційні сервери;

На Фіг.12 зображена схема, що ілюструє частину Фіг.2, де показаний один із варіантів реалізації даного винаходу;

Фіг.13 являє собою схему централізованого сервера замовлень, при його використанні для приймання команд від системи санкціонування передплатників для запиту зворотного звертання.

Фіг.14 являє собою схематичне зображення комунікаційних серверів;

Фіг.15 ілюструє змінювання частоти циклічного видавання EMM у залежності від часу передавання PPV-програми.

Фіг.16 являє собою схематичне зображення джерела повідомлень для видавання EMM;

Фіг.17 ілюструє спосіб збереження EMM у джерелі повідомлень;

Фіг.18 являє собою схематичне зображення смарт-карти;

Фіг.19 являє собою схематичне зображення розміщення розділів у пам'яті смарт-карти;

Фіг.20 являє собою схематичне зображення опису PPV-програми.

Загальна структура системи 1000 мовлення і приймання цифрового телебачення відповідно до даного винаходу наведена на Фіг.1. Винахід включає практично звичайну систему 2000 цифрового телебачення, що використовує відому систему ущільнення MPEG-2 для передавання ущільнених цифрових сигналів. Більш докладно, пристрій ущільнення MPEG-2 2002 у центрі мовлення приймає потік цифрових сигналів (звичайно потік відеосигналів). Пристрій ущільнення 2002 підключений до мультиплексору і скремблеру 2004 за допомогою каналу 2006. Мультиплексор 2004 приймає множини вхідних сигналів, збирає один або декілька несучих потоків і передає ущільнені цифрові сигнали в передавач 2008 центру мовлення через канал 2010, тип якого може бути різноманітним, включаючи телекомунікаційні канали. Передавач

2008 передає електромагнітні сигнали через канал "Земля-супутник" 2012 на супутниковий транспондер 2014, де виконується їхня обробка електронними засобами і передавання шляхом мовлення через віртуальний канал "супутник-земля" 2016 на наземний приймач 2018, що звичайно має форму тарілки, який належить кінцевому користувачу або арендований ним. Сигнали, прийняті приймачем 2018, передаються в суміщений приймач-декодер 2020, що належить кінцевому користувачу або арендований ним, і підключений до телевізора 2022 кінцевого користувача. Приймач-декодер 2020 декодує ущільнений MPEG-2 сигнал у телевізійний сигнал для телевізора 2022.

Система 3000 умовного доступу підключена до мультиплексора 2004 і приймача-декодера 2020 і розташована частково в центрі мовлення і частково в декодері. Вона дозволяє кінцевому користувачу здійснювати доступ до передач цифрового телебачення, що передаються шляхом мовлення, одного або декількох провайдерів мовлення. У приймач-декодер 2020 може встановлюватися смарт-карта, що може декодувати повідомлення, які стосуються комерційних пропозицій (одна або декілька телевізійних програм, що продаються провайдером мовлення). З використанням декодера і смарт-карти користувач може купувати передачі в режимі передплати або PPV-режимі.

Інтерактивна система 4000, також підключена до мультиплексора 2004 і приймача-декодера 2020 і також розміщена частково в центрі мовлення і частково в декодері, дозволяє кінцевому користувачу взаємодіяти з різноманітними прикладними програмами через модемний зворотний канал 4002.

Нижче буде описана більш докладно система умовного доступу 3000.

Як показано на Фіг.2, говорячи взагалі, система умовного доступу 3000 включає систему санкціонування передплатників (SAS) 3002. SAS 3002 підключена до однієї або більш систем управління передплатниками (SMS) 3004, по одній SMS для кожного провайдера мовлення, за допомогою відповідного TCP/IP-каналу 3006 (хоча в альтернативних реалізаціях замість нього можуть використовуватися канали інших типів). У альтернативному варіанті одна або декілька SMS можуть використовуватися спільно двома провайдерами мовлення, або один провайдер може використовувати дві SMS тощо.

Перші пристрої шифрування у вигляді шифрувальних блоків 3008, що використовують "материнські" смарт-карти 3010, підключаються до SAS через канал 3012. Другі пристрої шифрування, також у вигляді шифрувальних блоків 3014, що використовують материнські смарт-карти 3016, підключаються до мультиплексору 2004 через канал 3018. Приймач-декодер 2020 приймає "дочірню" смарт-карту 3020. Він підключається безпосередньо до SAS 3002 за допомогою комунікаційних серверів 3022 через модемний зворотний канал 4002. SAS, поряд з іншими сигналами, за запитом надсилає в дочірню карту права передплати.

Смарт-карти містять "секрети" одного або декількох комерційних операторів. "Материнська" смарт-карта шифрує різноманітні види повідом-

лень, а "дочірні" смарт-карти розшифровують ці повідомлення, якщо в них є на це права.

Перший і другий шифрувальні блоки 3008 і 3014 містять шасі, електронну плату VME, програмне забезпечення якої є записаним в програмованому ПЗП з електричним стиранням, до 20 електронних плат і одну смарт-карту 3010 і 3016 відповідно для кожної електронної плати, одну (карта 3016) для шифрування ECM і одну (карта 3010) для шифрування EMM.

Нижче буде описана докладніше робота системи умовного доступу 3000 системи цифрового телебачення, зокрема різні компоненти системи телебачення 2000 і системи умовного доступу 3000.

Мультиплексор і скремблер

На Фіг.1 і 2 показано, що в центрі мовлення цифровий відеосигнал спочатку ущільнюється (або швидкість передавання зменшується) із використанням пристрою ущільнення MPEG-2 2002. Цей ущільнений сигнал потім передається в мультиплексор і скремблер 2004 через канал 2006 для того, щоб мультиплексувати його з іншими даними, такими як інші ущільнені дані.

Скремблер генерує слово керування, яке використовується в процесі скремблювання і яке включається в потік даних MPEG-2 у мультиплексорі 2004. Слово керування генерується усередині системи і уможливорює дескремблювання програми суміщеним приймачем-декодером 2020 кінцевого користувача.

У потік даних MPEG-2 додаються також критерії доступу, що вказують, яким способом програма пропонується споживачам. Програма може пропонуватися як в однім із багатьох режимів "передплати", так і/або в однім із багатьох PPV-режимів. У режимі передплати кінцевий користувач передплачує одну або декілька комерційних пропозицій, або "букети", одержуючи, таким чином, права на перегляд будь-якого каналу з цих букетів. У переважному варіанті реалізації з букета каналів можна вибрати до 960 комерційних пропозицій. У PPV-режимі кінцевому користувачу дається можливість купувати передачі за бажанням. Це може забезпечуватися шляхом попереднього замовлення передач ("режим попереднього замовлення") або шляхом придбання програми відразу після початку мовлення ("імпульсивний режим"). У варіанті втілення, якому віддається перевага, всі користувачі є передплатниками незалежно від режиму перегляду - передплата або PPV, але, звичайно, PPV-глядачі не обов'язково повинні бути передплатниками.

Слово керування і критерії доступу використовуються для формування повідомлення ECM; це повідомлення є повідомленням, що передається разом з однією скремблюваною програмою. Це повідомлення містить слово керування (яке дозволяє дескремблювати програму) і критерії доступу для програми, що передається шляхом мовлення. Критерії доступу і слово керування передаються на другий шифрувальний блок 3014 через канал 3018. У цьому блоці ECM генерується, зашифровується і передається в мультиплексор і скремблер 2004.

Кожний сервіс, що передається провайдером

мовлення в потоці даних, містить декілька окремих компонент; наприклад, телевізійна програма включає відеокomпоненту, аудіокomпоненту, ком-поненту субтитрів тощо. Кожна з цих компонент сервісу для подальшого мовлення скремблюється і зашифровується окремо. Для кожної скремблю-ваної компоненти послуги потрібно окремих ECM.

#### Передавання програми

Мультіплексор 2004 приймає електричні сиг-нали, що містять зашифровані EMM, від SAS 3002, зашифровані ECM від другого шифрувального блоку 3014 і ущільнені програми від пристрою ущільнення 2002. Мультіплексор 2004 скремблює програми і передає скремблювані програми, скремблювані EMM і скремблювані ECM у вигляді електричних сигналів на передавач 2008 центру мовлення через канал 2010. Передавач 2008 пе-редає електромагнітні сигнали на супутниковий транспондер 2014 через канал "Земля-супутник" 2012.

#### Приймання програм

Супутниковий транспондер 2014 приймає й обробляє електромагнітні сигнали, передані пере-давачем 2008, і передає ці сигнали на наземний приймач 2018, що звичайно має форму тарілки, який належить кінцевому користувачу або арендо-ваний ним, через канал "супутник-Земля". Сигна-ли, прийняті приймачем 2018, передаються в су-міщений приймач-декодер 2020, що належить кінцевому користувачу або арендований ним, і підключений до телевізора кінцевого користувача 2022. Приймач-декодер 2020 демультіплексує сигнали з метою одержання скремблюваних про-грам із зашифрованими EMM і зашифрованими ECM.

Якщо програма не скремблювана, тобто з по-током даних MPEG-2 ECM не передається, при-мач-декодер 2020 виконує декомпресію даних і перетворює сигнал у відеосигнал для передавання його в телевізор 2022.

Якщо програма скремблювана, приймач-декодер 2020 добуває з потоку даних MPEG-2 від-повідне ECM і передає ECM у "дочірню" смарт-карту 3020 кінцевого користувача. Вона встанов-люється у відповідне гніздо приймача-декодера 2020. Дочірня смарт-карта 3020 контролює, чи має користувач права на дешифрування даного ECM і на доступ до даної програми. Якщо немає, то в приймач-декодер 2020 передається негативний результат, що вказує, що програма не може бути дескремблювана. Якщо кінцевий користувач має такі права, ECM розшифровується і добувається слово керування. Декодер 2020 може потім де-скремблювати програму з використанням даного слова керування. Потім виконується декомпресія потоку даних MPEG-2 і його перетворення у віде-осигнал для подальшого передавання в телевізор 2022.

#### Система управління передплатниками (SMS)

Система управління передплатниками (SMS) 3004 включає в себе базу даних 3024, що управ-ляє, крім іншого, усіма файлами кінцевих користу-вачів, комерційними пропозиціями (такими як та-рифи і заохочення), передплатами, інформацією, що відноситься до PPV, і даними, що стосуються споживання і санкціонування кінцевого користува-

ча. SMS може бути фізично віддалена від SAS.

Кожна SMS 3004 передає в SAS 3002 через відповідний канал 3006 повідомлення, що зумов-люють перетворення або створення повідомлень керування доступом (EMM), що підлягають пере-даванню кінцевому користувачу.

SMS 3004 також передає в SAS 3002 повідом-лення, що не передбачають ніякого перетворення або створення повідомлень EMM, але передбача-ють лише зміну стану кінцевого користувача (щодо санкціонування, наданого кінцевому користувачу при замовленні продукту, або суми, на яку кінце-вий користувач буде дебітований).

Як буде описано нижче, SAS 3002 передає по-відомлення (що звичайно запитують інформацію, таку як інформація, що надається за запитом зво-ротного звертання, або білінгова інформація) у SMS 3004, так що очевидно, що обмін даними між цими двома системами є двостороннім.

#### Повідомлення керування доступом (EMM)

EMM - це повідомлення, призначене для інди-відуального кінцевого користувача (передплатни-ка) або групи кінцевих користувачів (на противагу ECM, що призначається лише для однієї скремб-льованої програми або набору скремблюваних програм, що представляють частину однієї комер-ційної пропозиції). Кожна група може містити зада-ну кількість кінцевих користувачів. Така організація у вигляді групи має на меті оптимізувати викорис-тання смуги пропускання; таким чином, звернення до однієї групи може уможливити звернення до великої кількості кінцевих користувачів.

При практичному втіленні даного винаходу ви-користовуються різні спеціальні типи EMM. Індиві-дуальні EMM призначені для окремих передплат-ників і звичайно використовуються при наданні PPV-послуг; вони містять ідентифікатор групи і позицію передплатника в цій групі. Так звані "гру-пові" EMM (групової передплати) призначені для груп із, наприклад, 256 окремих користувачів, і використовуються звичайно для адміністрування деяких передплачуваних сервісів. Таке EMM міс-тить ідентифікатор групи і бітовий масив групи передплатників. Аудиторні EMM призначені для всієї аудиторії глядачів і можуть, наприклад, вико-ристовуватися операторами для надання деяких безкоштовних послуг. "Аудиторія" - це вся сукуп-ність передплатників, що мають смарт-карти з од-наковими ідентифікаторами оператора (OPI – OPerator Identifier). І, нарешті, "унікальні" EMM ад-ресовані для унікальних ідентифікаторів смарт-карт.

Структура типового EMM подана на Фіг.3. У загальному випадку, EMM, що реалізується у ви-гляді послідовності бітів цифрових даних, склада-ється з заголовка 3060, власне EMM 3062 і підпису 3064. Заголовок 3060, у свою чергу, складається з ідентифікатора типу 3066 для ідентифікації типу EMM - індивідуальний, груповий, аудиторний або якийсь інший, ідентифікатора розміру 3068, що вказує розмір EMM, необов'язкової адреси 3070 для EMM, ідентифікатора оператора 3072 і іден-тифікатора ключа 3074. Власне EMM, природно, істотно різняться в залежності від його типу. І, на-решті, підпис 3064, що як правило має розмір 8 байтів, містить інформацію для боротьби зі спо-

творенням інших даних у EMM.

Система санкціонування передплатників (SAS)

Повідомлення, що генеруються SMS 3004, передаються через канал зв'язку 3006 у систему санкціонування передплатників (SAS) 3002, яка, у свою чергу, генерує повідомлення, що підтверджують приймання повідомлень, що генеруються SMS 3004, і передає ці підтвердження в SMS 3004.

Як показано на Фіг.4, на рівні апаратних засобів SAS, як то є відомим, складається з мейнфрейм-комп'ютера 3050 (у переважному варіанті реалізації - комп'ютера DEC), підключеного до однієї або декількох клавіатур 3052 для введення даних і команд, одним або декількома відеомоніторами (VDU – Visual Display Unit) 3054 для відображення вихідної інформації і засобами 3056 збереження даних. Може мати місце деяка надмірність апаратних засобів.

На рівні програмного забезпечення в переважному варіанті реалізації SAS під управлінням стандартної відкритої операційної системи VMS виконує комплекс програмних засобів, архітектура яких буде описана нижче в загальному вигляді з посиланням на Фіг.5; очевидно, що програмні засоби можуть бути, як альтернатива, реалізовані апаратно.

У загальному вигляді, SAS містить область гілки передплати 3100 для надання прав у режимі передплати і для щомісячного автоматичного відновлення прав, область гілки PPV 3200 для надання прав для PPV-передач, і інжектор EMM 3300 для передавання повідомлень EMM, утворюваних в областях гілок передплати і PPV, у мультиплексорі і скремблері 2004 з їх подальшим спрямуванням у потік даних MPEG. Якщо мають бути надані інші права, такі як права пофайлової оплати (PPF – Pay Per File) у випадку завантаження комп'ютерного програмного забезпечення в персональний комп'ютер користувача, передбачаються також інші подібні області.

Однією з функцій SAS 3002 є управління правами доступу до телевізійних програм, що пропонується як комерційні пропозиції в режимі передплати або у PPV-режимі відповідно до різноманітних комерційних режимів (режим попереднього замовлення, імпульсивний режим). SAS 3002, відповідно до прав і інформації, прийнятими від SMS 3004, генерує для передплатника повідомлення EMM.

Область гілки передплати 3100 включає інтерфейс команд (CI – Command Interface) 3102, сервер технічного управління передплатниками (STM – Subscriber Technical Management) 3104, генератор повідомлення (MG – Message Generator) 3106 і шифрувальний блок (CU – Ciphering Unit) 3008.

Область гілки PPV 3200 містить сервер санкціонування (AS – Authorization Server) 3202, реляційну базу даних 3204 для збереження необхідної інформації про кінцевих користувачів, базу даних 3205 локального чорного списку, сервери 3206 баз даних для зазначеної бази даних, централізований сервер замовлень (OCS – Order Centralized Server) 3207, сервер для мовників (SPB) 3208, генератор повідомлень (MG) 3210, функції якого в основному ті ж, що і генератора повідомлень області гілки передплати, і тому далі докладно не описуються, і

шифрувальний блок 3008.

Інжектор EMM 3300 складається з множини джерел повідомлень (ME – Message Emitters) 3302, 3304, 3306 і 3308 і програмних мультиплексорів (SMUX – Software MultipleXer) 3310 і 3312. У переважному варіанті реалізації є два ME, 3302 і 3304, для MG 3106, і два інших ME, 3306 і 3308, для MG 3210. ME 3302 і 3306 підключаються до SMUX 3310, а ME 3304 і 3308 підключаються до SMUX 3312.

Кожний із трьох головних компонентів SAS (область гілки передплати, область гілки PPV і інжектор EMM) нижче буде розглянутий докладніше.

Область гілки передплати

Розглянемо спочатку область гілки передплати 3100, у якій інтерфейс команд CI 3102 призначений у першу чергу для відправлення повідомлень із SMS 3004 у сервер STM 3104, а також у OCS 3207, і з OCS у SMS. Інтерфейс команд приймає від SMS, як вхідні дані, як безпосередні команди, так і пакетні файли, що містять команди. Він виконує синтаксичний аналіз повідомлень, що надходять від сервера STM, і може формувати коректні повідомлення у випадку, якщо в прийнятому повідомленні міститься помилка (параметр поза межами діапазону, параметр пропущений тощо). Він протоколює команди, що надходять, у текстовій формі у файлі трасування 3110 і в двійковій формі у файлі відтворення 3112, для того щоб мати можливість відтворити послідовність команд. Протоколювання може бути відключене і розмір файла обмежений.

Тепер перейдемо до докладного опису сервера STM 3104 із використанням Фіг.6. Сервер STM фактично є ядром області гілки передплати, і його задачею є керування безплатними правами, підключення нових передплатників і відновлення існуючих передплатників. Як показано на Фіг.6, команди передаються в генератор повідомлень MG 3106, але в іншому форматі, відмінному від того, у якому вони передаються у сервер STM. Сервер STM виконаний з можливістю передавання повідомлення підтвердження для кожної команди в CI лише тоді, коли відповідна команда успішно оброблена і передана BMG.

Сервер STM містить базу даних передплатників 3120, у якій зберігається вся інформація про передплатників (номер смарт-карти, комерційні пропозиції, стан, група і положення в групі і т.д.). База даних виконує семантичні перевірки команд, що пересилаються від CI 3102, на відповідність умісту бази даних, і оновлює базу даних, коли команди є допустимими.

Сервер STM також управляє буфером типу FIFO 3122 між сервером STM і MG, а також резервним диском FIFO 3124. Призначенням буферів FIFO є усереднення потоку команд від CI, якщо MG не є в змозі якийсь час відповісти за якоюсь причиною. Можна також гарантувати, що у випадку аварійної відмови сервера STM або MG жодна команда не буде загублена, оскільки сервер STM виконує очищення буферів FIFO (тобто, пересилку в MG) при перезапуску. Буфери FIFO реалізовані у вигляді файлів.

Сервер STM містить у своєму ядрі сервер ав-



томатичного відновлення 3126, що автоматично генерує відновлення, і, при наявності запиту від оператора, безплатні права. У цьому сенсі генерування відновлень можна розглядати як таке, що включає генерування прав для першого разу, хоча буде зрозуміло, що генерування нових прав ініціюється в SMS. Як буде очевидно, обидві ці дії можуть виконуватися з застосуванням приблизно однакових команд і EMM.

Розміщення STM окремо від SMS, і сервера автоматичного відновлення - у SAS, а не в SMS 3004 (як у відомих системах), є особливо важливою відмінністю, оскільки це значно зменшує кількість команд, що необхідно передавати від SMS у SAS (зважаючи на те, що SMS і SAS можуть розташовуватися в різних місцях і ними можуть управляти різні оператори). Фактично дві основні команди, що вимагаються від SMS, - це команди запуску нової передплати і припинення існуючої передплати (наприклад, у випадку несплати). Шляхом мінімізації обміну командами між SMS і SAS зменшується імовірність збою при передаванні команди через канал 3006 між ними; крім цього, проектування SMS, взагалі кажучи, не потребує урахування особливостей системи умовного доступу 3000.

Виконання автоматичного відновлення показано на блок-схемі, приведений на Фіг.7. Для того, щоб зменшити пропускну спроможність, і припускаючи, що в переважній кількості відновлення є стандартними, відновлення відбувається по групах передплатників; у переважних реалізаціях кількість окремих передплатників у групі дорівнює 256. Блок-схема починається з початкового кроку 3130 і переходить до кроку 3132, де відбувається щомісячне активування функції відновлення (хоча, звичайно, буде зрозуміло, що можливі й інші періоди відновлення). З частотою в один місяць кінцевому користувачу даються права на поточний місяць і весь наступний місяць, після чого права вичерпуються, якщо вони не відновлені.

На кроку 3134 відбувається звернення до бази даних передплатників по групах і по окремих передплатниках з цієї групи, щоб визначити, чи мають бути відновлені права для конкретного окремого передплатника.

На кроку 3136 відповідно до вмісту бази даних передплатників формується бітовий масив групи передплатників, як показано на Фіг.8. Цей бітовий масив включає ідентифікатор групи ("G1" для групи 1) 3138 і 256 зон 3140 окремих передплатників. Окремі біти бітового масиву встановлюються рівними 1 або 0, у залежності від того, чи відновлюватимуться права конкретного передплатника. На Фіг.8 наведений типовий набір двійкових даних.

На кроку 3142 у генератор повідомлень 3106 передаються відповідні команди, включаючи бітовий масив групи передплатників. На кроку 3143 генератор повідомлень встановлює дату вичерпання прав, щоб вказати смарт-карті дату, після якої EMM даної передплати стає недійсним; як правило, ця дата відповідає кінцю наступного місяця.

На кроку 3144 генератор повідомлень генерує на основі вказаних команд групі повідомлення EMM і ініціює шифрування цих EMM шифруваль-

ним блоком 3008; згодом зашифровані повідомлення EMM спрямовуються в інжектор EMM 3300, який на кроку 3146 вводить ці повідомлення в потік даних MPEG-2.

Крок 3148 показує, що описана вище процедура повторюється для кожної групи. І, нарешті, обробка завершується на кроку зупинки 3150.

Описана вище блок-схема, представлена на Фіг.7, фактично є такою, що спеціально стосується відновлення передплати. Подібним чином STM управляє безплатними аудиторними правами і новими передплатниками.

Безплатні аудиторні права, що надаються для окремих конкретних телевізійних програм або груп таких програм, надаються за допомогою STM шляхом посилання генератору повідомлень команди генерувати відповідні аудиторні EMM (для всієї аудиторії) із датою вичерпання прав, заданою кількістю днів (або тижнів). MG обчислює точну дату вичерпання прав на основі цієї команди від STM.

У випадку появи нових передплатників, вони обробляються в два етапи. Спочатку, при покупці смарт-карти для приймача-декодера 2020, за бажанням оператора передплатнику даються безплатні права на заданий період часу (звичайно декілька днів). Це досягається шляхом генерування для передплатника бітового масиву, що містить відповідну дату вичерпання прав. Потім передплатник передає повністю оформлені папери оператору, що курує даного передплатника (у SMS). Як тільки папери оброблені, SMS передає в SAS команду запуску для цього конкретного передплатника. Після приймання SAS команди запуску STM посилає в MG команду призначити новому передплатнику унікальну адресу (із конкретним номером групи і позицією в групі) і генерувати спеціальне так зване EMM передплати на комерційну пропозицію (на противагу звичайному груповому EMM, що його використовують для відновлень) для надання прав конкретному передплатнику до кінця наступного місяця. З цього моменту відновлення передплатника може відбуватися автоматично, як описано вище. Використовуючи цей двоетапний процес, можна надавати нові права на передплату, поки SMS не видає команду зупинення.

Слід зазначити, що EMM передплати на комерційну пропозицію використовується для нових передплатників і для повторного активування існуючих передплатників. EMM групової передплати використовується для відновлення і призупинення.

Розглянемо Фіг.9; типове власне EMM передплати (тобто без заголовка і підпису), утворене за допомогою згаданої вище процедури, включає такі основні частини: як правило 256-бітовий масив передплати (або групи передплатників) 3152, 128 бітів шифрувальних ключів управління 3154 для шифрування EMM, 64 біта для кожного шифрувального робочого ключа 3156, щоб дозволити смарт-карті 3020 дешифрувати слово керування для забезпечення доступу до програм, що передаються шляхом мовлення, і 16 бітів дати вичерпання прав 3158 для вказування дати, після закінчення якої смарт-карта буде ігнорувати це EMM. Фактично у варіанті реалізації, якому віддається перевага, надаються три робочих ключа - ключ,

встановлений для поточного місяця, ключ, встановлений для наступного місяця, і ключ для відновлення у випадку відмови системи.

Більш докладно, ЕММ групової передплати повинно містити всі ці компоненти, за винятком шифрувальних ключів управління 3154. ЕММ передплати на комерційну пропозицію (призначене для окремого передплатника) повинно містити замість повного бітового масиву 3152 групи передплатників ідентифікатор групи ID, за яким йдуть позиція відповідного передплатника в групі, шифрувальні ключі управління 3154 і три робочих ключа 3156, за якими йде відповідна дата вичерпання прав 3158.

Генератор повідомлень MG 3106 служить для перетворення команд, що видаються сервером STM 3104, у ЕММ, що спрямовуються у джерело 3302 повідомлень. Звернемось до Фіг.5; спочатку MG генерує власне ЕММ і передає їх у шифрувальний блок CU 3008 для шифрування, що застосовується до ключів управління й робочих ключів. CU додає до ЕММ підпис 3064 (див. Фіг.3) і передає ЕММ назад в MG, де до нього додається заголовок. Повідомлення ЕММ, що передаються в джерело повідомлень, є, таким чином, повними повідомленнями ЕММ. Генератор повідомлень також визначає час початку і час закінчення мовлення і швидкість видавання повідомлень ЕММ і пересилає ці дані як вказівки разом із повідомленнями ЕММ у джерело повідомлень. MG тільки один раз виконує генерування певного ЕММ, і саме ME виконує його циклічне передавання.

Повернемось до Фіг.5; генератор повідомлень включає в себе свою власну базу даних 3160 ЕММ, у якій ЕММ зберігається протягом його життєвого циклу. Як тільки спливає час, протягом якого здійснюється передавання повідомлення, воно видаляється. База даних використовується для того, щоб забезпечити відповідність між MG і ME, так щоб, наприклад, коли певного кінцевого користувача призупинено, ME не продовжував посилати відновлення. У подібній ситуації MG виконує відповідні операції і пересилає їх у ME.

Після генерування ЕММ MG присвоює ЕММ унікальний ідентифікатор ID. Коли MG передає ЕММ у ME, він пересилає також ЕММ ID. Це забезпечує ідентифікацію конкретного ЕММ як у MG, так і в ME.

Щодо області гілки передплати слід також відзначити, що генератор повідомлень має два FIFO 3162 і 3164, по одному для кожного з джерел повідомлень 3302 і 3304 інжектора ЕММ 3300, для збереження шифрованих ЕММ. Оскільки область гілки передплати й інжектор ЕММ можуть бути рознесені на значну відстань, використання FIFO може забезпечити повну безперервність передавання ЕММ навіть у випадку відмови каналів 3166 і 3168 між ними. Два точно таких же FIFO є й в області гілки PPV.

Однією з особливостей генератора повідомлень (зокрема) і системи умовного доступу (загалом) є те, що зменшується розмір власне ЕММ 3062 завдяки об'єднанню параметра розміру й ідентифікатора для економії пам'яті. Це буде описано за допомогою Фіг.10, на якій наведено приклад ЕММ (це PPV-ЕММ, що є найпростішим ЕММ).

Зменшення розміру відбувається в ідентифікаторі Pid (скорочення від "packet identifier" або "parameter identifier") 3170. Він складається з двох частин: самого ідентифікатора (ID) 3172 і параметра розміру пакета 3174 (необхідного для того, щоб можна було виявити початок наступного пакета). Весь Pid уміщується в лише одному байті інформації - 4 розряди виділяються для ID і 4 розряди - для розміру. Оскільки для визначення розміру чотирьох двійкових розрядів явно недостатньо, використовується спеціальна відповідність між зазначеними бітами і фактичним розміром; ця відповідність описується таблицею перетворення, що зберігається в області пам'яті 3178 генератора повідомлень (див. Фіг.5). Типовою буде така відповідність:

```
0000=0
0001=1
0010=2
0011=3
0100=4
0101=5
0110=6
0111=7
1000=8
1001=9
1010=10
1011=11
1100=12
1101=16
1110=24
1111=32
```

Як можна бачити, параметр розміру не є прямо пропорційним фактичному розміру пакета - зв'язок скоріше квадратичний, ніж лінійний. Завдяки цьому уможливується більший діапазон допустимих значень розміру пакета.

Область гілки PPV

Що стосується області гілки PPV 3200, докладно зображеної на Фіг.5, сервер санкціонування AS 3202 має як свого клієнта централізований сервер замовлень OCS 3207, що запитує інформацію про кожного передплатника, що зв'язується із комунікаційними серверами 3022 для придбання PPV-продукту.

Якщо передплатник відомий AS 3202, виконується набір транзакцій. Якщо замовлення передплатника санкціонується, AS генерує рахунок і посилає його в OCS. У протилежному випадку він повідомляє в OCS, що замовлення не санкціоноване.

Тільки по завершенні всього цього набору транзакцій AS оновлює базу даних 3204 кінцевих користувачів за допомогою серверів (DBAS) 3206, якщо принаймні одну транзакцію санкціоновано; у такий спосіб оптимізується кількість звернень до бази даних.

Критерії, відповідно до яких AS санкціонує покупку, зберігаються в базі даних, доступ до якої здійснюється за допомогою DBAS. У однієї з реалізацій база даних є тією самою базою даних, що до неї звертається STM.

У залежності від параметрів користувача у санкціонуванні може бути відмовлено (PPV\_Forbidden, Casino\_Forbidden,...). Такі критерії оновлюються STM 3104 для SMS 3004.

Перевіряються й інші параметри, такі як допустимі межі для покупки (по кредитній карті, або автоматичним платежам, або по дозволений кількості покупок за юнітами на день).

У випадку платежу по кредитній карті перевіряється наявність номера кредитної карти в локальному чорному списку, що зберігається в базі даних 3205 локальних чорних списків.

Якщо всі перевірки успішні, AS:

1. Генерує рахунок і пересилає його в OCS, що завершує обробку цього рахунку і записує його у файл; потім цей файл пересилається в SMS для обробки (фактична виписка рахунку споживачу); і

2. Оновлює базу даних, в основному для встановлення нових меж для покупок.

Цей механізм "перевірити-і-згенерувати-рахунок-якщо-все-у-порядку" застосовується для кожної команди, що передплатник може запитати під час з'єднання (можна замовити, наприклад, 5 фільмів за один сеанс).

Слід зазначити, що AS має обмежену кількість інформації про передплатника, у порівнянні з інформацією, якою володіє SMS. Наприклад, AS не зберігає ім'я і адресу передплатника. З іншого боку, AS має номер смарт-карти передплатника, категорію передплатника за споживанням (так що різним передплатникам можуть бути зроблені різні пропозиції), і різноманітні прапорці, що вказують, наприклад, чи може передплатник робити покупки в кредит, або кредитування призупинено, або його смарт-карту викрадено. Використання скороченого обсягу інформації може допомогти скоротити кількість часу, що затрачається на санкціонування конкретного запиту передплатника.

Основною метою DBAS 3206 є збільшення продуктивності бази даних із погляду AS шляхом розпаралелювання доступу (тому в дійсності не має великого сенсу створювати конфігурацію тільки з однієї DBAS). AS визначає, скільки DBAS варто підключити. Певна конкретна DBAS може бути підключена тільки до одного AS.

OCS 2307 працює в основному з командами PPV. Він працює в декількох режимах.

По-перше, він обробляє команди, що видаються SMS, такі як оновлення продукту (наприклад, якщо рахунок уже записаний за допомогою SMS, OCS рахунок не генерує), оновлення "гаманця" у смарт-карті 3020 і відміна/поновлення сеансу.

Стадіями даної процедури є:

1. Ідентифікація відповідного передплатника (із використанням AS 3202);

2. Якщо він дійсний, формування відповідних команд для генератора повідомлень із метою відсилання відповідного EMM. Команди можуть бути:

Командами продукту,  
Відновлення "гаманця",  
Видалення сеансу.

Слід зазначити, що ці операції не передбачають виписування рахунків, оскільки виписування рахунків уже відоме з SMS. Ці операції подібні покупці "безплатного продукту".

По-друге, OCS обробляє команди, прийняті від передплатників через комунікаційні сервери 3022. Ці команди можуть прийматися або через модем, підключений до приймача-декодера 2020, або ак-

тивуватися голосом через телефон 4001, або активуватися клавішами за допомогою MINITEL, PRESTEL або подібної системи (якщо використовується).

По-третє, OCS має справу з запитом зворотного звертання, що видаються SMS. Ці останні два режими роботи будуть описані докладніше нижче.

У описаному вище режимі другого типу OCS працює з командами, прийнятими безпосередньо від кінцевого користувача (передплатника) через комунікаційні сервери CS 3022. До таких команд відносять замовлення продуктів (наприклад, конкретної PPV-передачі), ініційовані передплатником зміни параметрів передплати і перевизначення батьківського коду (батьківський код - це код, за допомогою якого батьки можуть обмежити дітям право доступу до визначених програм або класів програм).

Процес обробки цих команд буде описаний нижче докладніше з посиланнями на Фіг.11.

Замовлення продукту передплатником включає такі кроки:

1. Ідентифікація за допомогою AS абонента, що здійснює виклик через CS 3022, замовляючи конкретний продукт;

2. Перевірка дійсності запиту абонента, знову-таки з використанням AS (куди запит поміщається із використанням приймача-декодера 2020, що досягається шляхом перевірки даних смарт-карти 3020)

3. З'ясування ціни покупки;

4. Перевірка того, чи не перевищує ціна межі кредиту абонента і т.п.;

5. Приймання часткового рахунку від AS;

6. Заповнення додаткових полів у рахунку для формування повного рахунку;

7. Додавання повного рахунку у файл інформації про рахунки 3212 для наступної обробки; і

8. Відсилання відповідної команди (або команд) у генератор повідомлень PPV 3210 для генерування відповідного EMM (або декількох EMM).

EMM (або декілька EMM) відсилається(ються) або по модемному каналу 4002, якщо споживач розміщував замовлення продукту з використанням приймача-декодера 2020 (більш докладно це буде описано нижче), або, у протилежному випадку, передаються шляхом мовлення. Єдиний виняток має місце тоді, коли в модемному каналі відбувається збій (у випадку, коли споживач розміщає замовлення з використанням приймача-декодера); у цьому випадку EMM передається шляхом мовлення через ефір.

Змінювання параметрів передплати за запитом передплатника включає:

1. Ідентифікацію абонента (із використанням AS);

2. Передавання інформації у CI; CI, у свою чергу, переправляє цю інформацію в SMS; і

3. Через CI OCS приймає потім відповідь від SMS (у вигляді вартості даної зміни, якщо зміна є можливою).

Якщо зміна запитується з використанням приймача-декодера, OCS генерує підтвердження для SMS. У протилежному випадку, наприклад, у випадку звертання по телефону або через Minitel, підтвердження запитується в передплатника, і ця

відповідь відсилається в SMS через OCS і CI.

Перевизначення батьківського коду включає:

1. Ідентифікацію абонента (із використанням AS); і

2. Передавання в MG команди генерування відповідного EMM, що містить відповідний пароль перевизначення.

У випадку перевизначення батьківського коду команда перевизначення коду, з міркувань безпеки, не може надходити від приймача-декодера. Така команда може надходити тільки від SMS, через телефон або Minitel і т.п. Отже, у даному конкретному випадку, повідомлення EMM лише передаються через ефір шляхом мовлення, і ніколи не передаються по телефонній лінії.

З наведених вище прикладів різноманітних режимів роботи OCS зрозуміло, що користувач може мати прямий доступ до SAS, і, зокрема, OCS і AS, і що комунікаційні сервери підключаються безпосередньо до SAS, і, зокрема, до OCS. Ця важлива особливість пов'язана зі зменшенням для користувача часу передавання його команди в SAS.

Ця особливість ілюструється далі за допомогою Фіг.12, із якої можна побачити, як приставка кінцевого користувача, і, зокрема, приймач-декодер 2020, має можливість зв'язуватися безпосередньо із комунікаційними серверами 3022, пов'язаними з SAS 3002. Замість здійснення зв'язку між кінцевим користувачем і комунікаційними серверами 3022 системи SAS 3002 через SMS 3004, зв'язок здійснюється безпосередньо з SAS 3002.

Фактично забезпечуються два прямих канали зв'язку.

Перший прямий зв'язок здійснюється по головному каналу через телефон 4001 і відповідну телефонну лінію (і/або через MINITEL або подібний зв'язок, якщо є), коли кінцеві користувачі усе ще повинні вводити набори голосових команд або кодових номерів, але в порівнянні зі зв'язком через SMS 3004 час зв'язку скорочується.

Другий прямий зв'язок здійснюється від приймача-декодера 2020, і введення даних відбувається автоматично шляхом встановлення кінцевим користувачем його власної дочірньої смарт-карти 3020, у результаті чого кінцевий користувач звільняється від роботи з введення відповідних даних, що, у свою чергу, зменшує витрати часу й імовірність помилок при введенні.

Наступна важлива особливість, що витікає зі сказаного вище, стосується скорочення часу, що витрачається на передачу сформованого EMM кінцевому користувачу для того, щоб ініціювати перегляд кінцевим користувачем вибраного продукту.

Взагалі кажучи, відповідно до Фіг.12, ця особливість досягається, знов таки, за рахунок надання приймачу-декодеру 2020 кінцевого користувача можливості прямого зв'язку із комунікаційними серверами 3022, пов'язаними з SAS 3002.

Як описано вище, суміщений приймач-декодер 2020 безпосередньо підключається до комунікаційних серверів 3022 через модемний зворотний канал 4002, так що команди від декодера 2020 обробляються SAS 3002, генеруються повідомлення (включаючи EMM) і потім відсилаються на-

зад у декодер 2020 по зворотному каналу 4002. Для зв'язку між CS 3022 і приймачем-декодером 2020 використовується протокол (як буде описано нижче), так що CS приймає підтвердження приймання відповідного EMM, у такий спосіб підвищуючи надійність процедури.

Тоді, наприклад, у випадку режиму попереднього замовлення SAS 3002 приймає від кінцевого користувача через смарт-карту і декодер 2020, через модем і через телефонну лінію 4002 повідомлення, що запитують доступ до конкретної передачі/продукту, і повертає відповідне EMM по телефонній лінії 4002 і модему у декодер 2020, причому переважно, щоб модем і декодер були б розміщені разом у приставці (STB — Set-Top-Box). У такий спосіб кінцевому користувачу забезпечується можливість перегляду передачі/продукту без необхідності передавання EMM у потоку даних MPEG-2 2002 через мультіплексор і скремблер 2004, канал "земля-супутник" 2012, супутник 2014 і канал "супутник-земля" 2016. Це істотно зменшує час і потрібну пропускну спроможність. Забезпечується напевно, що як тільки передплатник заплатить за покупку, у приймач-декодер 2020 приходить EMM.

У режимі роботи описаної вище OCS 3207 третього типу, OCS має справу з запитом зворотного звертання, що видаються SAS. Це проілюстровано на Фіг.13. Ціль типових запитів зворотного звертання — забезпечення того, що приймач-декодер 2020 виконує зворотне звертання до SAS через зворотний модемний канал 4002, спрямовуючи інформацію, що потрібна SAS від приймача-декодера.

Відповідно до інструкцій інтерфейсу команд 3102 генератор повідомлень гілки передплати генерує і відсилає в приймач-декодер 2020 EMM зворотного звертання. З міркувань безпеки це EMM зашифровується за допомогою блока шифрування 3008. EMM може містити час/дату, коли приймач-декодер повинний "прокинутися" і виконати зворотне звертання, без прямого запитування; EMM звичайно може також містити номери телефонів, що термінал повинний набрати, кількість наступних спроб після невдалих викликів, і затримку між двома викликами.

Після приймання EMM або досягнення заданих часу/дати приймач-декодер 2020 зв'язується із комунікаційними серверами 3022. OCS 3207 спочатку ідентифікує абонента за допомогою AS 3202 і перевіряє визначені дані, такі як про власника смарт-карти і передплатника. Потім OCS запитує смарт-карту 3020 переслати різноманітну зашифровану інформацію (таку як відповідні номери сеансів, коли сеанс проглядався, скільки разів передплатнику дозволено повторно переглядати сеанс, режим перегляду сеансу, кількість юнітів, що залишилися, кількість попередньо замовлених сеансів і т.д.). Ця інформація розшифровується генератором повідомлень гілки PPV 3210, знов таки з використанням шифрувального блока 3008. OCS додає цю інформацію у файл інформації зворотного звертання 3214 для подальшої обробки і передавання в SMS 3004. З міркувань безпеки ця інформація зашифровується. Вся процедура повторюється доти, доки зі смарт-карти не буде

зчитана вся доступна інформація.

Особливо переважною особливістю засобу зворотного звертання є те, що перед читанням смарт-карти (відразу ж після ідентифікації абонента з використанням AS 3202, як описано вище) за допомогою SAS 3002 виконується перевірка того, що приймач-декодер дійсно є справжнім, а не піратською версією або комп'ютерною імітацією. Ця перевірка відбувається у такий спосіб. SAS генерує випадкове число, що приймається приймачем-декодером, зашифровує і потім повертається в SAS. SAS дешифрує цей число. Якщо дешифрування пройшло успішно і одержано оригінальне випадкове число, робиться висновок, що приймач-декодер є справжнім, і процедура продовжується. У протилежному випадку процедура переривається.

Іншими функціями, що можуть виконуватися при зворотному звертанні, є стирання застарілих сеансів із смарт-карти або наповнення "гаманця" (це буде описано нижче в розділі "Смарт-карта").

Щодо області гілки область гілки PPV 3200, нижче наводиться опис комунікаційних серверів CS 3022. На рівні апаратного забезпечення у переважному варіанті реалізації вони являють собою машину DEC із чотирма процесорами. На рівні архітектури програмного забезпечення, показаної на Фіг.14, у багатьох відношеннях комунікаційні сервери CS є звичайними. Одна важлива відмінність від традиційних конфігурацій випливає з того факту, що сервери повинні обслуговувати як приймач-декодер 2020, так і голосовий зв'язок через звичайні телефони 4001, а також, можливо, MINITEL або аналогічні системи.

Слід між тим відзначити, що на Фіг.14 показані два централізовані сервери замовлень 3207 (OCS1 і OCS2). Звичайно, може використовуватися будь-яка необхідна кількість OCS.

Комунікаційні сервери включають до свого складу два головних сервери ("CS1" і "CS2"), а також деяке число фронтальних серверів ("Frontal 1" і "Frontal 2"); хоча на фігурі показані тільки два фронтальних сервери, звичайно їх 10 або 12 на кожний головний сервер. Дійсно, хоча показані два головних сервери, CS1 і CS2, і два фронтальних сервери, Frontal 1 і Frontal 2, може використовуватися будь-яка їхня кількість. Як правило, бажаною є певна надмірність.

CS1 і CS2 з'єднані з OCS1 і OCS2 через канали TCP/IP 3230 верхнього рівня, тоді як CS1 і CS2 з'єднані з Frontal 1 і Frontal 2 через додаткові канали TCP/IP 3232.

Як показано, CS1 і CS2 містять сервери для "SENDER" (передача), "RECEIVER" (приймання), "VTX" (MINITEL, PRESTEL або їм подібні), "VOX" (голосовий зв'язок) і "TRM" (зв'язок через приймач-декодер). Вони підключені до шини "BUS" для обміну сигналами з фронтальними серверами.

CS1 і CS2 зв'язуються безпосередньо з приймачами-декодерами 2020 через їх модемні зворотні канали 4002, використовуючи відкритий протокол мережі X25. Між комунікаційними серверами 3022 і приймачами-декодерами 2020 використовується протокол відносно низького рівня, в одній переважній реалізації заснований на стандартному міжнародному CCITT протоколі V42, що забезпечує надійність завдяки наявності засобів вияв-

лення помилок і повторного передавання даних, а також використовує підпрограму перевірки контрольних сум для перевірки цілісності повторного передавання. Передбачається також механізм переривання для того, щоб перешкодити передаванню неприпустимих символів.

З іншого боку, голосовий телефонний зв'язок здійснюється через фронтальні комунікаційні сервери, кожний із яких може одночасно обслуговувати до, наприклад, 30 голосових з'єднань від з'єднання 3234 із локальною телефонною мережею через високошвидкісні "T2" (E1) стандартні телефонні ISDN лінії.

Трьома особливими функціями програмної частини комунікаційних серверів (які в альтернативному варіанті, звичайно, можуть бути цілком реалізовані апаратно) є, по-перше, перетворення інформації протоколу відносно низького рівня, прийнятої від приймача-декодера, в інформацію протоколу відносно високого рівня, виведену в OCS; по-друге, розподіл або керування кількістю одночасно здійснюваних з'єднань; і по-третє, забезпечення декількох паралельних каналів без виникнення перешкод. Що стосується останньої функції, комунікаційні сервери грають у певному сенсі роль мультиплексору при взаємодії з конкретним каналом, обумовленим ID (ідентифікатором) сеансу, що фактично використовується у всьому ланцюжку зв'язку.

У завершення того, що стосується області гілки PPV 3200, показаної на Фіг.5, сервер для мовлення програм (SPB) 3208 підключений до одного або декількох мовників PB 3250 (котрі звичайно є віддаленими від SAS) для приймання інформації програми. SPB відфільтровує для подальшого використання інформацію, що відповідає передачам PPV (сеанси).

Особливо важливою особливістю є те, що відфільтрована інформація програми-передачі передається SPB у MG, який, у свою чергу, посиляє директиву (команду керування) у ME для зміни по обставинах частоти циклічної видачі EMM; для виконання цього ME відшукує усі EMM з ідентифікатором відповідного сеансу і змінює циклічну частоту, установлену для таких EMM. Ця особливість може розглядатися як динамічне виділення смуги пропускання для конкретних EMM. Циклічна видача EMM описується більш докладно нижче в наступному розділі, що стосується інжектора EMM.

Нижче будуть описані обставини, при яких відбувається зміна циклічної частоти, із посиланням на Фіг.15, що демонструє, як циклічна частота 3252 підвищується за короткий час (скажемо, 10 хвилин) перед передачею певної PPV-програми і до кінця програми, від низької циклічної частоти, скажемо, один раз кожні 30 хвилин, до високої циклічної частоти, скажемо, один раз кожні 0,5-1 хвилину, для того, щоб задовольнити в цей час очікувані додаткові запити від користувачів на PPV-передачу. Таким способом смуга пропускання може виділятися динамічно, відповідно до прогнозованих запитів користувачів. Це може допомогти пом'якшити вимоги до смуги пропускання.

Циклічна частота інших EMM також може варіюватися. Наприклад, циклічна частота EMM передплати може варіюватися шляхом передавання

мультиплексором і скремблером 2004 відповідних директив про швидкість обміну.

Інжектор EMM

Що стосується інжектора EMM 3300, джерела повідомлень 3302-3308, які є частиною інжектора EMM і функціонують як засоби виведення для генератора повідомлень, докладно описуються за допомогою Фіг.16. Їхня функція - одержувати повідомлення EMM і циклічно їх передавати (по типу каруселі) через відповідні канали 3314 і 3316 у програмні мультиплексори 3310 і 3312 і далі в апаратні мультиплексори і скремблери 2004. У відповідь мультиплексори і скремблери 2004 генерують глобальну директиву швидкості передавання для керування всіма циклічними частотами повідомлень EMM; для цього ME беруть до уваги різноманітні параметри, такі як час циклу, розмір EMM і т.д. На Фіг. EMM\_X і EMM\_Y - це групи EMM для операторів X і Y, у той час як EMM-Z являють собою інші EMM, для оператора X або Y.

Далі розглянемо докладно одне із джерел повідомлень ME; відзначимо, що інші ME функціонують таким самим способом. ME працює під керуванням директив від MG, основні з яких - час початку і закінчення передавання і частоти видачі, а також номера сеансу, якщо EMM являє собою PPV EMM. Що стосується частоти видачі, у переважній реалізації відповідна директива може приймати одне з п'ятьох значень — від Very fast (дуже часто) до Very slow (дуже рідко). У директиві не вказуються чисельні значення, але замість цього ME відображає директиву на фактичне числове значення, що дається відповідною частиною SAS. У варіанті реалізації, якому віддається перевага, є п'ять наступних частот видачі:

- |                           |                  |
|---------------------------|------------------|
| 1. Very fast (дуже часто) | кожні 30 секунд. |
| 2. Fast (часто)           | щохвилини.       |
| 3. Medium (помірно)       | кожні 15 хвилин. |
| 4. Slow (рідко)           | кожні 30 хвилин. |
| 5. Very slow (дуже рідко) | кожні 30 хвилин. |

ME має першу і другу базу даних 3320 і 3322. Перша база даних призначена для тих EMM, дата мовлення котрих ще не наступила; вони зберігаються в базі даних послідовно у файлах, упорядкованих за часом. Друга база даних призначена для EMM, що підлягають негайному мовленню. На випадок аварійної відмови системи ME організовані таким чином, щоб мати можливість повторного читування відповідного записаного файла і виконання правильного мовлення. Всі файли, що зберігаються в базі даних, обновляються за запитом від MG, що забезпечує відповідність між директивами, що надходять, і уже відісланими в ME EMM. EMM, що передаються шляхом мовлення, також зберігаються в оперативній пам'яті 3324.

Використання FIFO 3162 і 3164 у генераторі повідомлень у комбінації з базами даних 3320 і 3322 у джерелі повідомлень забезпечує функціонування їх обох в автономному режимі, якщо канал 3166 між ними виявиться тимчасово ушкоджений; ME усе ще зможе здійснювати мовлення EMM.

Програмні мультиплексори (SMUX) 3310 і 3312 забезпечують інтерфейс між ME і апаратними мультиплексорами 2004. У переважній реалізації усі вони приймають EMM від двох ME, хоча в загаль-

ному випадку обмежень на кількість ME, що можуть бути підключені до одного SMUX, не існує. Мультиплексори SMUX накопичують EMM і потім пересилають їх відповідно до типу EMM у відповідні апаратні мультиплексори. Це необхідно тому, що апаратні мультиплексори приймають повідомлення EMM різних типів і уміщують їх у різні місця потоку MPEG-2. Крім цього, SMUX спрямовують глобальні директиви швидкості передавання від апаратних мультиплексорів у ME.

Дуже важлива особливість ME полягає в тому, що він видає EMM у випадковому порядку. Причина складається ось в чому. Джерело повідомлень не має можливості визначати або контролювати те, що воно передає в мультиплексор. Отже, можливо, що він може передати два EMM, що повинні бути прийняті і декодовані в приймачі-декодері 2020 безпосередньо одне за іншим. При таких обставинах у ситуації, коли EMM недостатньо розділені, можливо, що приймач-декодер і смарт-карта будуть не в змозі належним чином сприйняти і декодувати друге EMM. Циклічна передача EMM у випадковому порядку може розв'язати цю проблему.

Нижче з використанням Фіг.17 буде описаний засіб, за допомогою якого досягається рандомізація; у переважній реалізації необхідна програмна логіка реалізується за допомогою комп'ютерної мови ADA. Особливо важливою частиною рандомізації є правильне збереження EMM у базах даних 3320 і 3322 (які використовуються з метою резервування) і в оперативній пам'яті 3324. Для конкретної циклічної частоти й оператора EMM зберігають у двовірних масивах, по класах 3330 (скажемо, у порядку від A до Z), і по номерах у класах 3332 (від 0 до N). Додається третій вимір, що відповідає циклічній частоті 3334, так що виходить, що число двовірних масивів дорівнює кількості циклічних частот. У переважному варіанті реалізації є 256 класів, і в кожному класі - від 200 до 300 повідомлень EMM; є п'ять циклічних частот. Останній вимір додається до масиву наявності різних операторів; є стільки тривимірних масивів, скільки операторів. Збереження даних у такому вигляді може забезпечити швидкий пошук у випадку, коли MG бажає видалити конкретне EMM.

Збереження повідомлень EMM здійснюється відповідно до алгоритму хешування (відомому ще як "одностороння функція хешування"). Воно виконується на основі функції залишку від ділення, так що спочатку класи заповнюються по черзі, і потім починають використовуватися старші номери класів, при цьому кількість EMM у кожному класі залишається приблизно постійною. У розглянутому тут прикладі 256 класів. Коли MG посилає в ME EMM з ідентифікатором (ID) 1, цьому EMM присвоюється клас "1", і воно займає перший номер 3332 у класі 3330. EMM із ID 2 присвоюється клас "2", і так далі до класу 256. EMM із ID 257 знову присвоюється клас "1" (на основі функції залишку від ділення), і він займає другий номер у першому класі, і т.д.

Пошук конкретного EMM, наприклад, коли MG запитує видалення конкретного EMM, здійснюється за допомогою процедури, зворотної до описаної вище. Алгоритм хешування застосовується до ID

ЕММ для визначення класу, після чого встановлюється номер у класі.

Фактична рандомізація відбувається тоді, коли повідомлення ЕММ циклічно зчитуються з оперативної пам'яті 3324 із використанням засобів рандомізації 3340, реалізованих в апаратному і/або програмному забезпеченні джерела повідомлень. Зчитування здійснюється випадковим чином і, знов таки, засноване на алгоритмі хешування. По-перше, вибирається випадкове число (для приведення вище прикладу - у діапазоні від 1 до 256), щоб визначити необхідний клас. По-друге, вибирається ще одне випадкове число, щоб визначити необхідний номер у класі. Це друге випадкове число вибирається з урахуванням загального числа ЕММ у даному класі. Як тільки дане ЕММ вибране і його мовлення виконане, воно переміщується в другу ідентичну область пам'яті в ПЗП 3324, знов таки з використанням функції хешування. Таким чином, по мірі мовлення повідомлень ЕММ перша область зменшується в розмірі, і, як тільки буде використаний весь клас, він видаляється. Як тільки перша область пам'яті цілком спустошується, перед новим циклом мовлення ЕММ вона заміняється другою областю пам'яті, і навпаки.

Після двох або трьох циклів мовлення ЕММ описаним вище способом шанси того, що будь-які два ЕММ, призначені для одного кінцевого користувача, будуть передані безпосередньо одне за іншим, із погляду статистики, нехтуванно малі.

Через рівні інтервали, поки відбувається зберігання повідомлень ЕММ, комп'ютер 3050 обчислює кількість байтів пам'яті і на основі цього обчислює швидкість передавання для видачі повідомлень з урахуванням глобальної директиви швидкості передавання від мультиплексору і програмного мультиплексору.

Вище були згадані резервні бази даних 3320 і 3322. У переважній реалізації вони являють собою послідовні файли, у яких зберігається резервна версія вмісту оперативної пам'яті 3324. У випадку відмови джерела повідомлень і подальшого перезапуску або, у більш загальному випадку, коли МЕ перезапускається по якійсь причині, між оперативною пам'яттю і базами даних формується канал, по якому записані ЕММ завантажуються в оперативну пам'ять. Таким способом може бути усунутий ризик втрати повідомлень ЕММ у випадку відмови.

Точно так само, як описано вище, відбувається запис РРV ЕММ для ЕММ передплати, причому клас, як правило, відповідає даному оператору, і номер у класі відповідає номеру сеансу.

#### Смарт-карта

Дочірня смарт-карта, або смарт-карта передплатника, схематично зображена на Фіг.18 і містить 8-бітовий мікропроцесор 110, такий як мікропроцесор Motorola 6805, що має шину введення/виведення, підключену до стандартного масиву контактів 120, що при використанні підключаються до відповідного масиву контактів пристрою читання карти приймача-декодера 2020, що має звичайну конфігурацію. Мікропроцесор 110 сполучений за допомогою шини з переважно маскованим ПЗП 130, ОЗУ 140 і програмовним ПЗП 150 з електричним стиранням. Смарт-карта відпо-

відає стандартам ISO 7816-1, ISO 7816-2 і ISO 7816-3, що визначають деякі фізичні параметри смарт-карти, позиції контактів мікросхеми і деякі зв'язки між зовнішньою системою (і, зокрема, приймачем-декодером 2020) і смарт-картою відповідно, і тому далі описуватися не буде. Однією з функцій мікропроцесора 110 є керування пам'яттю смарт-карти, як описано нижче.

Програмовний ПЗП 150 з електричним стиранням містить динамічно утворювані розділи операторів 154, 155, 156 і динамічно утворювані розділи даних, що будуть описані нижче з використанням Фіг.19.

Як показано на Фіг.19, програмовний ПЗП 150 з електричним стиранням містить постійний розділ ID смарт-карти (або виробника) 151 із 8 бітів, що містить постійний ідентифікатор смарт-карти передплатника, встановлений виробником смарт-карти 3020.

При установці параметрів смарт-карти мікропроцесор 110 видає сигнал приймачу-декодеру 2020, цей сигнал містить ідентифікатор системи умовного доступу, використовуваний смарт-картою, і дані, формовані на основі даних, що зберігаються в смарт-карті, включаючи ID смарт-карти. Цей сигнал зберігається приймачем-декодером 2020, який потім використовує записаний сигнал для перевірки сумісності смарт-карти із системою умовного доступу, використовуваною приймачем-декодером 2020.

Програмовний ПЗП 150 з електричним стиранням містить також постійний розділ генератора випадкових чисел 152, що містить програму для генерування псевдовипадкових чисел. Ці випадкові числа використовуються для диверсифікації сигналів вихідних транзакцій, що генеруються смарт-картою 3020 і що пересилаються назад у пристрій мовлення.

Нижче розділу генератора випадкових чисел 152 поданий постійний розділ керування 153 розміром 144 байта. Постійний розділ керування 153 - це спеціальний розділ оператора, використовуваний програмою в ПЗП 130 при динамічному створенні (і видаленні) розділів 154, 155, 156, як буде описано нижче. Постійний розділ керування 153 містить дані, що стосуються прав смарт-карти щодо створення і видалення розділів.

Програма динамічного створення і видалення розділів викликається у відповідь на спеціальні ЕММ створення (або видалення) конкретного розділу, що передаються SAS 3002, приймаються приймачем-декодером 2020 і передаються в смарт-карту передплатника 3020. Для створення таких ЕММ оператору необхідні спеціальні кодифікатори для розділу керування. Це не дозволяє оператору видаляти розділи, що відповідають іншому оператору.

Нижче розділу керування 153 знаходиться послідовність розділів ідентифікаторів (ID) оператора 154, 155, 156 для операторів 1, 2N відповідно. Як правило принаймні один розділ ідентифікатора оператора попередньо завантажуються в програмовний ПЗП з електричним стиранням смарт-карти передплатника 3020, так що кінцевий користувач може дешифрувати програми, що передаються шляхом мовлення цим оператором. Наступ-

ні розділи ідентифікаторів оператора можуть пізніше створюватися динамічно з використанням розділу керування 153 у відповідь на сигнал вихідної транзакції, формований кінцевим користувачем (передплатником) за допомогою його смарт-карти 3020, як буде описано далі.

Кожний розділ ідентифікатора оператора 154, 155, 156 містить ідентифікатор групи, до якої належить смарт-карта 3020, і позицію смарт-карти в групі. Ці дані дозволяють смарт-карті (разом з іншими смарт-картами цієї групи) відповідати на мовлення EMM групової передплати, що має адресу цієї групи (але не позицію смарт-карти в групі), а також на індивідуальні EMM (передплати на комерційні пропозиції), адресовані тільки даній смарт-карті групи. У кожній групі може бути до 256 смарт-карт-членів, і ця особливість значно зменшує потрібну пропускну спроможність, необхідну для мовлення EMM.

Для того, щоб ще більш зменшити потрібну пропускну спроможність, необхідну для мовлення EMM групової передплати, дані групи в кожному розділі ідентифікатора оператора 154, 155, 156 і всіх подібних розділів в програмовному ПЗП з електричним стиранням смарт-карти 3020 і інших дочірніх смарт-карт безупинно обновляються, щоб дозволити конкретній смарт-карті змінити своє положення в кожній групі, заповнюючи в такий спосіб "діри", утворювані, наприклад, у результаті видалення карти-члена групи. Діри заповнюються SAS 3002, оскільки список цих дір знаходиться в сервері STM 3104.

У такий спосіб зменшується фрагментація, і кількість членів у кожній групі підтримується приблизно рівним максимальному числу 256 членів.

Кожний розділ ідентифікатора оператора 154, 155, 156 пов'язаний з одним або декількома "об'єктами даних оператора", що зберігаються в програмовному ПЗП з електричним стиранням 150. Як показано на Фіг.19, послідовність динамічно утворюваних об'єктів даних оператора 157-165 розташовується нижче розділів ідентифікаторів оператора. Кожний із цих об'єктів позначається за допомогою:

а) ідентифікатора 1, 2, 3N, відповідного зв'язаного з ним оператора 1, 2, 3N, як показано в лівій частині Фіг.19;

б) ID, що вказує тип об'єкта; і

с) розділу даних, зарезервованого для даних, як показано в правій частині кожного відповідного об'єкта даних оператора на Фіг.19. Слід відзначити, що кожному оператору відповідає набір об'єктів даних, подібний наборам об'єктів даних інших операторів, так що опис типів даних в об'єкті даних оператора 1 може бути застосований також для об'єктів даних всіх інших операторів. Крім цього, слід зазначити, що об'єкти даних розташовуються у фізично суміжних областях програмованого ПЗП з електричним стиранням, і що порядок їхнього розташування несуттєвий.

Видалення об'єкта даних створює "діру" 166 у смарт-карті, тобто, кількість байтів, що раніше займав віддалений об'єкт, не займаються негайно. Кількість байтів, що таким чином "вивільнилася", або "діра", позначаються:

а) ідентифікатором 0; і

б) ID, що вказує, що байти вільні для приймання об'єкта.

Наступний утворюваний об'єкт даних заповнює діру, що ідентифікується ідентифікатором 0. У такий спосіб забезпечується ефективне використання обмеженого обсягу пам'яті (4 кілобайта) програмованого ПЗП 150 з електричним стиранням.

Звертаючись до набору об'єктів даних, відповідних кожному оператору, нижче будуть описані приклади таких об'єктів даних.

Об'єкт даних 157 містить ключ EMM, що використовується для дешифрування зашифрованих повідомлень EMM, що їх приймає приймач-декодер 2020. Цей ключ EMM постійно зберігається в об'єкті даних 157. Цей об'єкт даних 157 може бути створений заздалегідь, до продажу смарт-карти 3020, і/або може бути створений динамічно при створенні нового розділу ідентифікатора оператора (як описано вище).

Об'єкт даних 159 містить ключ ECM, що пересилається відповідним оператором (у даному випадку, оператором 1), щоб дозволити кінцевому користувачу дешифрувати конкретний "букет" програм, які він передплатив. Звичайно нові ключі ECM розсилаються кожний місяць разом із EMM групової передплати (відновлення), що відновлює усі права кінцевого користувача на перегляд мовлення від оператора (у даному випадку - оператора 1). Використання окремих ключів EMM і ECM дозволяє продавати права на перегляд різними способами (у даній реалізації - за передплатою й індивідуально PPV) і також покращує захист. Режим PPV буде описаний нижче.

Оскільки періодично передаються нові ключі ECM, важливо не допустити використання користувачем старих ключів ECM, наприклад, шляхом вимикання приймача-декодера або переустановки годинника, із метою попередити закінчення терміну дійсності старого ключа ECM, перекриваючи таймер приймача-декодера 2020. Відповідно до цього розділ ідентифікатора оператора 154 містить область (що має звичайно розмір 2 байта), що містить дату закінчення терміну дійсності ключів ECM. Смарт-карта 3020 має можливість порівняти цю дату з поточною датою, що утримується в прийнятих ECM, і перешкодити дешифруванню, якщо поточна дата перевищує дату закінчення терміну дійсності ключів ECM. Дата закінчення терміну дійсності передається за допомогою повідомлень EMM, як описано вище.

Об'єкт даних 161 містить 64-бітовий масив передплати, що є точним відображенням програм оператора мовлення, які передплатив передплатник. Кожний біт відповідає одній програмі і встановлюється в "1", якщо передплата на програму оформлена, і в "0", якщо ні.

Об'єкт даних 163 містить деяку кількість юнітів, що можуть бути використані клієнтом у режимі PPV для придбання прав перегляду передачі, що наближається, наприклад, у відповідь на безкоштовний анонс або якесь інше оголошення. Об'єкт даних 163 містить також граничне значення, що може бути задано, наприклад, від'ємним, що уможливорює кредитування клієнта. Юніти можуть бути придбані, наприклад, у кредит за допомогою зворотного модемного каналу 4002, або, напри-



клад, із використанням голосового сервера в сполученні з кредитною картою. За кожну передачу може стягатися плата як в один юніт, так і в декілька.

Об'єкт даних 165 містить опис PPV-передачі, як показано у таблиці 167 на Фіг.20.

Структура 167, яка описує PPV-передачу, містить поля "ідентифікатор (ID) сеансу" 168, що ідентифікує сеанс перегляду (відповідний програмі, а також часу і даті мовлення), "режим сеансу" 169, що вказує, як придбане право перегляду (наприклад, у режимі попереднього замовлення), "індекс сеансу" 170 і "перегляд сеансу" 171.

При прийомі програми в режимі PPV приймач-декодер 2020 визначає, чи є програма такою, що продається в режимі PPV. Якщо це так, декодер 2020 перевіряє, із використанням даних, що зберігаються в структурі 167, що описує PPV-передачу, чи збережено у неї поле "ID сеансу" даної програми. Якщо поле "ID сеансу" там збережено, то слово керування добувається з ECM.

Якщо поле "ID сеансу" там не збережено, то за допомогою спеціальної прикладної програми приймач-декодер 2020 видає кінцевому користувачу повідомлення, що вказує, що він має право перегляду даного сеансу по ціні, скажемо, 25 юнітів, як зчитано з ECM, або повинний зв'язатися із сервером зв'язку 3022, щоб купити програму. При використанні юнітів, якщо кінцевий користувач відповідає "так" (за допомогою пульта дистанційного керування 2026 (див. Фіг.2)), декодер 2020 посилає ECM у смарт-карту, смарт-карта зменшує гаманець смарт-карти 3020 на 25 юнітів, записує ID сеансу 168, режим сеансу 169, індекс сеансу 170 і перегляд сеансу 171 в структуру опису PPV-передачі 167 і добуває з ECM та дешифрує слово керування.

У режимі попереднього замовлення EMM буде передано в смарт-карту 3020, так що смарт-карта збереже поля "ID сеансу" 168, "режим сеансу" 169, "індекс сеансу" 170 і "перегляд сеансу" 171 в структуру 167 опису PPV-передавання із використанням EMM.

Поле "індекс сеансу" 170 передбачено для диференціювання трансляцій одна від одної. Цей засіб дозволяє здійснювати санкціонування для підмножини трансляцій, наприклад, для 3 трансляцій із 5. Як тільки ECM з індексом сеансу, відмінним від поточного значення поля "індексу сеансу" 170, що зберігається у структурі 167 опису PPV-передачі, передається в смарт-карту, значення поля "перегляд сеансу" 171 зменшується на одиницю. Коли значення поля "перегляд сеансу" досягне нуля, смарт-карта відмовиться дешифрувати ECM з індексом сеансу, відмінним від поточного поля "індексу сеансу".

Вихідне значення поля "перегляд сеансу" залежить тільки від способу, котрим оператор мовлення бажає визначити дану передачу; значення поля "перегляд сеансу" для кожної програми може приймати будь-яке значення.

У мікропроцесорі 110 смарт-карти реалізована програма підрахунку і порівняння для виявлення такого моменту, коли вичерпаний ліміт на кількість переглядів певної програми.

Вказані поля "ID сеансу" 168, "режим сеансу"

169, "індекс сеансу" 170 і "перегляд сеансу" 171 структури 167 опису PPV-передачі можуть бути одержані зі смарт-карти за допомогою процедури "зворотного звертання", як було описано вище.

Кожний приймач-декодер 2020 містить ідентифікатор, який може ідентифікувати приймач-декодер унікальним способом, або може класифікувати його тим або іншим способом для того, щоб дозволити йому працювати тільки з конкретною індивідуальною смарт-картою, конкретним класом смарт-карт того самого, або відповідного, виробника, або будь-яким іншим класом смарт-карт, що призначений для використання винятково з цим класом приймачів-декодерів.

Таким чином, приймач-декодер 2020, що був наданий споживачу одним з операторів мовлення, захищається від використання несанкціонованих дочірніх смарт-карт 3020.

Додатково або як альтернатива до цього першого "узгодження" між смарт-картами і приймачем, програмовний ПЗП з електричним стиранням смарт-карти 3020 може містити поле або бітовий масив, що описує категорії приймачів-декодерів 2020, із якими вона може працювати. Вони можуть задаватися або під час виготовлення смарт-карти, або за допомогою спеціального EMM.

Бітовий масив, що зберігається в смарт-карті 3020, звичайно містить список, що включає до 80 приймачів-декодерів, кожний із яких ідентифікується відповідним ID приймача-декодера, із котрим смарт-карта може використовуватися. У відповідність кожному приймачу-декодеру ставиться значення "1" або "0", що вказує, відповідно, може або не може смарт-карта використовуватися з даним приймачем-декодером. Програма в пам'яті 2024 приймача-декодера відшукує ідентифікатор цього приймача-декодера в бітовому масиві, що зберігається в смарт-карті. Якщо ідентифікатор знайдений, і відповідному ідентифікатору значення дорівнює "1", смарт-карта "допускається"; якщо ні, смарт-карта не буде працювати з цим приймачем-декодером.

Додатково, якщо, звичайно внаслідок угоди між операторами, бажано санкціонувати використання в конкретному приймачі-декодері інших смарт-карт, "першим" смарт-картам будуть послані через транспондер 2014 спеціальні EMM із метою зміни їхніх бітових масивів.

Кожний оператор мовлення може диференціювати своїх передплатників відповідно до заздалегідь визначених критеріїв. Наприклад, деяке число передплатників може бути класифіковане як "VIP" (дуже важливі особи). Відповідно, кожний оператор мовлення може розділити своїх передплатників на множини підмножин, кожна підмножина може складатися з будь-якого числа передплатників.

Підмножина, до якої належить конкретний передплатник, встановлюється в SMS 3004. У свою чергу, SAS 3002 передає передплатнику EMM, що записує інформацію (звичайно довжиною 1 байт) про підмножину, до якої передплатник належить, у відповідний розділ даних оператора, скажемо, 154, програмовного ПЗП з електричним стиранням смарт-карти. У свою чергу, у міру того, як оператор мовлення здійснює мовлення програм, разом із

програмою передається ЕСМ, звичайно з 256 бітів, що вказує, яке підмножина передплатників може переглядати програму. Якщо, відповідно до інформації, що зберігається в розділі оператора, передплатник не має права на перегляд передачі, що визначається ЕСМ, перегляд програми забороняється.

Цей засіб може використовуватися, наприклад, для вимикання всіх смарт-карт даного оператора в конкретному географічному регіоні під час передавання конкретної програми, зокрема, програми, пов'язаної зі спортивним заходом, проведеним у даному географічному регіоні. Таким способом футбольні клуби й інші спортивні організації можуть продавати права передавання за межами їхнього локального регіону, одночасно забороняючи локальним болільникам перегляд заходу по телевізору. У такий спосіб болільники локального регіону стимулюються до придбання квитків і відвідування заходу.

Кожна з особливостей, пов'язана з розділами від 151 до 172, розглядається як окремий винахід, незалежно від динамічного створення розділів.

Очевидно, що даний винахід був описаний вище винятково у вигляді прикладу, і можливі різноманітні модифікації в межах даного винаходу.

Кожна особливість, викладена в описі, а також (де це доречно) пункти формули і фігури можуть бути надані незалежно або у відповідному поєднанні.

У вищезгаданих переважних варіантах реалізації деякі засоби запропонованого винаходу реалізовані з використанням програмного забезпечення. Проте фахівцю, звичайно, зрозуміло, що

будь-які з цих засобів можуть бути реалізовані апаратно. Також зрозуміло, що функції, виконувані апаратними засобами, програмне забезпечення комп'ютера тощо виконуються на або з використанням електричних і їм подібних сигналів.

Перехресні посилання виконані на наші заявки з тією же самою датою подання й озаглавлені як "Генерування сигналів і мовлення" (номер діла повіреного PC/ASD/19707), "Смарт-карта для використання в приймачі зашифрованих сигналів мовлення і приймач" (номер діла повіреного PC/ASD/19708), "Система мовлення і приймання і система умовного доступу для неї" (номер діла повіреного PC/ASD/19710), "Завантаження комп'ютерного файлу з передавача через приймач-декодер у комп'ютер" (номер діла повіреного PC/ASD/19711), "Передавання і приймання телевізійних програм і інших даних" (номер діла повіреного PC/ASD/19712), "Завантаження даних" (номер діла повіреного PC/ASD/19713), "Організація пам'яті комп'ютера" (номер діла повіреного PC/ASD/19714), "Розробка системи управління телебаченням і радіо" (номер діла повіреного PC/ASD/19715), "Витяг розділів даних із потоку даних, що транслюються" (номер діла повіреного PC/ASD/19716), "Система управління доступом" (номер діла повіреного PC/ASD/19717), "Система опрацювання даних" (номер діла повіреного PC/ASD/19718), "Система мовлення і приймання, а також приймач-декодер і віддалений контролер для неї" (номер діла повіреного PC/ASD/19720). Вміст цих документів включений сюди шляхом посилання. Перелік заявок включає і запропонований винахід.

Fig.1.

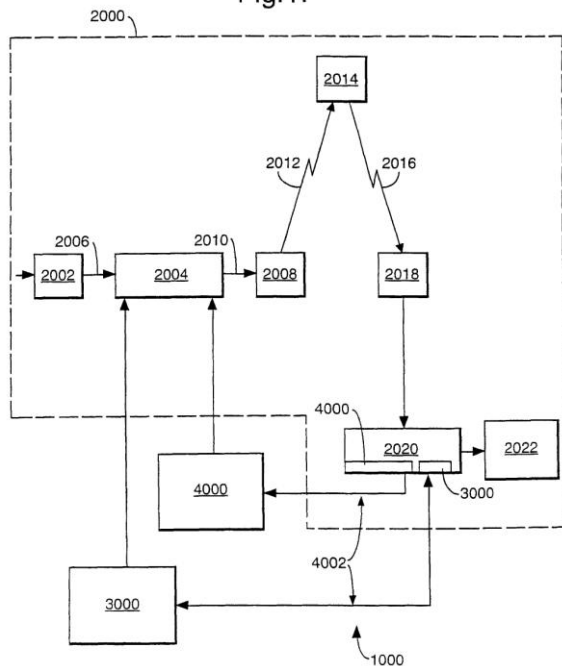
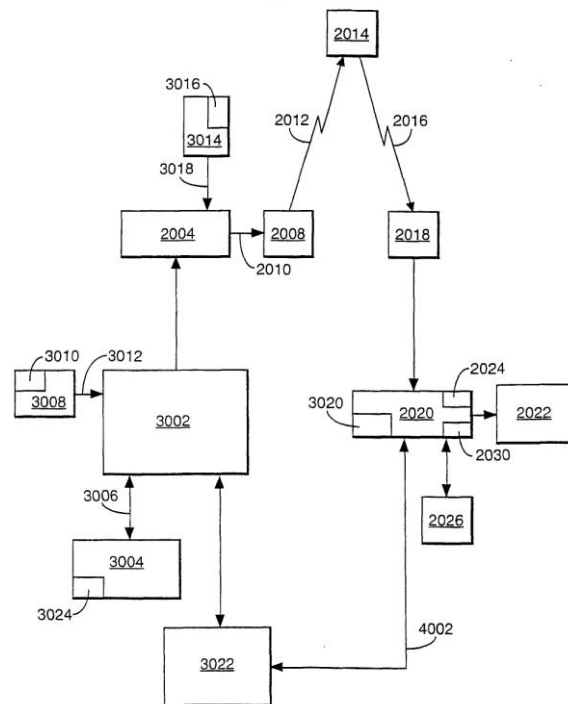


Fig.2.



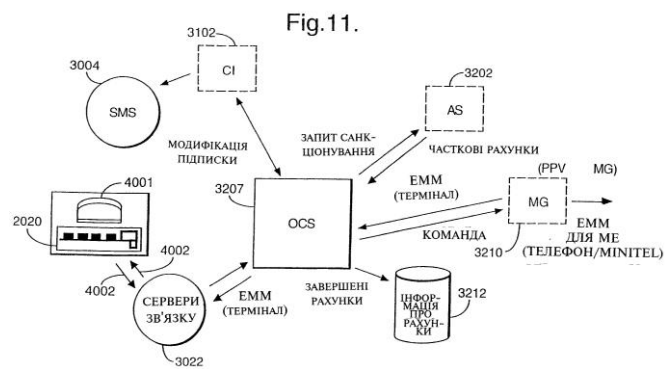
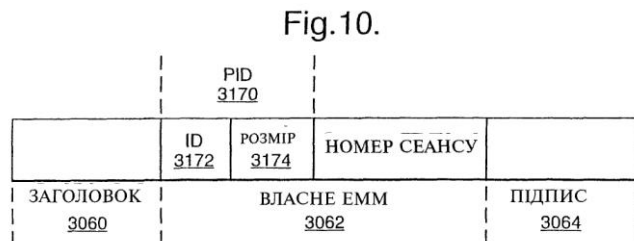
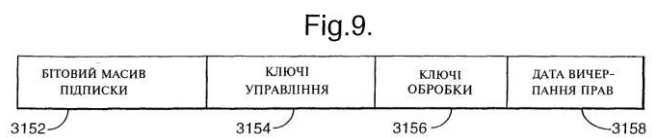
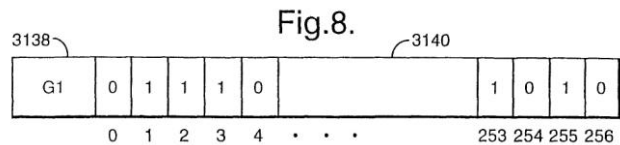
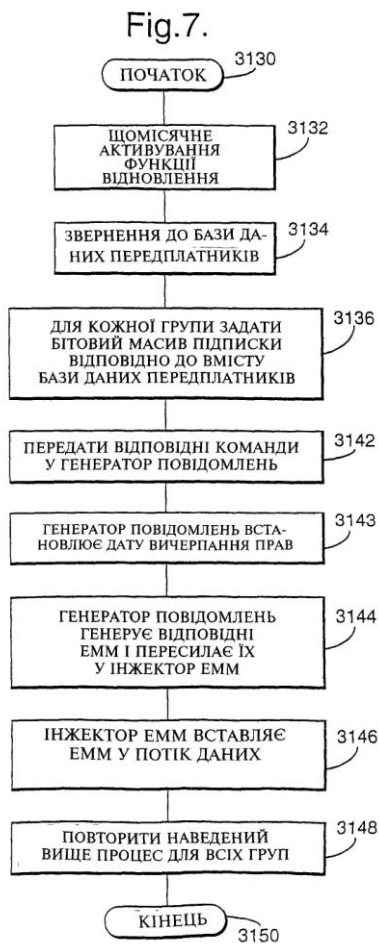
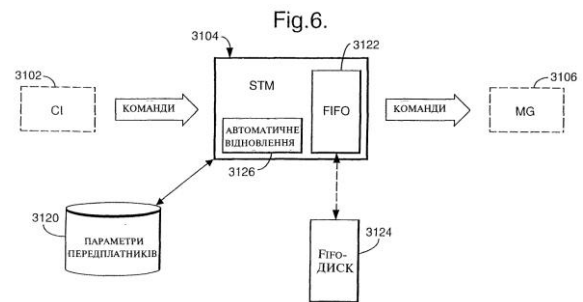
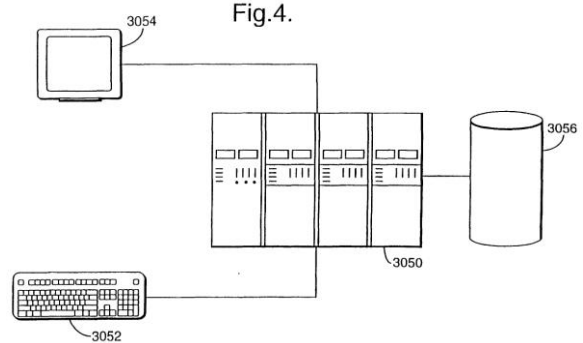
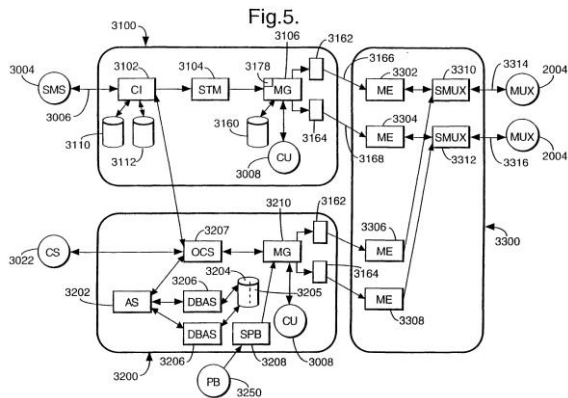


Fig.12.

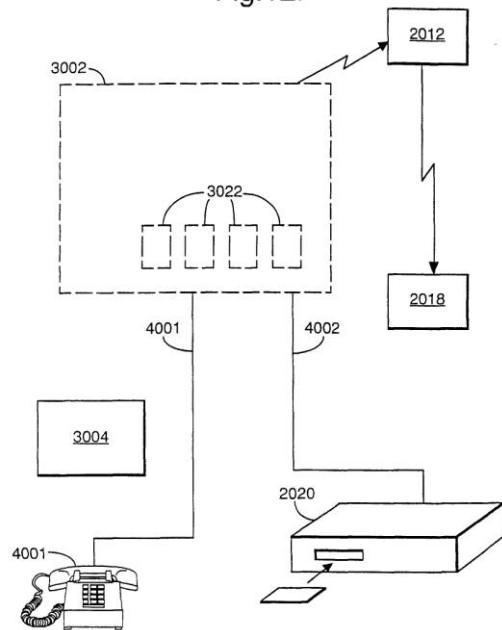


Fig.13.

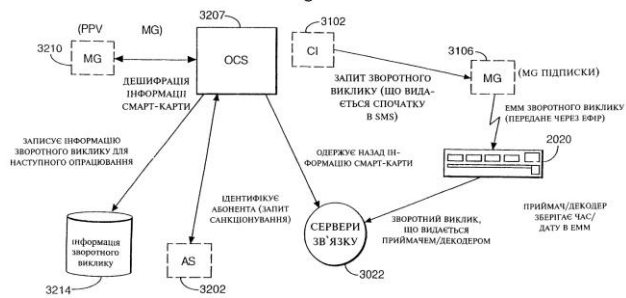


Fig.14.

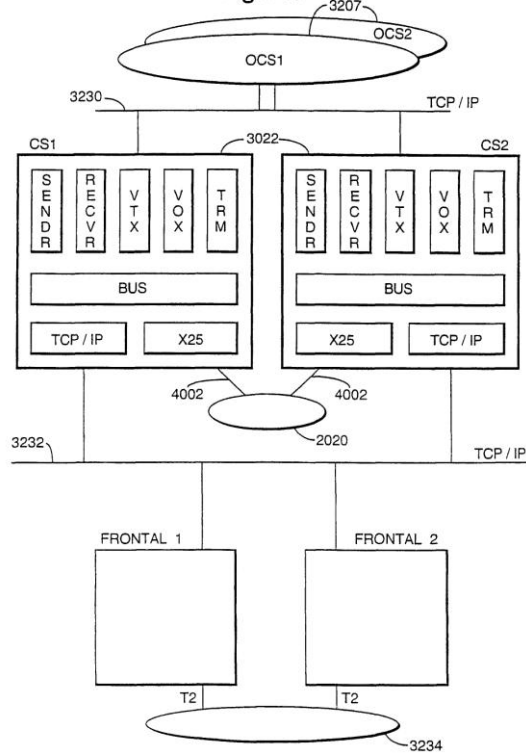


Fig.15.



Fig.16.

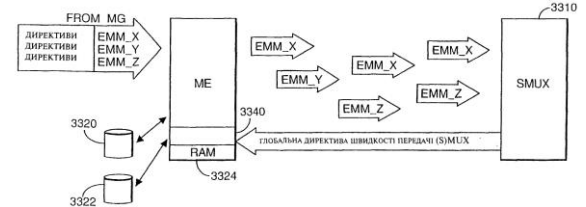


Fig.17.

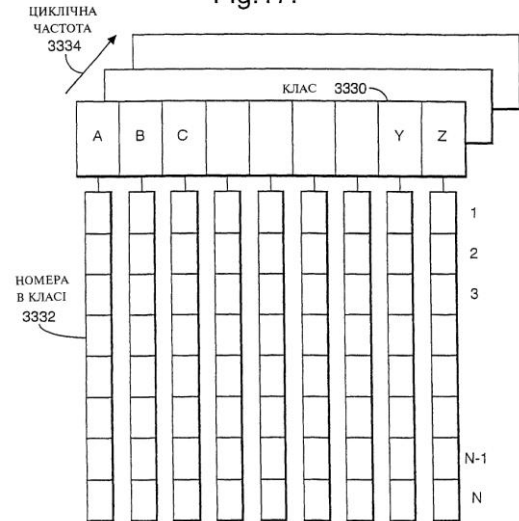


Fig.18.

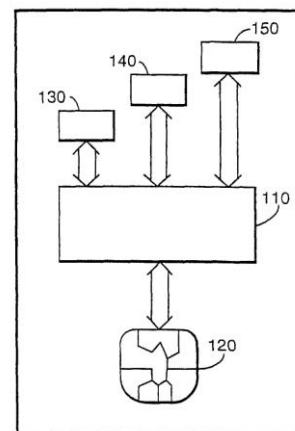


Fig.19.

РОЗДІЛ ID КАРТИ			151
РОЗДІЛ ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ			152
РОЗДІЛ УПРАВЛІННЯ			153
ID ОПЕРАТОРА 1			154
ID ОПЕРАТОРА 2			155
ID ОПЕРАТОРА N			156
1	КЛЮЧ ЕММ	ДАНІ	157
1	КЛЮЧ ЕСМ	ДАНІ	159
2	КЛЮЧ ЕММ	ДАНІ	
1	БІТОВИЙ МАСИВ ПІДПИСКИ	ДАНІ	161
0	БЕЗКОШТОВ- НИЙ ОБ'ЄКТ		166
3	КЛЮЧ ЕСМ	ДАНІ	
1	гаманець жетонів	ДАНІ	163
1	ПЕРЕДАЧА PPV	ДАНІ	165
N	КЛЮЧ ЕСМ	ДАНІ	

Fig.20.

167	ID СЕАНСУ	168
	РЕЖИМ СЕАНСУ	169
	ІНДЕКС СЕАНСУ	170
	ПЕРЕГЛЯД СЕАНСУ	171