



УКРАЇНА

(19) UA

(11) 61990

(13) C2

(51) 7 H04N5/913

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

(54) СПОСІБ І ПРИСТРІЙ ДЛЯ ЗАПИСУ КОДОВАНОЇ ЦИФРОВОЇ ІНФОРМАЦІЇ

1

2

(21) 2000095260

(22) 11 02 1999

(24) 15 12 2003

(86) PCT/IB99/00303, 11 02 1999

(31) 98400344 2

(32) 13 02 1998

(33) EP

(31) 98401513 1

(32) 18 06 1998

(33) EP

(46) 15 12 2003, Бюл. № 12, 2003 р

(72) Майяр Мішель, FR, Бенардо Крістіан, FR

(73) КАНАЛЬ+ СОСЬЕТЕ АНОНІМ, FR

(56) FR 2732537, МПК H04N 7/16, 9/76, 04 10 1996

EP 0714204, МПК H04N 5/913, 29 05 1996

EP 0763936, МПК H04N 5/913, 19 03 1997

(57) 1 Спосіб записування цифрових даних, що передаються, в якому цифрову інформацію, що передається, шифрують з використанням шифрувального ключа запису (E(NE)) і зберігають за допомогою записувального засобу (50) на носії запису, який відрізняється тим, що еквівалент згаданого шифрувального ключа запису (E(NE)) шифрують з використанням транспортного ключа запису (RT(A)) і зберігають на згаданому носії запису разом із зашифрованою інформацією

2 Спосіб за п. 1, який відрізняється тим, що згадана інформація, яку шифрують згаданим шифрувальним ключем запису (E(NE)), включає дані співкерування (CW), які використовують для дескремблювання переданих скрембльованих даних, що їх також записують на згаданий носій запису

3 Спосіб за п. 1 або 2, який відрізняється тим, що згаданий шифрувальний ключ запису (E(NE)) і/або згаданий транспортний ключ запису (RT(A)) зберігають в переносному захисному модулі (52), що використовується із згаданим записувальним засобом (50)

4 Спосіб за будь-яким з попередніх пунктів, який відрізняється тим, що згадану інформацію, що передається, перед передаванням шифрують і перед спрямуванням в згаданий записувальний засіб (50) її приймають декодувальним засобом (12)

5 Спосіб за п. 4, який відрізняється тим, що разом з декодувальним засобом (12) використовують певний переносний захисний модуль (30), який використовують для зберігання керуючих

ключів забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо), що застосовуються для дешифрування згаданої шифрованої інформації, що передається

6 Спосіб за п. 5, який відрізняється тим, що згаданий шифрувальний ключ запису (E(NE)) і/або згаданий транспортний ключ запису (RT(A)) функціонують відповідно до першого алгоритму шифрування (DES), а згадані керуючі ключі забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо) функціонують відповідно до другого алгоритму шифрування (CA)

7 Спосіб за будь-яким з попередніх пунктів, який відрізняється тим, що згаданий транспортний ключ запису (RT(A)) формують в центральному блоці санкціонування запису (21, 24, 25), а копію цього ключа передають в згаданий записувальний пристрій (50)

8 Спосіб за п. 7, який відрізняється тим, що згаданий транспортний ключ запису (RT(A)) у варіанті, якому віддається перевага, шифрують додатковим ключем шифрування (K0(NSIM)) перед його передаванням у згаданий записувальний засіб (50)

9 Спосіб за будь-яким з попередніх пунктів, який відрізняється тим, що центральна система керування доступом (21, 24, 25) передає керуючі ключі забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо) в згаданий записувальний засіб (50)

10 Спосіб за п. 9, який відрізняється тим, що згадані керуючі ключі забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо) передають в переносний захисний модуль (52), що використовується із згаданим записувальним засобом (50)

11 Спосіб за п. 9 або 10, який відрізняється тим, що згаданий записувальний засіб (50) сам дескремблює інформацію, що передається, використовуючи згадані керуючі ключі забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо), перед повторним шифруванням згаданої інформації з використанням шифрувального ключа запису (E(NE)) і її збереженням на згаданому носії запису

12 Спосіб за будь-яким з пп. 9 - 11, який відрізняється тим, що згадана центральна система керування доступом (21, 24, 25) у варіанті, якому віддається перевага, шифрує керуючі ключі

(13) C2

(11) 61990

(19) UA

забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо) з використанням додаткового ключа шифрування (K0(NSIM)) перед їх передаванням в згаданий записувальний засіб (50)

13 Спосіб за будь-яким з пп 9-12, який **відрізняється** тим, що згаданий записувальний засіб (50) передає згаданий центральній системі керування доступом запит, який включає в себе інформацію, що ідентифікує необхідні ключі забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо), причому автентичність цього запиту завіряється згаданим записувальним засобом (50) за допомогою певного ключа (K0(NSIM)), унікального для даного записувального засобу

14 Спосіб за п 1, який **відрізняється** тим, що в ньому використовуються декодувальний засіб (12) і захисний модуль (30), що використовується з цим декодувальним засобом, а також записувальний засіб (50) і захисний модуль (52), що використовується з цим записувальним засобом, і тим, що копію транспортного ключа запису (RT(A)) зберігають в згаданому захисному модулі (30), що використовується з декодувальним засобом (12), і/або в згаданому захисному модулі (52), що використовується із записувальним засобом

15 Спосіб за п 14, який **відрізняється** тим, що згаданий транспортний ключ запису (RT(A)) формується або згаданим захисним модулем (52) записувального засобу, або згаданим захисним модулем (30) декодувального засобу і передається іншому захисному модулю

16 Спосіб за п 15, який **відрізняється** тим, що згаданий транспортний ключ запису (RT(A)) у варіанті, якому віддається перевага, шифрують перед передаванням в згаданий інший захисний модуль і дешифрують за допомогою ключа (K0(NS)), унікального для цього іншого захисного модуля

17 Спосіб за п 16, який **відрізняється** тим, що згадані захисний модуль (30) декодувального засобу і захисний модуль (52) записувального засобу виконують процедуру взаємної перевірки автентичності, і унікальний ключ дешифрування (K0(NS)) передають в згаданий інший захисний модуль від згаданого захисного модуля, в якому здійснюють шифрування, в залежності від результатів цієї перевірки автентичності

18 Спосіб за п 17, який **відрізняється** тим, що згадана процедура взаємної перевірки автентичності виконується з використанням, серед іншого, аудиторного ключа (K1(C)), відомого обою захисним модулям (30, 52)

19 Спосіб за будь-яким з пунктів 14-18, який **відрізняється** тим, що згаданий захисний модуль (30) декодувального засобу має керуючі ключі забезпечення доступу до трансляції (K0(NS), K0'(Op1, NS) тощо), для дешифрування інформації, яка передається в шифрованій формі, і сеан-

совий ключ (K3(NSIM)) для повторного шифрування цієї інформації перед її передаванням в згаданий захисний модуль (52) записувального засобу, причому згаданий захисний модуль (52) записувального засобу має еквівалент цього сеансового ключа (K3(NSIM)) для дешифрування згаданої інформації перед її шифруванням згаданим транспортним ключем запису (RT(A))

20 Спосіб за п 19, який **відрізняється** тим, що згаданий сеансовий ключ (K3(NSIM)) формується згаданим захисним модулем декодувального засобу або згаданим захисним модулем (52) записувального засобу і передається іншому модулю зашифрованим з використанням унікального ключа шифрування (K0(NS)), так що дешифрування можливе тільки в згаданому іншому захисному модулі

21 Записувальний засіб (50), виконаний з можливістю використання в способі за будь-яким з попередніх пунктів, який включає в себе захисний модуль (52) для шифрування цифрової інформації, що передається, з використанням шифрувального ключа запису (E(NE)) для її збереження на носії запису, який **відрізняється** тим, що згаданий захисний модуль (52) також виконаний з можливістю шифрування згаданого шифрувального ключа запису (E(NE)) для його збереження на носії запису з використанням транспортного ключа запису (RT(A))

22 Переносний захисний модуль (52), виконаний з можливістю використання в записувальному засобі за п 21, який **відрізняється** тим, що він має шифрувальний ключ запису (E(NE)) для шифрування цифрової інформації, що передається, для її подальшого записування, і транспортний ключ запису (RT(A)) для шифрування згаданого шифрувального ключа запису для його подальшого записування

23 Декодувальний засіб (12), виконаний з можливістю використання в способі за будь-яким з пунктів 14 - 20, який включає в себе захисний модуль (30), виконаний з можливістю зберігання копії транспортного ключа запису (RT(A))

24 Декодувальний засіб (12) за п 23, який включає в себе захисний модуль (30), виконаний з можливістю дескремблювання інформації, що передається, з використанням одного або декількох ключів забезпечення доступу до трансляції (K0(NS), K0'(Op, NS) тощо) перед її повторним шифруванням з використанням сеансового ключа (K3(NSIM)) для її подальшого передавання в записувальний засіб

25 Переносний захисний модуль (30), виконаний з можливістю використання в декодувальному засобі (12) за п 23 або 24, який має принаймні копію згаданого транспортного ключа запису (RT(A))

Даний винахід відноситься до способу і пристрою для записування скремблзованих цифрових даних, наприклад, трансляційних телепередач

Передача шифрованих даних добре відома в

галузі платних телевізійних систем, в яких скремблзована аудіовізуальна інформація передається, звичайно через супутник, численним абонентам, кожний з яких має в своєму розпорядженні деко-

дер або суміщений приймач/декодер (IRD - Integrated Receiver/Decoder), здатний дескремблювати програму, що передається, для подальшого перегляду

Звичайно скрембльовані цифрові дані передаються разом зі словом управління для дескремблювання цифрових даних, причому саме слово управління зашифроване робочим ключем і передається в шифрованій формі. Скрембльовані цифрові дані і зашифроване слово управління приймаються декодером, який використовує еквівалент робочого ключа для дешифрування зашифрованого слова управління і подальшого дескремблювання даних, які передаються. Абонент, що сплатив передплату, буде періодично отримувати робочий ключ, необхідний для дешифрування шифрованих слів управління, щоб зробити можливим перегляд кожної конкретної програми

З появою цифрових технологій якість даних, що передаються, багаторазово зросла. Основна проблема, пов'язана з даними в цифровій формі, складається в легкості їх копіювання. Якщо дескрембльовану програму пропускають через аналоговий канал зв'язку (наприклад, канал зв'язку "Pentel") для перегляду і записування на стандартному відеоманітофоні, якість виявляється не вищою за ту, що дає стандартний аналоговий запис на касету. Тому ризик, що такий запис може бути використаний як майстер-стрічка для виготовлення піратських копій, не вище, ніж у випадку з придбаною в магазині аналоговою касетою.

Навпаки, будь-які дескрембльовані цифрові дані, передані по прямому цифровому каналу зв'язку на один з цифрових записувальних пристроїв нового покоління (наприклад, відеоманітофон D-VHS), будуть мати ту ж якість, що і вихідна передана програма, і тому можуть бути скопійовані будь-яку кількість разів без найменшого погіршення якості зображення або звуку. Отже, в цьому випадку існує значний ризик того, що дескрембльовані дані будуть використані як майстер-запис для виготовлення піратських копій.

У заявці № 9503859 на видачу патенту Франції описаний можливий спосіб розв'язання цієї проблеми, з використанням системи, в якій ніколи не дозволяється записувати дескрембльовані цифрові дані на носій цифрового запису. Замість цього декодер, описаний в цій заявці, для записування направляє на носій запису дані в скрембльованій формі. Слово управління, необхідне для дескремблювання даних, перешифровується за допомогою іншого ключа і зберігається на носії запису разом з скрембльованими даними. Цей новий ключ

з відомий тільки приймачу/декодеру і замінює собою робочий ключ, необхідний для отримання слова управління, необхідного для перегляду програми.

Перевага такої системи полягає в тому, що дані ніколи не зберігаються у "відкритій" формі і їх не можна переглянути, не маючи нового ключа, що зберігається в декодері. Система має також ту перевагу, що, оскільки робочий ключ міняється щомісячно, застосування ключа, вибраного декодером для повторного шифрування слова управ-

ління, записаного на цифровій стрічці, означає, що декодер як і раніше буде здатний дешифрувати слово управління, записане на стрічці, навіть після закінчення передплатного місяця.

Недолік системи, запропонованої в цій попередній патентній заявці, полягає в тому, що запис можна переглядати тільки у взаємодії з цим конкретним декодером. Якщо цей декодер виходить з ладу або замінюється, запис більше не може бути відтворений. І точно так само неможливо відтворити запис безпосередньо в пристрої відтворення цифрових записів без підключення декодера.

Мета даного винаходу в його різних аспектах - подолати деякі або всі недоліки, властиві цьому відомому рішення.

Згідно з даним винаходом, є запропонованим спосіб записування цифрових даних, що передаються, в якому цифрову інформацію, що передається, шифрують з використанням шифрувального ключа запису і зберігають за допомогою записувального засобу на носії запису, який відрізняється тим, що еквівалент згаданого шифрувального ключа запису шифрують з використанням транспортного ключа запису і зберігають на згаданому носії запису разом із зашифрованою інформацією.

Перевага цього способу полягає в тому, що згаданий спеціальний ключ шифрування, що використовується для шифрування інформації, сам постійно записується разом з відповідною зашифрованою інформацією. Щоб забезпечити подальший доступ до записаної інформації, одна або декілька резервних копій згаданого транспортного ключа запису може зберігатися не в записувальному пристрої, а в іншому місці, як буде описано нижче.

У одному з варіантів здійснення винаходу згадана інформація, зашифрована згаданим шифрувальним ключем запису, являє собою дані слів управління, необхідні для дескремблювання переданих скрембльованих даних, також записаних на згаданому носії запису. Можливі і інші варіанти здійснення, наприклад, такий, в якому згадана зашифрована інформація відповідає просто переданим даним, які зрештою будуть читані або продемонстровані, наприклад, відповідає самій аудіовізуальній інформації, а не слову управління, що використовується для її дескремблювання.

У одному з варіантів здійснення винаходу згаданий шифрувальний ключ запису і/або згаданий транспортний ключ запису зберігають в переносному захисному модулі, що використовується із згаданим записувальним засобом. Цей модуль може являти собою, наприклад, будь-який відповідний пристрій типу карти з мікропроцесором і/або запам'ятовувальним пристроєм, такий як PCMCIA-карта, карта типу PC-card, смарт-карта, SIM-карта тощо. У альтернативних реалізаціях згадані ключі можуть зберігатися в захисному модулі, вбудованому в згаданий записувальний засіб.

Нижче, якщо не буде вказано прямо, що мова йде саме про переносний пристрій або саме вбудований пристрій, потрібно розуміти, що згадка "захисного модуля" має на увазі обидві можливі реалізації.

У одному з варіантів здійснення винаходу зга-

дану інформацію, що передається, перед передачею шифрують і приймають декодувальним засобом перед її направленням в згаданий записувальний засіб. Декодер може бути фізично окремим від записувального засобу або суміщеним з ним. Як буде детально описано нижче, згадана інформація, що передається, може в деяких випадках оброблятися і/або повторно зашифровуватися декодером перед її направленням в згаданий записувальний засіб.

Згаданий декодувальний засіб може бути сам асоційований з деяким переносним захисним модулем, що використовується для зберігання керуючих ключів забезпечення доступу до трансляції, які застосовуються для дешифрування згаданої шифрованої інформації, що передається. У деяких варіантах здійснення винаходу він може відрізнятися від того захисного модуля, який асоційований із згаданим записувальним засобом. Однак у випадку, наприклад, декодера, суміщеного із записувальним засобом, один і той же захисний модуль може бути використаний для зберігання всіх ключів.

У одному з варіантів здійснення винаходу згадані шифрувальний ключ запису і/або транспортний ключ запису функціонують відповідно до першого алгоритму шифрування, а згадані керуючі ключі забезпечення доступу до трансляції функціонують у відповідності з другим алгоритмом шифрування.

Наприклад, згадані шифрувальний ключ запису і транспортний ключ запису можуть використовувати симетричний DES-алгоритм, а згадані ключі забезпечення доступу до трансляції можуть функціонувати у відповідності зі спеціально розробленим алгоритмом, унікальним для даної системи управління доступом до мовлення. Це надає менеджеру системи можливість зберігати контроль над алгоритмом, вибраним для згаданих ключів забезпечення доступу до трансляції і, в той же час, дозволяє використати стандартний алгоритм для ключів, що відносяться до запису.

У одному з варіантів здійснення винаходу згаданий транспортний ключ запису формують в центральному блоці санкціонування записування, а копію цього ключа передають в згаданий записувальний засіб. У разі втрати або пошкодження носія, що містить ключ, асоційованого із згаданим записувальним засобом, резервна копія або щонайменше засіб для формування згаданого транспортного ключа буде завжди доступним в згаданому центральному блоці санкціонування записування.

З міркувань безпеки згаданий транспортний ключ запису переважно шифрують додатковим ключем шифрування перед його передачею в записувальний засіб. Цей додатковий ключ шифрування може бути заснований, наприклад, на деякому ключі шифрування, спільному для всіх захисних модулів записувальних пристроїв, модифікованому серійним номером даного захисного модуля, так що тільки цей захисний модуль може прочитати таке повідомлення.

У тому випадку, коли система містить приймач/декодер, фізично окремий від згаданого записувального засобу, може виявитися бажаним,

щоб згаданий записувальний засіб мав ті ж права доступу, що і згаданий приймач/декодер, наприклад, щоб дозволити приймачу/декодеру просто передавати потік даних "таким, як є" в записувальний засіб для обробки в останньому.

Відповідно, в одному з варіантів здійснення винаходу згадана центральна система керування доступом передає керуючі ключі забезпечення доступу до трансляції в переносний захисний модуль, асоційований із згаданим записувальним засобом. До їх числа можуть входити, наприклад, копії ключів, що звичайно зберігаються в переносному захисному модулі, асоційованому з декодером, що використовується для дескремблювання передач.

У цьому варіанті здійснення винаходу згаданий записувальний засіб саме дескремблює інформацію, що передається, використовуючи ключі забезпечення доступу до трансляції, перед повторним шифруванням згаданої інформації з використанням шифрувального ключа запису і її збереженням на згаданому носії запису.

Аналогічно тому, як це робиться у разі передачі згаданого транспортного ключа, згадана центральна система керування доступом переважно шифрує керуючі ключі забезпечення доступу до трансляції з використанням деякого додаткового ключа шифрування перед їх передачею в згаданий записувальний засіб. Цей додатковий ключ шифрування може являти собою аудиторний ключ, однаковий для всіх захисних модулів, але модифікований серійним номером даного записувального засобу.

Щоб надати центральній системі керування доступом можливість правильно ідентифікувати ті ключі забезпечення доступу до трансляції, які необхідно передати в згаданий записувальний засіб, згаданий записувальний засіб переважно передає згаданий центральній системі керування доступом запит, що включає в себе інформацію, яка ідентифікує згадані необхідні ключі забезпечення доступу до трансляції, причому автентичність цього запиту завіряється згаданим записувальним засобом за допомогою деякого ключа, унікального для даного записувального засобу. Він може відповідати, наприклад, згаданому ключу, який використовується для шифрування даних, що передаються від згаданого центральної системи керування доступом в згаданий записувальний засіб.

Для згаданих вище реалізацій даного винаходу були описані декілька варіантів здійснення, в яких, зокрема, центральний блок санкціонування записування формує транспортні ключі запису і зберігає їхні копії, і в яких центральна система керування доступом передає в записувальний засіб копії ключів для забезпечення доступу до трансляції. Можливі і альтернативні варіанти здійснення винаходу.

Наприклад, в одному з варіантів здійснення, що містить декодувальний засіб і асоційований з ним захисний модуль, а також записувальний засіб і асоційований з ним захисний модуль, копію транспортного ключа запису зберігають або в згаданому захисному модулі, асоційованому із згаданим декодувальним засобом, або в згаданому захисному модулі, асоційованому із згаданим

записувальним засобом, або в обох згаданих модулях. Завдяки цьому резервний ключ, необхідний для дешифрування запису, завжди буде в наявності, навіть у разі втрати або виходу з ладу іншого захисного модуля. Зокрема, що найраціональніше, копія згаданого транспортного ключа запису може бути збережена в захисному модулі декодера.

Згаданий транспортний ключ запису може формуватися, наприклад, згаданим захисним модулем записувального засобу і передаватися згаданому захисному модулю декодувального засобу, або навпаки. З міркувань безпеки згаданий транспортний ключ запису переважно шифрують перед передачею в захисний модуль декодера і дешифрують за допомогою ключа, унікального для того захисного модуля, який приймає згаданий транспортний ключ запису.

Цей унікальний ключ і його еквівалент можуть бути вбудовані у відповідні захисні модулі під час їх створення. Однак в альтернативному варіанті згадані захисний модуль декодера і захисний модуль записувального засобу виконують процедуру взаємного посвідчення автентичності, і унікальний ключ дешифрування передають від шифруючого захисного модуля в інший захисний модуль в залежності від результатів цієї взаємної процедури.

У одному з варіантів здійснення винаходу згадана процедура взаємного посвідчення автентичності виконується з використанням, серед іншого, аудиторного ключа, відомого обою захисним модулям. Це може бути, наприклад, загальний ключ, відомий всім декодерам і записувальним засобам, ідентифікований серійним номером кожного модуля.

У варіанті, що розвиває цей варіант здійснення з двома захисними модулями, згаданий захисний модуль декодувального засобу має керуючі ключі забезпечення доступу до трансляції, для дешифрування інформації, що передається в шифрованій формі, і сеансовим ключем для повторного шифрування цієї інформації перед її передачею в згаданий захисний модуль записувального засобу, причому згаданий захисний модуль записувального засобу має еквівалент цього сеансового ключа для дешифрування згаданої інформації перед її шифруванням з використанням згаданого транспортного ключа запису.

Цей сеансовий ключ може формуватися згаданим захисним модулем декодувального засобу або згаданим захисним модулем записувального засобу і передаватися іншому з модулів зашифрування з використанням унікального ключа шифрування, так що дешифрування можливе тільки в згаданому іншому захисному модулі.

Даний винахід також розповсюджується на записувальний засіб для використання в описаному вище способі, декодувальний засіб і переносний захисний модуль для застосування в кожному з цих засобів.

Терміни "скрембльований" і "шифрований", "слово керування" і "ключ" використовуються в різних частинах цього тексту з міркувань літературності мови. Однак потрібно розуміти, що не існує принципової різниці між поняттями "скрембльовані дані" і "шифровані дані", або між поняттями "слово керування" і "ключ". Також термін "еквівалентний

ключ" відноситься до деякого ключа, призначеного для дешифрування даних, зашифрованих деяким раніше згаданим ключем, або навпаки. Якщо це не представляється обов'язковим в контексті, що викладається, або якщо прямо не обумовлено іншого, не робиться принципової різниці між ключами, асоційованими з симетричними алгоритмами, і ключами, асоційованими з алгоритмами з відкритим/секретним ключами.

Термін "приймач/декодер" або "декодер", що використовується тут, може означати приймач для прийому кодованих або некованих сигналів, наприклад, телевізійних і/або радіосигналів, які можуть передаватися засобами трансляції або іншими засобами. Цей термін може також мати на увазі декодер для декодування сигналів, що приймаються. У число реалізацій таких приймачів/декодерів може входити суміщений з приймачем декодер для декодування сигналів, що приймаються, наприклад, в призначеній для користувача приставці (set-top box), декодер, що функціонує в поєднанні з фізично окремим приймачем, або декодер, який може виконувати додаткові функції, такі, як функції Web-браузера, або суміщений з іншими пристроями, наприклад, з відеомагнітофоном або телевізором.

Термін "цифрова система передачі", як він використовується тут, охоплює будь-яку систему для передачі або трансляції, наприклад, переважно аудіовізуальних або мультимедійних цифрових даних. Хоч даний винахід особливо застосовний для трансляційних систем цифрового телебачення, винахід може бути також застосований в спеціалізованих телекомунікаційних мережах для мультимедійних прикладних програм для Інтернету, в мережах кабельного телебачення тощо.

Термін "система цифрового телебачення", як він використовується тут, охоплює, наприклад, будь-яку супутникову, наземну, кабельну або іншу систему.

Нижче будуть описані, виключно як приклади, декілька варіантів здійснення даного винаходу з посиланнями на нижчеперелічені креслення, на яких

на фіг. 1 представлена загальна архітектура системи цифрового телебачення згідно з даним винаходом,

на фіг. 2 представлена архітектура системи умовного доступу, показаної на фіг. 1,

на фіг. 3 представлені рівні шифрування системи умовного доступу,

на фіг. 4 представлена схема підключення декодера і пристрою для записування цифрової інформації згідно з цим варіантом здійснення даного винаходу,

на фіг. 5 представлена в схематичній формі організація зон в оснащених пам'яттю картах, асоційованих з декодером і записувальним пристроєм, показаними на фіг. 4,

На фіг. 6 і фіг. 7 представлені операції процедури підготовки повідомлень для обміну інформацією між картою декодера і центральним сервером згідно з першим варіантом здійснення даного винаходу,

на фіг. 8 представлена криптологічна архітектура карти декодера при формуванні шифруваль-

ного ключа запису згідно з першим варіантом здійснення даного винаходу,

на фіг 9 і фіг 10 представлена процедура підготовки повідомлень ECM і EMM для їх записування на носій цифрового запису згідно з першим варіантом здійснення даного винаходу,

на фіг 11 представлені операції процедури дешифрування, що виконуються при відтворенні запису, виконаного згідно з першим варіантом здійснення даного винаходу,

на фіг 12 представлена в схематичній формі організація зон в оснащених пам'яттю картах, асоційованих з декодером і записувальним пристроєм, згідно з другим варіантом здійснення винаходу,

на фіг 13 і фіг 14 представлені операції процедури початкового взаємного посвідчення автентичності і передачі даних між оснащеною пам'яттю картою декодера і оснащеною пам'яттю картою записувального пристрою згідно з другим варіантом здійснення винаходу,

на фіг 15 представлені створення і передача сеансового ключа, який буде використаний обома оснащеними пам'яттю картами під час записування програми згідно з другим варіантом здійснення винаходу,

на фіг 16 представлено функціонування карти записувального пристрою при формуванні шифрувального ключа запису згідно з другим варіантом здійснення винаходу,

На фіг 17 представлена обробка ECM, які передаються картою декодера, що виконується при передачі слова керування CW в шифрованій формі в карту записувального пристрою, згідно з другим варіантом здійснення винаходу,

На фіг 18 і фіг 19 представлена підготовка ECM і EMM для записування на цифровий носій запису згідно з другим варіантом здійснення винаходу, і

На фіг 20 представлений обмін даними між картою декодера і картою записувального пристрою

Загальна схема системи 1 передавання і прийому цифрового телебачення приведена на фіг. 1. Даний винахід включає в себе практично звичайну систему цифрового телебачення 2, яка використовує систему ущільнення MPEG-2 для передачі ущільнених цифрових сигналів. Більш детально, пристрій 3 ущільнення MPEG-2 в центрі мовлення приймає потік цифрових сигналів (наприклад, потік аудіо- або відеосигналів). Пристрій 3 ущільнення підключений до мультиплексора і скремблера 4 за допомогою каналу зв'язку 5. Мультиплексор 4 приймає численні додаткові вхідні сигнали, збирає один або декілька транспортних потоків і передає ущільнені цифрові сигнали в передавач 6 центра мовлення через канал зв'язку 7, тип якого, природно, може бути різним, включаючи канали телекомунікацій.

Передавач 6 передає електромагнітні сигнали через канал "Земля-супутник" 8 на супутниковий ретранслятор 9, де виконується їх обробка електронними засобами і трансляція через віртуальний канал "супутник-Земля" 10 на наземний приймач 11, що звичайно має форму тарілки, який належить кінцевому користувачеві або орендований

ним. Сигнали, що приймаються приймачем 11, передаються в суміщений приймач/декодер 12, який належить кінцевому користувачеві або орендований ним, і підключений до телевізора 13 кінцевого користувача. Приймач/декодер 12 декодує ущільнений сигнал MPEG-2 в телевізійний сигнал для телевізора 13.

Система 20 умовного доступу підключена до мультиплексора 4 і приймача/декодера 12 і розташовується частково в центрі мовлення, а частково в декодері. Вона дозволяє кінцевому користувачеві отримувати доступ до цифрових телевізійних передач від одного або декількох операторів мовлення. У приймач/декодер 12 може бути встановлена смарт-карта, здатна дешифрувати повідомлення, які відносяться до комерційних пропозицій (тобто до однієї або декількох телевізійних програм, що продаються оператором мовлення). За допомогою декодера 12 і смарт-карти кінцевий користувач може купувати передачі в режимі передплати або в режимі плати за перегляд.

Може бути передбачена інтерактивна система 17, також підключена до мультиплексора 4 і приймача/декодера 12 і також розташована частково в центрі мовлення, а частково в декодері, яка дозволяє кінцевому користувачеві взаємодіяти з різними прикладними програмами через модемний зворотний канал 16.

Нижче буде описана більш детально система 20 умовного доступу. Як показано в загальному вигляді на фіг. 2, система 20 умовного доступу включає в себе систему санкціонування абонентів (SAS) 21. SAS 21 підключена до однієї або більш систем керування абонентами (SMS) 22, по одній SMS для кожного оператора мовлення, за допомогою відповідного каналу TCP/IP 23 (хоч в альтернативних реалізаціях замість нього можуть використовуватися канали інших типів). У альтернативному варіанті одна SMS може використовуватися спільно двома операторами мовлення, або один оператор може використати дві SMS тощо.

Перші пристрої шифрування у вигляді шифрувальних блоків 24, що використовують "материнські" смарт-карти 25, підключені до SAS через канал зв'язку 26. Другі пристрої шифрування, також у вигляді шифрувальних блоків 27, що використовують материнські смарт-карти 28, підключені до мультиплексора 4 через канал зв'язку 29. Приймач/декодер 12 приймає переносний захисний модуль в формі, наприклад, "дочірньої" смарт-карти 30. Він підключений безпосередньо до SAS 21 за допомогою комунікаційних серверів 31 через модемний зворотний канал 16. SAS, нарівні з іншими даними, за запитом посиляє в дочірню карту права передплати.

Смарт-карти містять "секрети" одного або декількох комерційних операторів. "Материнська" смарт-карта шифрує різні види повідомлень, а "дочірні" смарт-карти дешифрують ці повідомлення, якщо у них є на це права.

Перший і другий шифрувальні блоки 24 і 27 містять шасі, електронну плату VME, програмне забезпечення якого записане в програмовний ПЗП з електричним стиранням (ППЗПЕС), до 20 елект-

ронних плат і одну смарт-карту 25 і 28 відповідно для кожної електронної плати, одну (карта 28) для шифрування повідомлень ECM і одну (карта 25) для шифрування повідомлень EMM

Нижче функціонування системи 20 умовного доступу системи цифрового телебачення буде описане більш детально застосовно до різних компонентів системи 2 телебачення і системи 20 умовного доступу, Мультиплексор і скремблер

Як показано на фіг 1 і фіг 2, в центрі мовлення цифровий аудіо- або відеосигнал спочатку ущільнюють (або зменшують швидкість передачі) з використанням пристрою 3 ущільнення MPEG-2. Цей ущільнений сигнал потім передають в мультиплексор і скремблер 4 через канал зв'язку 5 для того, щоб мультиплексувати його з іншими даними, такими як інші ущільнені дані

Скремблер генерує слово керування, що використовується в процесі скремблювання і включається в потік даних MPEG-2 в мультиплексорі. Слово керування генерується всередині системи і дозволяє суміщеному приймачу/декодеру 12 кінцевого користувача дескремблювати програму

У потік даних MPEG-2 додаються також критерії доступу, що вказують, яким чином програма пропонується на продаж. Програма може пропонуватися на продаж як в одному з багатьох режимів "передплати", так і/або в одному з багатьох режимів "з оплатою за перегляд" (PPV - Pay Per View). У режимі передплати кінцевий користувач передплачує одну або декілька комерційних пропозицій, або "букетів", дістаючи таким чином права на перегляд будь-якого каналу з цих букетів. У варіанті реалізації, якому віддається перевага, з букета каналів можна вибрати до 980 комерційних пропозицій

У режимі сплати "за перегляд" кінцевому користувачеві надається можливість купувати передачі за бажанням. Це може забезпечуватися або шляхом попереднього замовлення передач ("режим попереднього замовлення"), або шляхом придбання програми відразу після початку мовлення ("імпульсний режим"). У реалізації, якій віддається перевага, всі користувачі є абонентами незалежно від режиму перегляду - передплата або PPV, але, звичайно, PPV-глядачі не обов'язково повинні бути абонентами. Повідомлення керування правами (ECM)

Як слово керування, так і критерії доступу використовуються для формування повідомлення керування правами (ECM). ECM - це повідомлення, що підлягає передачі разом з окремою скремблюваною програмою, повідомлення містить слово керування (яке дозволяє дескремблювати програму) і критерії доступу трансляційної програми. Критерії доступу і слово керування передаються на другий шифрувальний блок 27 через канал зв'язку 29. У цьому блоці ECM генерується, зашифровується і передається в мультиплексор і скремблер 4. Під час трансляційної передачі слово керування звичайно змінюється кожні декілька секунд, тому і повідомлення ECM також передаються періодично, щоб дати можливість дескремблювати слово керування, що змінюється. З міркувань резервування кожне повідомлення ECM звичайно включає в себе два слова керування

поточне слово керування і наступне слово керування

Кожна послуга, що транспортується оператором мовлення в потоці даних, містить декілька різних компонент, наприклад, телевізійна програма включає в себе компоненту відеоданих, компоненту аудіоданих, компоненту субтитрів тощо. Кожна з цих компонент послуги для подальшої передачі на ретранслятор 9 скремблюється і зашифровується окремо. Для кожної скремблюваної компоненти послуги потрібне окреме ECM. У альтернативному варіанті реалізації для всіх скремблюваних компонент послуги може потребуватися одне єдине ECM. Декілька ECM генеруються також в тому випадку, коли декілька систем умовного доступу керують доступом до однієї і тієї ж програми, що передається

Повідомлення керування наданням прав (EMM)

EMM - це повідомлення, призначене для індивідуального кінцевого користувача (абонента) або групи кінцевих користувачів. Кожна група може містити задану кількість кінцевих користувачів. Така організація у вигляді групи має на меті оптимізувати використання смуги пропускання, таким чином доступ до однієї групи може дозволити досягнути великої кількості кінцевих користувачів

Можуть бути використані різні спеціальні типи EMM. Індивідуальні EMM призначені для індивідуальних абонентів і звичайно використовуються при наданні послуг з оплатою за перегляд, вони містять ідентифікатор групи і позицію абонента в цій групі

EMM групової передплати призначені для груп із, скажемо, 256 індивідуальних користувачів, і використовуються звичайно для адміністрування деяких послуг по передплаті. Такі EMM містять ідентифікатор групи і бітовий масив абонентів групи

Аудиторні EMM призначені для всієї аудиторії глядачів і можуть, наприклад, використовуватися окремими операторами для надання деяких безкоштовних послуг "Аудиторія глядачів" - це вся сукупність абонентів, що мають смарт-карти з однаковими ідентифікаторами системи умовного доступу (CA ID - Conditional Access System Identifier) і, нарешті, "унікальні" EMM адресовані смарт-картам з унікальним ідентифікатором

EMM можуть генеруватися різними операторами для керування доступом до прав на програми, що передаються цими операторами, як коротко описано вище. EMM можуть також генеруватися менеджером системи умовного доступу для конфігурування системи умовного доступу загалом. Трансляція програми

Мультиплексор 4 приймає електричні сигнали, що містять шифровані повідомлення EMM від SAS 21, шифровані повідомлення ECM від другого шифрувального блоку 27 і ущільнені програми від пристрою ущільнення 3. Мультиплексор 4 скремблює програми і передає скремблювані програми, шифровані EMM і шифровані ECM на передавач 6 центра мовлення через канал зв'язку 7. Передавач 6 передає електромагнітні сигнали на супутниковий ретранслятор 9 через канал "Земля-супутник" 8. Прийом програм

Супутниковий ретранслятор 9 приймає і обробляє електромагнітні сигнали, що передаються передавачем 6, і передає ці сигнали на наземний приймач 11, що звичайно має форму тарілки, який належить кінцевому користувачеві або орендований ним, через канал "супутник-Земля" 10. Сигнали, що приймаються приймачем 11, передаються в суміщений приймач/декодер 12, який належить кінцевому користувачеві або орендований ним і підключений до телевізора кінцевого користувача 13. Приймач/декодер 12 демультимплексує сигнали з метою отримання скрембльованих програм з шифрованими EMM і шифрованими ECM.

Якщо програма не скрембльована, тобто з потоком MPEG-2 не передане повідомлення ECM, приймач/декодер 12 виконує декомпресію даних і перетворює сигнал у відеосигнал для передачі його в телевізор 13.

Якщо програма скрембльована, приймач/декодер 12 витягує з потоку даних MPEG-2 відповідне повідомлення ECM і передає це ECM в "дочірню" смарт-карту 30 кінцевого користувача. П'єзодатчик встановлюють в гніздо приймача/декодера 12. Дочірня смарт-карта 30 перевіряє, чи має цей кінцевий користувач права на дешифрування даного ECM і на доступ до даної програми. Якщо ні, то в приймач/декодер 12 передається негативний результат, що вказує, що програма не може бути дескрембльована. Якщо ж кінцевий користувач має такі права, ECM дешифрується і з нього витягується слово керування. Декодер 12 може потім дескремблювати програму з використанням даного слова керування. Потім виконується декомпресія потоку даних MPEG-2 і його перетворення у відеосигнал для подальшої передачі в телевізор 13. Система керування абонентами (SMS).

Система керування абонентами (SMS) 22 включає в себе базу даних 32, яка керує, крім іншого, всіма файлами кінцевих користувачів, комерційними пропозиціями, передплатою, докладними відомостями про PPV і даними, що стосуються споживання і санкціонування кінцевого користувача. SMS може бути фізично віддалена від SAS.

Кожна SMS 22 передає в SAS 21 через відповідний канал зв'язку 23 повідомлення, які спричиняють перетворення або створення повідомлень керування наданням прав (EMM), що підлягають передачі кінцевим користувачам.

SMS 22 також передає в SAS 21 повідомлення, які не передбачають якого б то не було перетворення або створення повідомлень EMM, але передбачають тільки зміну статусу кінцевого користувача (відносно санкціонування, що надається кінцевому користувачеві при замовленні продукту, або суми, на яку кінцевий користувач буде дебетований).

SAS 21 посилає в SMS 22 повідомлення (що звичайно запитують інформацію, таку як інформація зворотного виклику або інформація про рахунок), так що очевидно, що зв'язок між цими двома системами є двостороннім.

Система санкціонування абонентів (SAS)

Повідомлення, що генеруються SMS 22, передаються через канал зв'язку 23 в систему санкціонування абонентів (SAS) 21, яка, в свою чергу, генерує повідомлення, що підтверджують прийом

повідомлень, що генеруються SMS 22, і передає ці підтвердження в SMS 22.

У загальному вигляді, SAS містить область п'єзоплати для надання прав в режимі передплати і для щомісячного автоматичного відновлення прав, область п'єзоплати за перегляд (PPV) для надання прав на PPV-передачі, і інжектор EMM для передачі повідомлень EMM, що створюються в областях п'єзоплати передплати і PPV, в мультимплексорі і скремблері 4 з подальшою їх подачею в потік даних MPEG. Якщо повинні бути надані інші права, такі як права пофайлової оплати (PPF - Pay Per File) у разі завантаження комп'ютерного програмного забезпечення в персональний комп'ютер користувача, передбачаються також інші подібні області.

Одна з функцій SAS 21 складається в керуванні правами доступу до телепередач, доступних як комерційні пропозиції в режимі передплати, або таких, що продаються як PPV-передачі, відповідно до різних комерційних режимів (режим попереднього замовлення, імпульсний режим). SAS 21, відповідно до цих прав і інформації, що приймаються від SMS 22, генерує повідомлення EMM для абонента.

EMM передаються в шифрувальний блок (CU - Ciphering Unit) 24 для шифрування ключами керування і робочими ключами. Шифрувальний блок (CU) підписує EMM і передає EMM назад в генератор повідомлень (MG - Message Generator) в SAS 21, де додається заголовок EMM передаються в передавач повідомлень (ME - Message Emitter) у вигляді повних EMM. Генератор повідомлень визначає час початку і кінця мовлення і частоту випуску EMM і передає ці відомості як відповідні вказівки разом з EMM в передавач повідомлень. Генератор повідомлень генерує дані EMM тільки один раз, циклічну передачу повідомлень EMM виконує передавач повідомлень.

Після генерування EMM генератор повідомлень (MG) присвоює EMM унікальний ідентифікатор. Коли MG передає це EMM в ME, він пересилає також ідентифікатор EMM. Це забезпечує ідентифікацію конкретного EMM як в MG, так і в ME.

У таких системах, як системи "одночасного" шифрування, які виконані з можливістю роботи з декількома системами умовного доступу, наприклад, асоційованих з декількома операторами, потоки EMM, асоційовані з кожною системою умовного доступу, генеруються окремо, а перед передачею мультимплексуються мультимплексором 4. Рівні шифрування системи.

Нижче з посиланнями на фіг 3 буде даний загальний огляд рівнів шифрування у трансляційній системі. Операції шифрування, що відносяться до трансляційної передачі цифрових даних, показані під позицією 41, канал передачі (наприклад, супутниковий канал, як описано вище) - під позицією 42, і операції дешифрування в приймачі - під позицією 43.

Цифрові дані N скремблюються словом керування CW перед тим, як будуть передані в мультимплексор Mр для подальшої передачі. Як показано в нижній частині фіг 3, ці дані, що передаються, включають в себе ECM, що містить, серед іншого,

слово керування CW, зашифроване блоком шифрування Ch1, керованим першим ключем шифрування Kex. У приймачі/декодері сигнал обробляється в демультимплексорі DMp і дескремблері D, перш ніж він буде направлений в телевізор 2022 для перегляду. Блок дешифрування DCh1, який також має ключ Kex, дешифрує повідомлення ECM з демультимплексованого сигналу, щоб отримати слово керування CW, що використовується згодом для дескремблювання сигналу.

З міркувань безпеки слово керування CW, включене в зашифроване повідомлення ECM, змінюється в середньому кожні 10 секунд, або біля того. Навпаки, перший ключ шифрування Kex, що використовується приймачем для декодування ECM, змінюється раз в місяць або біля того за допомогою повідомлення EMM оператора. Ключ шифрування Kex шифрується другим блоком шифрування ChP за допомогою індивідуалізованого групового ключа K1(GN). Якщо даний абонент входить до числа тих, які вибрані для отримання оновленого ключа Kex, блок дешифрування DChP декодера розшифрує повідомлення, використовуючи свій груповий ключ K1(GN), щоб отримати ключ Kex цього місяця.

Блоки дешифрування DChP і DCh1 і відповідним ним ключів розміщуються на смарт-карті, наданій абоненту і встановленій в пристрій зчитування смарт-карт декодера. Ключі можуть формуватися, наприклад, відповідно до будь-якого відомого алгоритму, що передбачає використання симетричного ключа, або у відповідності зі спеціально розробленим алгоритмом, що передбачає використання симетричного ключа.

Як буде описано нижче, з різними операторами або провайдером мовлення, так само як і з різними постачальниками систем умовного доступу, можуть бути асоційовані різні ключі. У приведеному вище описі груповий ключ K1(GN) зберігається в смарт-карті, асоційований з декодером, і використовується для дешифрування повідомлень EMM. Фактично ж різні оператори будуть мати різні унікальні ключі абонентів K1(Op1, GN), K1(Op2, GN) тощо. Кожний груповий ключ генерується оператором і модифікується деяким значенням, асоційованим з тією групою, до якої належить даний абонент. Різні зони пам'яті в смарт-карті зберігають ключі для різних операторів. Кожний оператор може також мати деякий унікальний ключ, асоційований виключно з даною смарт-картою, і аудиторний ключ для всіх абонентів послуг, що надаються цим оператором (дивись вище).

Крім того, менеджер системи умовного доступу також може мати комплект ключів. Зокрема, деяка конкретна смарт-карта може містити ключ KO(NS), унікальний для даного користувача, і аудиторний ключ K1(C), спільний для всіх смарт-карт. У той час як ключі оператора звичайно використовуються для декодування повідомлень EMM, пов'язаних з правами на трансляційні передачі, ключі менеджера системи умовного доступу можуть бути використані для дешифрування повідомлень EMM, пов'язаних із змінами в системі умовного доступу загалом, як буде описано нижче.

Наведений вище опис системи, проілюстрований фіг 3, відноситься до організації керування

доступом у трансляційній системі, в якій передачі дескремблюються декодером і негайно демонструються. Нижче будуть описані, з посиланнями на фіг 4, елементи системи керування доступом для випадку записування і відтворення скрембльованої передачі.

Як і раніше, декодер 12 приймає скрембльовані трансляційні передачі через приймач 11. Декодер оснащений переносним захисним модулем 30, зручно, щоб він був виконаний в формі смарт-карти, але він може також являти собою будь-який інший відповідний пристрій, оснащений пам'яттю або мікропроцесором. Декодер 12 оснащений модемним каналом 16, наприклад, для зв'язку з серверами, що обробляють інформацію умовного доступу, а також виконаний з можливістю спрямування дескрембльованої аудіовізуальної інформації, що підлягає перегляду, в телевізор 13, наприклад, через канал Pentel 53. Система додатково включає в себе цифровий записувальний пристрій 50, такий як цифровий відеоманітофон системи D-VHS або пристрій записування на DVD, виконаний з можливістю обміну даними з декодером, наприклад, через шину 51 типу IEEE 1394. Записувальний пристрій 50 використовує деякий носій запису (не показаний), на який записується інформація.

Записувальний пристрій 50 виконаний з додатковою можливістю функціонування з переносним захисним модулем 52, який містить, серед іншого, ключі, що використовуються для керування доступом до відтворення запису. Переносний захисний модуль може являти собою будь-який портативний пристрій звичайного відомого типу, оснащений пам'яттю і/або мікропроцесором, такий як смарт-карта, PCMCIA-карта, оснащений мікропроцесором, ключ тощо. У даному випадку переносний захисний модуль 52 позначений як SIM-карта, відома з галузі переносних (мобільних) телефонів.

Пристрій 50 цифрового записування оснащений прямим каналом з дисплеєм 13. У альтернативних реалізаціях цифрова аудіовізуальна інформація може перед демонстрацією передаватися із записувального пристрою 50 в декодер 12. Крім того, хоч декодер 12, записувальний пристрій 50 і дисплей 13 показані як окремі елементи, можливі варіанти, в яких деякі або всі ці елементи можуть бути інтегровані, наприклад, в суміщеному декодері/телевізорі, суміщеному декодері/записувальному пристрою тощо.

Крім того, хоч винахід описується тут застосовно до записування трансляційної аудіовізуальної інформації, його цілком зручно використати, наприклад, застосовно до трансляційної аудіоінформації, що згодом записується за допомогою пристрою записування на цифрові аудіокасети DAT або пристрою читання і записування міні-дисків, або навіть застосовно до трансляційної прикладної програми, що записується на жорсткий диск комп'ютера.

Нижче будуть описані перший і другий варіанти здійснення винаходу з посиланнями на фіг 5-11 і фіг 12-19, відповідно. У першому варіанті здійснення для керування формуванням і резервним збереженням ключів, що дозволяють здійснити доступ до запису, використовується центральний

сервер. Крім того, в цьому варіанті здійснення дешифрування і дескремблювання трансляційної передачі перед записом виконується в реальному масштабі часу SIM-картою записувального пристрою. У другому варіанті здійснення смарт-карта декодера керує резервним збереженням ключів доступу до запису, а також бере участь в дешифруванні і декодуванні трансляційних передач в реальному масштабі часу. Перший варіант здійснення винаходу

На фіг 5 представлена структура зон пам'яті смарт-карти 30 і SIM-карти 52, асоційованих з декодером і записувальним пристроєм, відповідно.

Як видно, смарт-карта 30 декодера зберігає декілька ключів, призначених для функціонування з симетричним алгоритмом шифрування/дешифрування, асоційованим з системою умовного доступу. У представленому прикладі для операцій, пов'язаних з доступом до трансляційних передач, використовується спеціально розроблений алгоритм "CA" іх потрібно відрізнити від операцій, що виконуються SIM-картою 52 з використанням алгоритму DES і звичайно пов'язаних із записом і відтворенням інформації на цифровому носії (дивись нижче).

Перший комплект ключів, асоційований з менеджером системи умовного доступу, показаний в зоні 55, вміщений в смарт-карту в момент індивідуалізації. До числа цих ключів входить ключ K0, модифікований числом NS, унікальним для цієї карти. Зона 55 менеджера системи може містити і інші ключі, такі як аудиторний ключ K1 (не показаний), модифікований константою C і спільний для всіх смарт-карт, що обслуговуються цим менеджером системи умовного доступу.

Друга зона 56 містить ключі, асоційовані з одним або декількома операторами мовлення. Ці ключі можуть бути записані в момент індивідуалізації карти 30 менеджером системи умовного доступу, але можуть, що трапляється більш часто, бути створеними за допомогою спеціально переданого повідомлення EMM при запуску декодера.

Як згадувалося вище, до числа ключів деякого оператора можуть входити ключ K0', модифікований числом NS, унікальним для даної карти, груповий ключ K1', модифікований номером групи GN, і аудиторний ключ K2', модифікований константою Z і спільний для карт всіх абонентів, що обслуговуються цим оператором.

Нарешті, смарт-карта містить значення унікального номера NS цієї карти, записане в момент індивідуалізації і таке, що зберігається в зоні 57 пам'яті смарт-карти.

Як показано далі на фіг 5, SIM-карта 52, асоційована з пристроєм записування цифрової інформації, включає в себе дві секції, 58 і 59, асоційовані з ключами і операціями, що проводяться з використанням алгоритмів CA і DES, відповідно. Секція 59, асоційована з операціями, що використовують алгоритм CA, включає в себе першу зону 60 менеджера системи і зону 61 операторів. Ключі в зоні менеджера системи записані в карту в момент індивідуалізації менеджера системи умовного доступу, до числа цих ключів входить ключ K0, модифікований серійним номером NSIM даної SIM-карти, а також комунікаційний транспортний

ключ T, також модифікований серійним номером NSIM карти. Обидва ці ключі є унікальними для даної карти.

SIM-карта також включає в себе зону 61 операторів, призначену для зберігання ключів, асоційованих з одним або декількома операторами. На фіг 5 SIM-карта представлена такою, якою вона буває в момент її створення і індивідуалізації менеджером системи умовного доступу, до її установки в записувальний пристрій. З цієї причини і зона 61 операторів, і зона 58 DES показані пустими, тобто без яких-небудь збережених ключів.

Нарешті, SIM-карта включає в себе зону 63, призначену для зберігання унікального серійного номера NSIM даної SIM-карти.

Як згадувалося вище, в цьому варіанті здійснення винаходу SIM-карта 52 записувального пристрою виконана з можливістю виконання в реальному масштабі часу дешифрування і дескремблювання трансляційних даних автономно і незалежно від смарт-карти 30, асоційованої з декодером. Для проведення цих операцій необхідно, щоб SIM-карта 52 записувального пристрою мала дублювати ключів, які звичайно зберігаються в зонах менеджера системи і операторів 55 і 56 смарт-карти декодера (дивись фіг 5). Як буде описано нижче, після того як необхідні ключі інсталювані в SIM-карту 52 записувального пристрою, декодер 12 буде направляти потік даних трансляційної передачі без якої-небудь обробки, "як є", в пристрій 50 записування цифрових даних і карту 52.

У цьому варіанті здійснення винаходу формування копій ключів, асоційованих з трансляційною передачею, забезпечує центральна система 21 умовного доступу, при цьому пристрій 50 записування цифрових даних передає запит у відповідний сервер, наприклад, через модемний канал зв'язку, наданий декодером 12. У альтернативному варіанті, можна уявити собі, що сам записувальний пристрій буде оснащений модемом для спрямовування цього запиту. У цьому варіанті здійснення центральна система умовного доступу служить для регулювання у відношенні як керуючих ключів забезпечення доступу до трансляції, так і керуючих ключів забезпечення доступу до запису, як буде описано нижче.

Щоб забезпечити серверу центральної системи умовного доступу можливість формування копій ключів, асоційованих зі смарт-картою декодера, необхідно, щоб повідомлення-запит від SIM-карти записувального пристрою включало в себе ідентифікатор самої смарт-карти декодера (наприклад, серійний номер цієї смарт-карти NS), одночасно з наданням захищеного підтвердження своєї власної автентичності.

Внаслідок цього на першому кроці смарт-карта 30 декодера передає SIM-карті 52 свій серійний номер NS і список операторів Op1, Op2 тощо. З міркувань безпеки сама ця передача може бути зашифрована простим транспортним алгоритмом шифрування, що застосовується до всіх передач між декодером 12 і записувальним пристроєм 50. Щоб уникнути надмірного ускладнення креслень, ключі, пов'язані з цим шифруванням, не показані. Серійний номер NS карти декодера потім зберігає-

ється в зоні менеджера системи SIM-карти

SIM-карта 52 записувального пристрою потім встановлює зв'язок з системою 21 умовного доступу і запитує унікальний номер NMERE системи 21 умовного доступу в сервері умовного доступу (дивись фіг 2) Користуючись отриманою таким чином інформацією, SIM-карта 52 записувального пристрою генерує повідомлення з використанням алгоритму CA, як показано на фіг 6

Згідно з прийнятими тут умовними позначеннями, симетричний алгоритм, який повинен бути використаний на даному криптографічному кроці (CA або DES) показаний овалом Зачорнений вхід в овал означає введення даних, які повинні бути зашифровані, і/або даних, що є модифікатором – дивись шифрування номера смарт-карти і списку операторів під позицією 70 на фіг 6 Кроки дешифрування для різниці позначені негативним показником міри, наприклад, CA⁻¹ або DES⁻¹

На першому кроці, показаному на фіг 6 і позначеному позицією 70, номер NS смарт-карти і список операторів шифруються ключем K0(NSIM), для формування повідомлення 71, що містить серійний номер NSIM SIM-карти і зашифровані дані На другому кроці 72 шифровані дані шифруються повторно ключем T(NSIM, NMERE), який створений шляхом модифікування ключа T(NSIM) унікальним значенням NMERE, відповідним даній системі умовного доступу Кроки 70, 71 можуть виконуватися в зворотному порядку Сформоване таким чином повідомлення 73 і підпис пересилаються потім в сервер умовного доступу 21, шифрувальний блок 24 і материнську карту 25

Система умовного доступу 21 дешифрує згадане повідомлення, як показано на фіг 7 Система має оригінал ключа K0, як показано позицією 76 Внаслідок модифікування ключа K0 значенням NSIM, що міститься в повідомленні, як показано позицією 77, формується ключ K0(NSIM) Цей ключ K0(NSIM) використовується спочатку для підтвердження правильності підпису (поз 78) У тому випадку, якщо підпис недостовірний, обробка повідомлення закінчується, як показано позицією 81

У доповнення до ключа K0 система має також транспортний ключ T або щонайменше ключ T(NMERE), що представляє значення цього ключа T, модифіковане унікальним номером NMERE системи умовного доступу Модифікування ключа T(NMERE) значенням NSIM, що міститься в повідомленні, дозволяє системі сформувати ключ T(NSIM, NMERE) Для спрощення крок підготовки цього ключа на фіг 7 не показаний

Менеджер системи, який має в своєму розпорядженні ключі K0(NSIM) і T(NSIM, NMERE), може тепер дешифрувати повідомлення на кроці 79, щоб отримати серійний номер NS смарт-карти декодера і список операторів, асоційований з даним абонентом Потім менеджер системи додатково перевіряє, чи дійсно список операторів відповідає серійному номеру смарт-карти, і після цього компонує в повідомлення EMM значення копій ключів, які будуть необхідні SIM-карті записувального пристрою для дешифрування передач, включаючи копію ключа K0(NS) смарт-карти, а також різні ключі K0'(Op1, NS), K1'(Op1, GN) тощо опера-

торів

Система керування доступом готує також транспортний ключ запису RT(A), який буде згодом використовуватися SIM-картою для керування доступом під час записування і відтворення цифрових записів, про що буде докладніше розказано нижче Відповідно до вибору алгоритму, якому віддається перевага для роботи із записом, цей ключ буде сформований з ключа RT алгоритму DES, модифікованого випадковим числом A Ключ RT постійно зберігається в материнській карті, а копія значення A зберігається з міркувань резервування в базі даних, асоційованій з оператором системи Завдяки цьому значення ключа RT(A) можна відтворити в будь-який момент

Копії ключів K0(NS), K0'(Op1, NS), Kex тощо смарт-карти, а також транспортного ключа RT(A) запису, компонуються потім в повідомлення EMM, що передається в SIM-карту записувального пристрою З міркувань безпеки це повідомлення шифрується ключем K0(NSIM), щоб гарантувати, що цю інформацію зможе отримати тільки правильна SIM-карта

У разі будь-яких подальших змін або оновлень, наприклад, що відносяться до ключів оператора або інших прав доступу, SIM-карта (як копія смарт-карти) буде отримувати всі повідомлення ECM і EMM, необхідні для дешифрування інформації, що передається

На фіг 8 показаний стан SIM-карти 52 записувального пристрою безпосередньо перед записуванням інформації, що передається Карта 59 пристрою для записування цифрової інформації тепер має записані зони 60 менеджера системи і 61 операторів, а також збережені значення транспортного ключа запису RT(A) алгоритму DES, показаного під позицією 85 Крім того, карта генерує шифрувальний ключ E(NE) запису, показаний позицією 86 і який отримується на кроці 87 модифікуванням показаного позицією 88 ключа E алгоритму DES випадковим числом NE, показаним позицією 89 У цьому випадку ключ E(NE) використовується як сеансовий ключ і може змінюватися від записування до записування Пара ключів E(NE) і RT(A) буде використана надалі у всіх операціях шифрування і дешифрування цифрового запису

Зі посиланнями на фіг 9 нижче будуть описані операції процедури обробки записувальним пристроєм повідомлення ECM, асоційованого з трансляційною передачею Після появи на кроці 90 повідомлення ECM, карта перевіряє на кроці 91, чи має вона права на читання цієї конкретної передачі, наприклад, чи є вона передачею від одного з операторів, який міститься в її списку операторів Якщо так, то на кроці 92 з повідомлення ECM витягується зашифроване слово керування CW У іншому випадку, якщо таких прав немає, обробка припиняється на кроці 93 Використовуючи робочий ключ цього місяця Kex відповідного оператора, показаний позицією 94, карта на кроці 95 декодує зашифроване значення, щоб отримати слово керування CW у відкритій формі, як показано під позицією 96

Далі карта записувального пристрою на кроці 97 знову шифрує слово керування CW, використовуючи ключ E(NE) алгоритму DES, показаний під

позицією 98, і формує ЕСМ, що включає в себе знову зашифроване слово керування, для його введення в потік даних замість первинного ЕСМ. Скрембльована передача разом з послідовністю нових повідомлень ЕСМ записується після цього пристроєм для записування цифрової інформації на носій запису.

Одночасно на кроці 101, показаному на фіг 10, SIM-карта записувального пристрою шифрує значення ключа E(NE), показаного позицією 100, за допомогою транспортного ключа запису RT(A), показаного позицією 102, щоб сформувати повідомлення 103 типу EMM. Це повідомлення EMM потім записується на цифровий носій запису на початку, або в заголовку, запису. Як видно з попереднього опису, якщо не враховувати резервної копії, що зберігається в базі даних системи умовного доступу, ключ RT(A) є унікальним для даної карти записувального пристрою, і це повідомлення EMM не може бути дешифроване ніякою іншою картою, крім карти записувального пристрою, яка згенерувала це повідомлення.

Зі посиланнями на фіг 11 нижче будуть описані операції процедури дешифрування і дескремблювання запису. Передусім, повідомлення EMM 111, записане в заголовку запису, дешифрується на кроці ПО за допомогою транспортного ключа запису 112, який зберігається в SIM-карті. За умови, що це EMM було спочатку створене з використанням цього ж транспортного ключа запису, то внаслідок дешифрування на кроці 110 буде отриманий шифрувальний ключ E(NE) запису, поз. 116.

У процесі відтворення даного запису повідомлення ЕСМ 113 виділяються з потоку даних і дешифруються на кроці 114 за допомогою шифрувального ключа E(NE) запису, щоб на кроці 115 отримати слово керування CW, яке було використане для скремблювання фрагмента потоку даних, відповідного даному ЕСМ. Це слово керування CW далі подається разом з скрембльованими аудіовізуальними даними в дескремблювальний блок, чи то в SIM-карті записувального пристрою, чи то в самому записувальному пристрої, і отримують дескрембльовані вихідні аудіовізуальні дані для подальшого виведення на екран телевизора або інший аналогічний пристрій.

Зрозуміло, що наявність резервного засобу для формування копії транспортного ключа RT(A) на материнській карті 25 центральної системи керування доступом означає, що, у разі втрати або виходу з ладу SIM-карти 52 записувального пристрою, буде можливо відновити її зміст на новій карті записувального пристрою, щоб зробити можливе відтворення раніше зроблених записів.

Вищеописаний варіант здійснення винаходу характеризується тим, що транспортний ключ запису RT(A) генерується і зберігається у вигляді резервної копії в центральному сервері, а також тим, що SIM-карта записувального пристрою містить копії ключів оператора, необхідні для незалежного дешифрування і дескремблювання передачі в реальному масштабі часу. Другий варіант здійснення, описаний нижче з посиланнями на фігури з 12 по 19, не підлягає таким обмеженням, але пропонує реалізацію, в якій більш значну роль відіграє смарт-карта декодера. Другий варіант здійснення

винаходу

На фіг 12 представлена структура зон умовного доступу смарт-карти 30 декодера і зон SIM-карти 52 записувального пристрою в системі такого типу. Як і раніше, обидві карти містять зони, зарезервовані для операцій, що використовують алгоритм CA, і зберігання ключів, зокрема, зони менеджера системи 55, 60 і зони оператора 56, 61.

У цьому варіанті здійснення зона 55 менеджера системи карти декодера 30 містить, в доповнення до ключа KO(NS), аудиторний ключ K1(C), спільний для всіх карт, індивідуалізованих і підтримуваних менеджером системи, і сформований шляхом модифікування ключа алгоритму CA константою C. Цей ключ K1(C) є в наявності також в зоні 60 менеджера системи карти 52 записувального пристрою.

Інша істотна відмінність від структури зон попереднього варіанту здійснення полягає в тому, що смарт-карта 30 додатково оснащена алгоритмом DES і включає в себе зону 120 операцій алгоритму DES.

Щоб забезпечити смарт-карті декодера і SIM-карті записувального пристрою можливість спільного функціонування і, зокрема, забезпечити можливість зрештою формування транспортного ключа запису RT, необхідно, щоб було проведено взаємне підтвердження автентичності обох карт.

Як показано на фіг 13, на першому кроці 121 SIM-карта 52 записувального пристрою запитує випадкове число у смарт-карти 30 декодера, а та передає у відповідь число A1 на кроці 122. Це число потім використовується для того, щоб модифікувати аудиторний ключ K1(C) на кроці 123 і сформувати ключ K1(C, A1), показаний позицією 124. Потім SIM-карта генерує друге випадкове число A2, показане позицією 125, яке, в свою чергу, шифрується ключем K1(C, A1) на кроці 126. Перед передачею в смарт-карту це повідомлення ще раз шифрується і підписується на кроці 128 другим ключем K1(C, NSIM), показаним під позицією 127 і сформованим шляхом модифікування аудиторного ключа K1(C) значенням NSIM. Сформоване таким чином повідомлення 129 передається в смарт-карту 30 декодера як запит серійного номера NS і відповідного йому індивідуального ключа KO(NS).

Як показано на фіг 14, після прийому смарт-картою 30 декодера переданого значення NSIM воно використовується смарт-картою для генерування ключа K1(C, NSIM). Потім значення A2 дешифрується на кроці 130 за допомогою цього ключа і ключа K1(C, A1), отриманого смарт-картою з використанням випадкового числа A1, яке було сформоване нею раніше і було збережено в її пам'яті.

Це значення випадкового числа A2, отримане на кроці 131, використовується потім для того, щоб модифікувати аудиторний ключ K1(C) з отриманням ключа K1(C, A2), показаного під позицією 132. Потім на кроці 133 ключем K1(C, A2) шифрується унікальний серійний номер NS смарт-карти і системний ключ KO(NS), для отримання повідомлення 134.

Як і раніше, потім це повідомлення повторно шифрується на кроці 135 з використанням ключа K1(C, NSIM), показаного позицією 136, і згадане

повідомлення повертається в SIM-карту 52 записувального пристрою, як показано позицією 137

SIM-карта записувального пристрою генерує ключі K1(C, A2) і K1(C, NSIM), показані позицією 138, модифікуючи ключ K1(C) серійним номером NSIM і випадковим числом A2, сформованим і збереженим раніше. Ці ключі використовуються для дешифрування згаданого повідомлення на кроці 139, щоб отримати унікальний серійний номер NS і унікальний ключ KO(NS) смарт-карти, після чого ця інформація записується в пам'ять SIM-карти записувального пристрою на кроці 140.

На відміну від попереднього варіанту здійснення винаходу, в якому для забезпечення незалежної роботи SIM-карти записувального пристрою використовувалися копії всіх ключів менеджера системи і оператора, тут копія ключа KO(NS) і серійний номер NS смарт-карти використовуються для того, щоб встановити сеансовий ключ для записування, а також для того, щоб забезпечити безпечний обмін інформацією між картами під час сеансу записування, особливо - безпечну передачу транспортного ключа запису.

У цьому варіанті здійснення винаходу вихідне дешифрування слова керування CW виконується смарт-картою з використанням ключів оператора і робочих ключів, оновлюваних щомісяця, які вона має. Хоч можливі варіанти, в яких слово керування CW під час створення запису може бути передане безпосередньо в SIM-карту, з міркувань безпеки для цього бажано використати сеансовий ключ.

Фіг 15 показує один з способів формування такого ключа. Як видно, SIM-карта записувального пристрою бере випадковий ключ K3, показаний позицією 141, і на кроці 142 модифікує цей ключ серійним номером SIM-карти NSIM, показаним позицією 143. Ключ K3 може бути будь-яким з безлічі таких ключів, що зберігаються з цією метою в зоні менеджера системи. Створений таким способом на кроці 144 сеансовий ключ K3(NSIM) алгоритму CA шифрується потім на кроці 145 за допомогою раніше отриманого системного ключа KO(NS) смарт-карти, показаного позицією 146. Сформоване таким чином повідомлення 147 потім передається в смарт-карту декодера 55, яка використовує свій ключ KO(NS) для дешифрування повідомлення на кроці 148 і зберігає сеансовий ключ K3(NSIM) в пам'яті карти на кроці 149.

Зі посиланнями на фіг 16 нижче буде описаний стан SIM-карти записувального пристрою перед операцією записування. Зона 60 менеджера системи містить ключ KO(NS) смарт-карти і сеансовий ключ K3(NSIM), так само як і звичайно присутні системні ключі KO(NSIM) тощо (не показані). Додатково карта створює шифрувальний ключ запису алгоритму DES з ключа E алгоритму DES, показаного позицією 150, модифікуючи цей ключ на кроці 151 випадковим числом NE, показаним позицією 152. Як і раніше, отриманий в результаті шифрувальний ключ E(NE) запису буде використаний при повторному шифруванні слів керування, відповідних даній програмі. Схожим способом, транспортний ключ RT(A) запису, показаний позицією 153, формується для застосування при шифруванні шифрувального ключа E(NE) запису, що також записується на цифровий носій запису.

На відміну від попереднього варіанту здійснення винаходу, в якому транспортний ключ запису генерувався в сервері керування доступом, тут ключ RT(A) генерується самою SIM-картою записувального пристрою з використанням ключа алгоритму DES, модифікованого випадковим числом A. Щоб зберегти резервну копію цього ключа, його копія передається в смарт-карту декодера. З очевидних міркувань безпеки, ця копія передається в зашифрованій формі, наприклад, зашифрована ключем KO(NS) смарт-карти, що зберігається до цього часу в пам'яті SIM-карти.

Як показано на фіг 20, при першій установці в записувальний пристрій SIM-карта 52 записувального пристрою спочатку передає запит 190 в смарт-карту, щоб з'ясувати, чи було вже сформоване значення ключа RT(A). Цей запит розглядається смарт-картою декодера на кроці 191.

Якщо результат негативний, SIM-карта 52 записувального пристрою генерує випадковий ключ RT алгоритму DES на кроці 192, значення якого модифікується на кроці 193 випадковим числом A, показаним позицією 194, для формування ключа RT(A), показаного позицією 195. Це значення ключа RT(A) потім шифрується на кроці 196 з використанням спеціалізованого алгоритму і ключа KO(NS), показаного позицією 197, а отримане в результаті повідомлення 198 передається потім в смарт-карту 30 декодера для дешифрування і збереження резервної копії ключа RT(A).

Якщо ж на кроці 191 отримана позитивна відповідь, тоді раніш збережене значення RT(A) на кроці 199 передається в SIM-карту 52 записувального пристрою.

Повернемося до фіг 17, де показані дві смарт-карти 30 декодера під час записування скрембльованої передачі. Як згадувалося вище, в цьому варіанті здійснення винаходу смарт-карта декодера, використовуючи ключі оператора, перш ніж повідомити значення слова керування CW SIM-карті 52 записувального пристрою, виконує початкові кроки шифрування.

Як показано на фіг 17, смарт-карта 30 декодера приймає ECM 160 для його обробки в зоні оператора 56. Спочатку смарт-карта 30 перевіряє, чи має вона права доступу до цієї програми. За умови, що це дійсно так, шифроване слово керування CW витягується з повідомлення ECM на кроці 162 і дешифрується на кроці 163 з використанням відповідного робочого ключа Kex, показаного позицією 164. У іншому випадку процес закінчується, як показано позицією 165.

Як згадано вище, відкрите значення слова керування CW, показане позицією 166, не може бути прямо передане в SIM-карту записувального пристрою. Тому слово керування CW шифрується на кроці 167 з використанням сеансового ключа K3(NSIM), показаного позицією 168, і отримане в результаті значення 169 передається в SIM-карту записувального пристрою для виконання подальших кроків процесу.

Як видно з фіг 18, слово керування, зашифроване сеансовим ключем, приймається SIM-картою 52 записувального пристрою, яка виконує дешифрування на кроці 170, використовуючи еквівалент сеансового ключа K3(NSIM), раніше збережений в

пам'яті і показаний позицією 171 Відкрите значення слова керування CW (поз, 172) передається потім в зону DES цієї карти для шифрування на кроці 173 за допомогою шифрувального ключа E(NE) запису, показаного позицією 174 Отримане в результаті шифроване значення далі включається в повідомлення ECM і вводиться в потік даних для записування з як і раніше скрембльованими даними на носій запису

У той же час і таким же способом, як в першому варіанті здійснення, значення шифрувального ключа запису, показаного позицією 180 на фіг 19, шифрується на кроці 181 транспортним ключем RT(A) запису, показаним позицією 182 Отримане в результаті шифроване значення 183 включається в повідомлення EMM для введення в заголовок цифрового запису

Під час відтворення цього запису, як описано раніше з посиланнями на фіг 11, повідомлення EMM, яке збережене в заголовку запису і яке містить шифрувальний ключ E(NE) запису, дешифрується SIM-картою записувального пристрою за допомогою транспортного ключа RT(A) запису Шифрувальний ключ E(NE) запису використовується потім для дешифрування кожного ECM, щоб отримати слово керування CW, відповідне асоційованому з ним фрагменту скрембльованого запи-

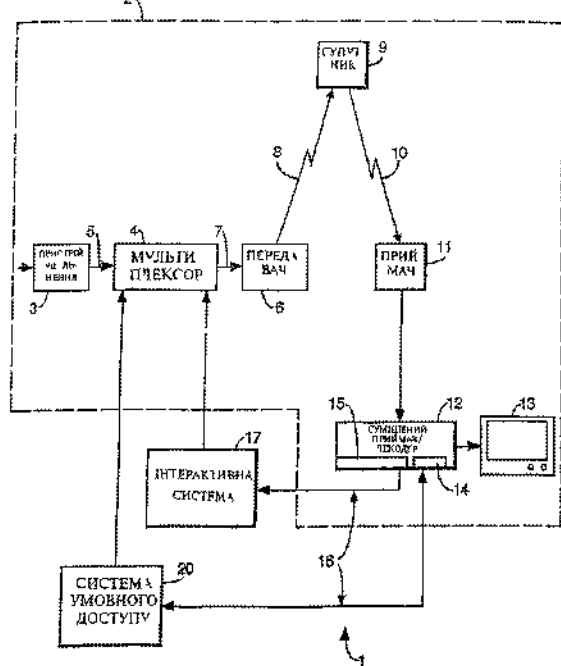
су Потім запис дескремблюється і відтворюється

Зрозуміло, що наявність резервної копії транспортного ключа RT(A), яка зберігається в смарт-карті декодера, означає, що, у разі втрати або виходу з ладу SIM-карти записувального пристрою, буде можливо зробити замість неї іншу карту записувального пристрою Однак, на відміну від попереднього варіанту здійснення винаходу, тут немає необхідності використовувати центральний сервер для зберігання цієї копії-дублікату

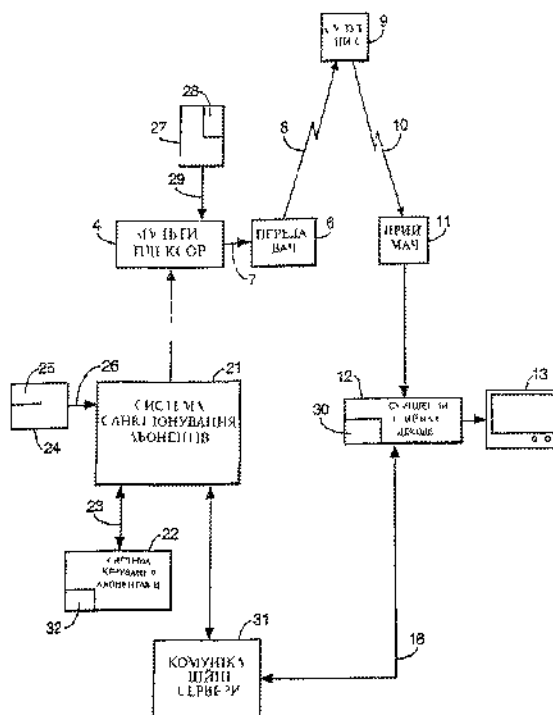
Природно, можливі і альтернативні варіанти здійснення винаходу Наприклад, у вищеписаних варіантах здійснення шифрувальний ключ E(NE) запису генерується за допомогою деякого ключа і випадкового числа Однак в альтернативних варіантах здійснення ключ E(NE) може генеруватися з ключа, модифікованого серійним номером самого записувального пристрою (а не його SIM-карти), щоб зв'язати даний запис і з SIM-картою записувального пристрою, і з самим записувальним пристроєм

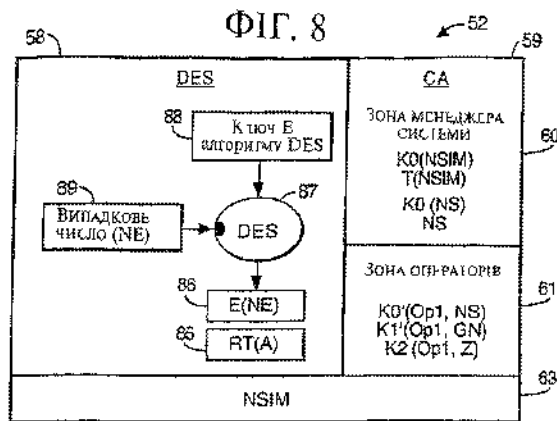
Крім того, певні елементи першого варіанту здійснення, такі як централізоване зберігання транспортного ключа і такий, що автономно працює, записувальний пристрій незалежні один від іншого і можуть бути використані у другому варіанті здійснення, і навпаки

ФІГ. 1

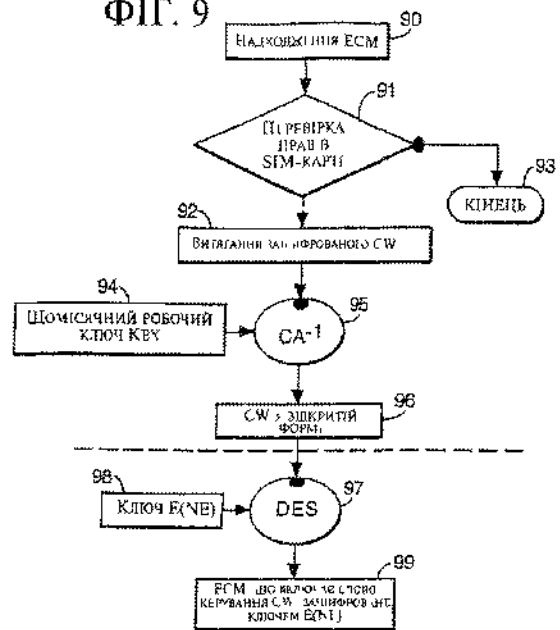


ФІГ. 2

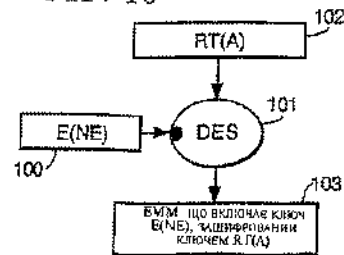




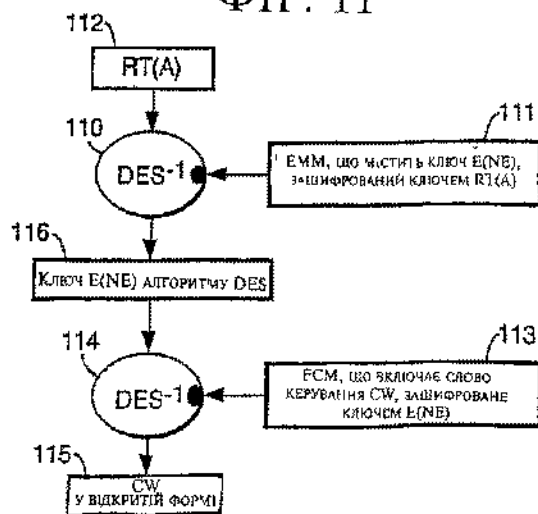
ФІГ. 9



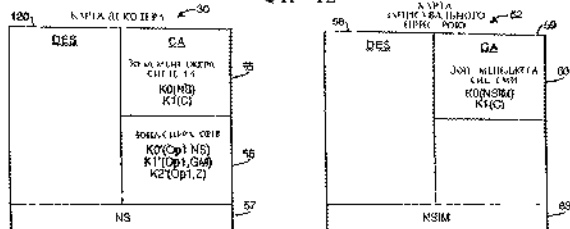
ФІГ. 10



ФІГ. 11



ФІГ. 12



ФІГ. 13

