



УКРАЇНА

(19) UA (11) 93307 (13) C2
(51) МПК
G06F 13/14 (2011.01)
G06F 21/24 (2011.01)
H04L 29/06 (2011.01)

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ ФУНКЦІОНУВАННЯ СИСТЕМИ УМОВНОГО ДОСТУПУ ДЛЯ ВЖИВАННЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ І СИСТЕМА ДЛЯ ЙОГО ЗДІЙСНЕННЯ

1

(21) а200909088
(22) 24.12.2007
(24) 25.01.2011
(86) PCT/RU2007/000723, 24.12.2007
(31) 2007108939
(32) 13.03.2007
(33) RU
(46) 25.01.2011, Бюл.№ 2, 2011 р.
(72) САХАРОВ ОЛЕГ ВЕНІАМІНОВИЧ, RU
(73) САХАРОВ ОЛЕГ ВЕНІАМІНОВИЧ, RU
(56) US 2003/0101253 A1; 29.05.2003
WO 2003107625 A1; 24.12.2003
WO 2002084980 A1; 24.10.2002
RU 2285353 C2; 10.10.2006
(57) 1. Спосіб функціонування системи умовного доступу CAS для вживання в комп'ютерних мережах, який **відрізняється** тим, що використовують не менше одного сервера адаптації потоків САП контенту провайдера, що привласнює потокам контенту унікальні адреси базового Інтернет-протоколу IP для керованої оператором комп'ютерної мережі УКС, доступ до яких можливий через безліч мережевих терміналів СТ, що містять в собі програвач контенту, дескремблер, модуль запиту доступу до контенту, зв'язаний через комп'ютерну мережу з сервером управління доступом передплатника СУД в комп'ютерну мережу і сервером-валідатором, що надає для СТ сесійні ключі SK, що захищають слова, що управляють CW, для даних контенту провайдера, забезпечують виконання наступних дій:
процесу адаптації захищеного скрембльованого потоку контенту провайдера для ретрансляції в УКС, при якій на САП відбувається перекапсуляція потоку біт контенту у формат, придатний для передачі за допомогою IP адресації, при цьому блоки скрембльованих/зашифрованих даних потоків контенту провайдера не видозмінюються, а слова, що управляють CW, необхідні для дескремблювання/розшифровки даних контенту, зашифровуються за допомогою SK, що передаються на САП від сервера-валідатора, і поміщаються в потік повідомлень управління правами ЕСМ, процедури формування доступу до контенту, при якій за допомогою інтерактивної взаємодії з елект-

2

ронним програмним гідом EPG, функціонально пов'язаним з СУД, СТ генерує запит ініціації доступу до вибраного потоку по IP адресі сервера-валідатора, що містить в собі ідентифікатор ID СТ і умовний номер вибраного потоку контенту, у відповідь на який сервер-валідатор для СТ передплатника генерує запит для підтвердження повноважень доступу до контенту, у відповідь СТ посилає повідомлення з персональною ключовою фразою, при успішній авторизації передплатника сервер-валідатор генерує повідомлення для СУД, що містить ID СТ і умовний номер потоку контенту, що вирішує доступ для даного СТ до вибраного контенту передплатника, далі СУД посилає повідомлення для СТ, що містить IP адресу вибраного потоку контенту, одночасно з цим формується захищений канал зв'язку між СТ і сервером-валідатором, по якому сервер-валідатор у відповідь на запити посилає повідомлення з поточними SK,
процедури відтворення потоку контенту СТ, при цьому СТ з прийнятих від САП по IP адресі даних вибраного потоку провайдера демультимплексує ECM, дешифрує CW за допомогою SK, дескремблює за допомогою CW дані контенту і відтворює їх програвачем, при цьому відтворення потоку може бути зупинене як оператором комп'ютерної мережі шляхом відмови доступу для даного терміналу до IP адреси контенту в УКС на абонентському порту, так і за ініціативою сервера-валідатора, при його відмові видати запрошуваний терміналом SK.
2. Спосіб за п. 1, який **відрізняється** тим, що САП видаляє у вихідному потоці контенту ECM і повідомлення управління наданням прав ЕММ провайдера контенту, при цьому допускається призначати новому потоку ECM IP адресу, відмінну від IP адреси решти частки контенту.
3. Спосіб за п. 1, який **відрізняється** тим, що в САП відбувається інкапсуляція потоку контенту провайдера у формат транспортного потоку TS для трансляції в UDP пакетах для multicast або unicast IP адрес.
4. Спосіб за п. 1, який **відрізняється** тим, що в САП відбувається інкапсуляція потоку контенту провайдера у формати MPEG1, MPEG2, MPEG4,

(11) 93307 (13) C2
(19) UA

WM, RA, RV, AVI, OGG, MP3, PCM, WAV, AIFF, ADPCM для передачі по протоколах HTTP, RTP, RTSP, FTP.

5. Спосіб за п. 1, який **відрізняється** тим, що потік контенту передається на САП у вигляді DVB сигналів DVB-S, DVB-T, DVB-C, DVB-H або по ASI або SPI інтерфейсам.

6. Спосіб за п. 1, який **відрізняється** тим, що потік контенту передається на САП у вигляді аналогових відео-, аудіосигналів.

7. Спосіб за п. 1, який **відрізняється** тим, що потік контенту передається на САП через комп'ютерну мережу в UDP пакетах для multicast і unicast IP адрес.

8. Спосіб за п. 1, який **відрізняється** тим, що контент передається на САП у вигляді файлів у форматах TS, MPEG1, MPEG2, MPEG4, WM, RA, RV, AVI, OGG, MP3, PCM, WAV, AIFF, ADPCM.

9. Спосіб за п. 8, який **відрізняється** тим, що дані файлів контенту, що передаються на САП, заздалегідь скрембльовані/зашифровані за допомогою CW.

10. Спосіб за п. 9, який **відрізняється** тим, що CW передаються на САП у складі ECM.

11. Спосіб за п. 9, який **відрізняється** тим, що CW передаються на САП в окремому файлі.

12. Спосіб за будь-яким з п. 10 або п. 11, який **відрізняється** тим, що файли контенту передаються на САП через комп'ютерну мережу по протоколах HTTP, RTP, RTSP, FTP.

13. Спосіб за будь-яким з п. 10 або п. 11, який **відрізняється** тим, що файли контенту передаються на САП на змінному носії DVD, CD, Flash пам'яті жорсткому диску.

14. Спосіб за п. 1, який **відрізняється** тим, що дані ретрансльованого потоку контенту провайдера захищаються за допомогою спільного алгоритму скремблювання CSA.

15. Спосіб за п. 1, який **відрізняється** тим, що дані ретрансльованого потоку контенту провайдера захищаються за допомогою алгоритмів шифрування RC4, AES-128, ГОСТ 28147-89, DES, HC-128.

16. Спосіб за п. 15, який **відрізняється** тим, що дані потоку контенту провайдера скремблюються/шифруються на САП.

17. Спосіб за п. 1, який **відрізняється** тим, що для підтвердження повноважень СТ, сервер-валідатор генерує html сторінку, де пропонується вибір варіантів підтвердження умов доступу до контенту або якщо такий вибір був обумовлений передплатником раніше, можливість прийняти варіант підписки за умовчанням.

18. Спосіб за п. 1, який **відрізняється** тим, що для підтвердження повноважень СТ, сервер-валідатор генерує html сторінку, де пропонується ввести PIN код.

19. Спосіб за п. 1, який **відрізняється** тим, що при виборі варіанта контенту при інтерактивній взаємодії з EPG, пропонується ввести PIN код або ключову фразу, яка далі у складі повідомлення запиту надходить на сервер-валідатор.

20. Спосіб за п. 1, який **відрізняється** тим, що для перевірки повноважень доступу до контенту, сервер-валідатор використовує як ID мережеву апаратну адресу MAC терміналу, призначену для те-

рміналу IP адресу, серійний номер терміналу, ключову фразу, PIN код або їх комбінацію.

21. Спосіб за п. 1, який **відрізняється** тим, що сервер-валідатор генерує повідомлення для сервера управління доступом мережею про дозвіл доступу до контенту СТ передплатника, у складі якого передають як ID апаратну мережеву адресу MAC, призначену IP адресу СТ, серійний номер терміналу, ключову фразу, PIN код або їх комбінацію.

22. Спосіб за п. 1, який **відрізняється** тим, що після запиту доступу до контенту СТ до серверу-валідатора при відхиленні повноважень для доступу до контенту формується повідомлення для СУД про заборону доступу до контенту для терміналу з вказаним ID, при цьому для даного СТ СУД конфігурує заборону доступу до IP адреси контенту в УКС на абонентському порту.

23. Спосіб за п.1, який **відрізняється** тим, що валідатор взаємодіє із СТ, використовуючи протоколи передачі пароля PIN коду, використовуючи алгоритми MD5, SHA1, ГОСТ Р 34.11-94 .

24. Спосіб за п.1, який **відрізняється** тим, що сервер-валідатор взаємодіє з терміналом, встановлюючи захищене з'єднання по протоколах SSL/TLS, IPSec, PPTP.

25. Спосіб за п.1, який **відрізняється** тим, що СУД взаємодіє із СТ передплатника через EPG по протоколах http/https.

26. Спосіб за п. 1, який **відрізняється** тим, що сформовані у валідаторі SK надходять на САП, де за допомогою алгоритмів шифрування AES-128, ГОСТ 28147-89, DES, HC-128 зашифровують CW перед їх приміщенням в ECM.

27. Спосіб за п. 1, який **відрізняється** тим, що сесійні ключі SK для САП і абонентських терміналів представлені наборами ключів, що діють одночасно, але з різним часом дії, набір ключів з часом дії 1, 3, 5, 15 хвилин, 1, 3, 5, 12 годин, день, тиждень, місяць, декаду, квартал, рік.

28. Спосіб за п. 1, який **відрізняється** тим, що сесійні ключі SK генеруються або беруться з попереднього запису в сервері-валідаторі.

29. Спосіб за п. 1, який **відрізняється** тим, що сесійні ключі SK передаються в сервер-валідатор від провайдера контенту.

30. Спосіб за п. 1, який **відрізняється** тим, що для доступу до потоку контенту провайдера при multicast IP адресації використовується протокол IGMP.

31. Спосіб за п. 1, який **відрізняється** тим, що для доступу абонента до порту комп'ютерної мережі використовуються протоколи RADIUS, SNMP, ARP або їх комбінація.

32. Спосіб за п. 1, який **відрізняється** тим, що CW провайдера дешифруються через офіційний модуль умовного доступу CAM провайдера контенту.

33. Спосіб за п. 1, який **відрізняється** тим, що CW провайдера передаються через захищений канал з сервера провайдера контенту.

34. Спосіб за п. 32 або п. 33, який **відрізняється** тим, що в CW дешифруються з ECM потоку контенту провайдера в САП.

35. Спосіб за п. 32 або п. 33, який **відрізняється** тим, що в CW дешифруються з ЕСМ потоку контенту провайдера в сервері-валідаторі.

36. Спосіб за п. 32 або п. 33, який **відрізняється** тим, що в CW передається на СТ у відкритому вигляді, але по захищеному каналу зв'язку.

37. Спосіб за п. 1, який **відрізняється** тим, що в САП допускається в окремі пакети даних потоку контенту провайдера вводити спеціальні малопомітні спотворення - водяні знаки.

38. Спосіб за п. 1, який **відрізняється** тим, що СУД генерує повідомлення для системи білінга оператора комп'ютерної мережі для початку/закінчення тарифікації доступу мережевого терміналу до потоку контенту провайдера.

39. Спосіб за п. 1, який **відрізняється** тим, що сервер-валідатор генерує повідомлення для системи білінга оператора комп'ютерної мережі для початку/закінчення тарифікації доступу мережевого терміналу до потоку контенту провайдера.

40. Спосіб за п. 1, який **відрізняється** тим, що повідомлення для системи білінга оператора комп'ютерної мережі надходять одночасно від сервера-валідатора і від СУД.

41. Спосіб за п. 1, який **відрізняється** тим, що сервер-валідатор відповідає на запити СТ для видачі SK, згідно з вбудованою в нього базою даних, що містить не менше одного з наступних полів: PIN код, мережева апаратна адреса терміналу, лічильник тимчасового ліміту, що залишився, і термін дії для використання PIN коду даного запису.

42. Спосіб за п. 1, який **відрізняється** тим, що після авторизації передплатника допускається надання сервером-валідатором, по запитах СТ, сесійних ключів SK для групи потоків контенту провайдера без ініціації повторних процедур формування доступу для потоку контенту провайдера.

43. Спосіб за п. 1, який **відрізняється** тим, що модуль білінга оператора комп'ютерної мережі через сервер-валідатор надає звіти для провайдеру контенту.

44. Система умовного доступу для вживання в комп'ютерних мережах, що містить не менше одного сервера адаптації потоків САП контенту провайдера, що привласнює потокам контенту унікальні адреси базового Інтернет-протоколу IP для керованої оператором комп'ютерної мережі УКС, доступ до яких можливий через безліч мережевих терміналів СТ, що містять в собі програвач контенту, дескремблер, модуль запити доступу до контенту, зв'язаний через комп'ютерну мережу з сервером управління доступом передплатника СУД в комп'ютерну мережу і сервером-валідатором, що надає для СТ сесійні ключі SK, що захищають слова, що управляють CW, для даних контенту провайдера, причому САП забезпечує виконання процесу адаптації захищеного скрембльованого потоку контенту провайдера для ретрансляції в УКС, при ретрансляції на САП відбувається перекапсуляція потоку біт контенту у формат, придатний для передачі за допомогою IP адресації, при цьому блоки скрембльованих/зашифрованих даних потоків контенту провайдера не видозмінюються, а слова, що управляють CW, необхідні для

дескремблювання/розшифровки даних контенту, зашифровуються за допомогою SK, що передаються на САП від сервера-валідатора, і поміщаються в потік повідомлень управління правами ЕСМ, процедура формування доступу до контенту полягає в тому, що за допомогою інтерактивної взаємодії з електронним програмним гідом EPG, функціонально пов'язаним з СУД, СТ генерує запит ініціалізації доступу до вибраного потоку по IP адресі сервера-валідатора, що містить в собі ідентифікатор ID СТ і умовний номер вибраного потоку контенту, у відповідь на який сервер-валідатор для СТ передплатника генерує запит на підтвердження повноважень доступу до контенту, у відповідь СТ посилає повідомлення з персональною ключовою фразою, при успішній авторизації СТ сервер-валідатор генерує повідомлення для СУД, що містить ID СТ і умовний номер потоку контенту, що вирішує доступ для даного СТ до вибраного контенту передплатника, далі СУД посилає повідомлення для СТ, що містить IP адресу вибраного потоку контенту, одночасно з цим формується захищений канал зв'язку між СТ і сервером-валідатором, по якому сервер-валідатор у відповідь на запити посилає повідомлення з поточними SK, процедури відтворення потоку контенту СТ, що полягає в тому, що СТ з прийнятих від САП по IP адресі даних вибраного потоку провайдеру демультимплексує ЕСМ, дешифрує CW за допомогою SK, дескремблює за допомогою CW дані контенту і відтворює їх програвачем, при цьому відтворення потоку може бути зупинене або оператором комп'ютерної мережі шляхом відмови доступу для даного терміналу до IP адреси контенту в УКС на абонентському порту, або за ініціативою сервера-валідатора, при його відмові видати запрошуваний терміналом SK.

45. Система за п. 44, яка **відрізняється** тим, що як термінал використовується комп'ютерна приставка сет топ бокс STB.

46. Система за п. 44, яка **відрізняється** тим, що як термінал використовується персональний комп'ютер зі встановленим на ньому відповідним програмним забезпеченням.

47. Система за п. 44, яка **відрізняється** тим, що модуль електронного програмного гіда EPG вбудований до СУД.

48. Система за п. 44, яка **відрізняється** тим, що модуль EPG виконаний у вигляді одного або декількох серверів.

49. Система за п. 44, яка **відрізняється** тим, що у складі САП присутній один або більш офіційний модуль умовного доступу САМ провайдеру контенту.

50. Система за п. 44, яка **відрізняється** тим, що у складі сервера-валідатора присутній один або більш офіційний САМ провайдеру контенту.

51. Система за п. 44, яка **відрізняється** тим, що допускається функціонування безлічі серверів-валідаторів, що належать різним провайдерам контенту.

52. Система за п. 44, яка **відрізняється** тим, що в її складі є модуль білінга.

53. Система за п. 52, яка **відрізняється** тим, що модуль білінга поєднаний з сервером-валідатором.

54. Система за п. 52, яка **відрізняється** тим, що модуль білінга поєднаний з СУД.

55. Система за п. 44, яка **відрізняється** тим, що сервер-валідатор містить базу даних, що має не менше одного з наступних полів: PEM код, мережева апаратна адреса MAC CT передплатника, IP адреса CT передплатника, лічильник тимчасового ліміту, що залишився, термін дії для використання PEN коду даного запису.

56. Система за п. 55, яка **відрізняється** тим, що сервер-валідатор містить у складі бази даних як

обов'язкове поле записи PIN коду, причому безлічі PIN кодів відповідає безліч карт оплати.

57. Система за п. 56, яка **відрізняється** тим, що карти оплати представлені на матеріальному носії з їх записом, захищеним захисним шаром і поширюваних в торгівельній мережі.

58. Система за п. 56, яка **відрізняється** тим, що карти оплати представлені у вигляді записів PIN кодів на серверах електронної комерції.

59. Система за п. 44, яка **відрізняється** тим, що сервер-валідатор розташовується на території провайдера контенту.

60. Система за п. 44, яка **відрізняється** тим, що сервер-валідатор і СУД мають спільну адресу.

Винахід відноситься до системи мовлення і прийому і системи умовного доступу для неї для вживання в комп'ютерних мережах.

В даний час найбільш широкого поширення набула дистрибуція провайдерами мультимедійного контенту (аудіовізуальних матеріалів) в цифрових форматах, використовуючи при цьому для поширення контенту як передачу записів контенту у вигляді файлів, так і реалізації специфікацій Digital Video Broadcasting (DVB). При цьому, рівень обхвату населення комп'ютерними мережами неухильно розширюється, що викликає інтерес до них як перспективна середа дистрибуції мультимедійного контенту. Проте, для повсюдного впровадження технологій мовлення мультимедійного контенту в комп'ютерних мережах в даний час є ряд стримуючих чинників - основними з них є - досить висока вартість устаткування головних станцій, що перетворюють криптографічний захищений формат мультимедійного контенту в новий криптографічний захищений формат, придатний для використання в комп'ютерній мережі. З іншого боку постачальники мультимедійного контенту не завжди можуть довіряти операторам комп'ютерних мереж і бажають мати незалежний від операторів мереж механізм контролю за підписчиками, що гарантує, виключення зловживань потенційними споживачами контенту.

У патенті США № 6307939 розкритий спосіб зниження витрат при організації ретрансляції захищеного контенту (адаптації) для дистрибуції у складі іншої мережі з системою умовного доступу.

Спосіб пропонує не видозмінювати характер криптозахисту (скремблювання) даних контенту, а лише модифікувати потік індивідуальних повідомлень ECM, EMM (згідно угод, прийнятих в техніку SIMULCRYPT, стандартизованою специфікацією ETSI TS 101 197 V1.2.1), за допомогою яких слово, що управляє (CW), для дескремблера передається на абонентський термінал підписчика. Проте, при реалізації вказаного способу в комп'ютерній мережі очевидні наступні недоліки: для дешифровки CW передбачається використовувати способи характерні для однонаправлених мереж передачі цифрового мультимедійного контенту (таких як супутникове DVB-S і кабельне телебачення DVB-C), що пов'язане з ускладненням терміналів підпи-

счиків і підвищеною уразливістю для зловживань шляхом підробки модулів і карт умовного доступу.

Спосіб обмеження доступу до контенту засобами управління комп'ютерною мережею розкривається в патенті США № 7188245, де показані варіанти обмеження доступу до контенту використовуючи протоколи і апаратні засоби управління (конфігурації) комп'ютерної мережі. Подібні способи організації обмеження привабливі з точки зору оператора мережі - оскільки всі необхідні компоненти для цього вже містяться в структурі більшості комп'ютерних мереж. Проте даний спосіб не може задовольнити дистрибутерів мультимедійного контенту, оскільки залишається з одного боку можливість для заховання дійсної кількості підписчиків в звітах для провайдера контенту, а з іншого боку залишається можливість неконтрольованого копіювання і подальшого поширення контенту нечесними підписчиками доступу до мережі оператора.

Історично склалася ситуація, коли основним критерієм, яким керуються провайдери контенту, для визначення можливості дистрибуції в тій або іншій мережі є можливість прямого і незалежного від оператора мережі контролю за підпискою для кожного абонентського терміналу. Способи, що допускають подібний контроль (для: легальних підписчиків), описуються в патентах США № 6532539 № 6898285 № 7120253, № 7149309. Проте всі описані у вищезгаданих заявках способи, не можуть гарантувати недоступність контенту, для недобросовісних підписчиків при використанні ними широко відомою і поширеною піратами DVB контенту технології характерної для однонаправлених мереж передачі даних, відомої як кардшарінг. Дана недобросовісна технологія полягає в тому, що підписчики встановлюють у себе програмне забезпечення, у складі якого є дескремблер і модуль запитів на сторонній кард сервер, який може містити в своєму складі легальний модуль системи умовного доступу (CAM), причому, з точки зору провайдера цей сервер розглядається як цілком легальний термінал підписчика, але при цьому він може по запитах інших користувачів видавати їм дешифровані CW. Більш того, подібний спосіб маніпуляції з системою умовного доступу (CAS) в комп'ютерній мережі може виявитися ще зручнішим і набути дуже широкого поширення. Таким

чином, зрозуміло, що провайдери мультимедійного контенту насторожено, розглядають відомі CAS для редистрибуції якісного мультимедійного контенту через комп'ютерні мережі, отже, потрібна нова система забезпечення доступу до ретранслюваного в комп'ютерній мережі контенту, одночасно з цим технічна реалізація такого рішення має бути максимально простою, щоб бути економічно привабливою для операторів комп'ютерних мереж. Очевидно, задовольнити повною мірою суперечливим вимогам, провайдерами мультимедійного контенту, що висувуються, з одного боку, і вимогам операторів вже існуючих комп'ютерних мереж з іншою, може лише спосіб умовного доступу здійснюючий комплексний підхід до поставленого завдання - що поєднує в собі збереження вимог до якості захисту забезпечуваною поширеними системами умовного доступу для однонаправлених каналів зв'язку (побудованих на основі криптографічних протоколів таких як системи Viaccess, Irdeto, NDS), одночасно з можливістю організації умовного доступу на основі управління і конфігурації комп'ютерної мережі спільно з використанням криптографічних протоколів авторизації і протоколів захищених з'єднань, таких як протокол захисних сокетів (Secure Socket Layer SSL) або IP Security (IPSec).

Найбільш близьким по своїй технічній суті до винаходу, що заявляється, є спосіб розкритий в патенті № EP 1525732, де описується спосіб взаємодії між підписником, сервером для авторизації підписчика і сервером що надає контент від провайдера, що дозволяє запропонувати добре захищені рішення для доступу до контенту в комп'ютерних мережах, проте в ньому мається на увазі безпосередня участь сесійних ключів для підписників в процесі підготовки (шифрування) контенту для трансляції. Це скрутно для більшості вже існуючих провайдерів контенту, оскільки вимагає істотної модифікації використовуваного ними програмно-апаратного забезпечення через те що спосіб не передбачає використання засобів для прямої ретрансляції захищеного контенту з потоками повідомлень управління правами (ECM) і надання прав (EMM) і адаптації вказаного контенту в комп'ютерній мережі, при збереженні контролю в подібному випадку за підписниками з боку сторони провайдера контенту.

Дане технічне рішення вибране прототипом. Прототип і винахід, що заявляється, мають наступні спільні ознаки:

- система умовного доступу для вживання в комп'ютерних мережах, що містить функціональні еквіваленти пристроїв, характерні для винаходу, що заявляється,

- сервера адаптації потоків (САП) контенту провайдера, безліч мережевих терміналів (СТ), що містять в собі програвач контенту, дескремблер, модуль запиту доступу до контенту, зв'язаний через комп'ютерну мережу з сервером управління доступу підписчика (СУД) в комп'ютерну мережу сервером валідатором.

В основу винаходу поставлено завдання створення способу функціонування і системи, що забезпечує можливість ретрансляції захищеного

провайдером контенту в комп'ютерній мережі, при збереженні контролю за підписниками з боку провайдера контенту.

Поставлене завдання здійснене в способі, що заявляється:

використанням не менше одного сервера адаптації потоків (САП) контенту провайдера, що привласнює потокам контенту унікальні адреси базового Інтернет-протоколу (IP) для керованої оператором комп'ютерної мережі (УКС), доступ до яких можливий через безліч мережевих терміналів (СТ), що містять в собі програвач контенту, дескремблер, модуль запиту доступу до контенту, зв'язаний через комп'ютерну мережу з сервером управління доступом підписчика (СУД) в комп'ютерну мережу і сервером-валідатором, що надає для СТ сесійні ключі (SK), що захищають слова (CW), що управляють, для даних контенту провайдера, що забезпечує виконання наступних дій:

процесу адаптації захищеного (скрембльованого) потоку контенту провайдера для ретрансляції в УКС, при якій на САП відбувається перекапсуляція потоку біт контенту у формат, придатний для передачі за допомогою IP адресації, при цьому блоки скремблених/зашифрованих даних потоків контенту провайдера не видозмінюються, а слова, що управляють (CW), необхідні для дескремблювання/расшифровки даних контенту, зашифровуються за допомогою SK, що передаються на САП від сервера-валідатора, і поміщаються в потік повідомлень управління правами (ECM), процедури формування доступу до контенту, при якій за допомогою інтерактивної взаємодії з електронним програмним гідом (EPG), функціонально пов'язаним з СУД, СТ генерує запит ініціації доступу до вибраного потоку по IP адресі сервера-валідатора, ідентифікатор (ID) СТ і умовний номер вибраного потоку контенту, що містить в собі, у відповідь на який сервер-валідатор для СТ підписчика генерує запит для підтвердження повноважень доступу до контенту, у відповідь СТ посилає повідомлення з персональною ключовою фразою, при успішній авторизації підписчика сервер-валідатор генерує повідомлення для СУД, що містить ID СТ, і умовний номер потоку контенту, що вирішує доступ для даного СТ до вибраного контенту підписчика, далі СУД посилає повідомлення для СТ, що містить IP адресу вибраного потоку контенту, одночасно з цим, формується захищений канал зв'язку між СТ і сервером-валідатором по якому сервер-валідатор у відповідь на запити посилає повідомлення з поточними SK, процедури відтворення потоку контенту СТ, при цьому СТ з прийнятих від САП по IP адресі даних вибраного потоку провайдера демультимплексує ECM, дешифрує CW за допомогою SK, дескремблює за допомогою CW дані контенту і відтворює їх програвачем, при цьому відтворення потоку може бути зупинене як оператором комп'ютерної мережі шляхом відмови доступу для даного терміналу до IP адресі контенту в УКС на абонентському порту, так і за ініціативою сервера-валідатора, при його відмові видати запрошуваний терміналом SK.

- При цьому САП видаляє у вихідному потоці контенту ECM і повідомлення управління надан-

ням прав (EMM) провайдера контенту, при цьому допускається призначати новому потоку ECM IP адресу, відмінну від IP адреси решти частки контенту.

- У САП відбувається інкапсуляція потоку контенту провайдера у формат транспортного потоку (TS) для трансляції в UDP пакетах для multicast або unicast IP адрес.

- У САП відбувається інкапсуляція потоку контенту провайдера у формати MPEG1, MPEG2, MPEG4, WM, RA, RV, AVI, OGG, MP3, PCM, WAV, AIFF, ADPCM для передачі по протоколах HTTP, RTP, RTSP, FTP.

- Потік контенту передається на САП у вигляді DVB сигналів (DVB-S, DVB-T, DVB-C, DVB-H) або по ASI або SPI інтерфейсам.

- Потік контенту передається на САП у вигляді аналогових (відео, аудіо) сигналів.

- Потік контенту передається на САП через комп'ютерну мережу в UDP пакетах для multicast і unicast IP адрес.

- Контент передається на САП у вигляді файлів у форматах TS, MPEG1, MPEG2, MPEG4, WM, RA, RV, AVI, OGG, MP3, PCM, WAV, AIFF, ADPCM.

- Дані файлів контенту, що передаються на САП заздалегідь скрембльовані/зашифровані за допомогою CW.

- CW передаються на САП у складі ECM, а на САП в окремому файлі, при цьому, файли контенту передаються на САП через комп'ютерну мережу по протоколах HTTP, RTP, RTSP, FTP на змінному носії DVD, CD, Flash пам'яті, жорсткому диску.

- Дані ретрансльованого потоку контенту провайдера захищаються за допомогою спільного алгоритму скремблювання (CSA).

- Дані ретрансльованого потоку контенту провайдера захищаються за допомогою алгоритмів шифрування RC4, AES-128, ГОСТ 28147-89, DES, HC-128.

- Дані потоку контенту провайдера скремблюються/шифруються на САП.

- Для підтвердження повноважень СТ, сервер-валідатор генерує html сторінку, де пропонується вибір варіантів підтвердження умов доступу до контенту, або якщо такий вибір був обумовлений підписчиком раніше, можливість прийняти варіант підписки за умовчанням.

- Для підтвердження повноважень СТ, сервер-валідатор генерує html сторінку де пропонується ввести PIN код.

- При виборі варіанту контенту при інтерактивній взаємодії з EPG, пропонується ввести PIN код або ключову фразу, яка далі у складі повідомлення запиту поступає на сервер-валідатор.

- Для перевірки повноважень доступу до контенту, сервер-валідатор використовує як ID мережеву апаратну адресу (MAC) терміналу, призначену для терміналу IP адресу, серійний номер терміналу, ключову фразу, PIN код або їх комбінацію.

- Сервер-валідатор генерує повідомлення для сервера управління доступом мережею, про дозвіл доступу до контенту СТ підписчика, у складі якого передаються як ID апаратну мережеву адресу

(MAC), призначену IP адресу СТ, серійний номер терміналу, ключову фразу, PIN код або їх комбінацію.

- Після запиту доступу до контенту СТ до серверу-валідатору при відхиленні повноважень для доступу до контенту формується повідомлення для СУД про заборону доступу до контенту для терміналу з вказаним ID, при цьому для даного СТ СУД конфігурує заборону доступу до IP адресу контенту в УКС на абонентському порту.

- Валідатор взаємодіє із СТ використовуючи протоколи передачі пароля (PGN коду) використовуючи алгоритми MD5, SHA1, ГОСТ Р 34.11-94.

- Сервер-валідатор взаємодіє з терміналом встановлюючи захищене з'єднання по протоколах SSL/TLS, IPSec, PPTP.

- СУД взаємодіє із СТ підписчика через EPG по протоколах http/https.

- Сформовані у валідаторі SK поступають на САП, де за допомогою алгоритмів шифрування AES-128, ГОСТ 28147-89, DES, HC-128 зашифровують CW перед їх приміщенням в ECM.

- Сесійні ключі SK для САП і абонентських терміналів представлені наборами ключів, що діють одночасно, але з різним часом дії (набір ключів з часом дії 1, 3, 5, 15, хвилин, 1, 3, 5, 12 годин, день, тиждень, місяць, декаду, квартал, рік).

- Сесійні ключі SK генеруються або беруться з попереднього запис в сервері-валідаторі.

- Сесійні ключі SK передаються в сервер-валідатор від провайдера контенту.

- Для доступу до потоку контенту провайдера при multicast IP адресації використовується протокол IGMP.

- Для доступу абонента до порту комп'ютерної мережі використовуються протоколи RADIUS, SNMP, ARP або їх комбінація.

- CW провайдера дешифруються через офіційний модуль умовного доступу (CAM) провайдера контенту.

- CW провайдера передаються через захищений канал з сервера провайдера контенту.

- CW дешифруються з ECM потоку контенту провайдера в САП.

- У CW дешифруються з ECM потоку контенту провайдера в сервері -валідаторі.

- У CW передається на СТ у відкритому вигляді, але по захищеному каналу зв'язку.

- У САП допускається в окремі пакети даних потоку контенту провайдера вводити спеціальні малопомітні спотворення – водяні знаки.

- СУД генерує повідомлення для системи биллінга оператора комп'ютерної мережі для початку/закінчення тарифікації доступу мережевого терміналу до потоку контенту провайдера.

- Сервер-валідатор генерує повідомлення для системи биллінга оператора комп'ютерної мережі для початку/закінчення тарифікації доступу мережевого терміналу до потоку контенту провайдера.

- Повідомлення для системи биллінга оператора комп'ютерної мережі поступають одночасно від сервера-валідатора і від СУД.

- Сервер-валідатор відповідає на запити СТ для видачі SK, згідно вбудованої в нього бази даних, що містить не менш одного з наступних полів:

PIN код, мережева апаратна адреса терміналу, лічильник тимчасового ліміту, що залишився, і термін дії для використання PIN коду даного запису.

- Після авторизації підписчика допускається надання сервером-валідатором, по запитах СТ, сесійних ключів SK для групи потоків контенту провайдера без ініціації повторних процедур формування доступу для потоку контенту провайдера.

- Модуль білінга оператора комп'ютерної мережі через сервер-валідатор надає звіти для провайдера контенту.

Поставлене завдання вирішене в системі, що заявляється тим, що вона включає не менше одного сервера адаптації потоків (САП) контенту провайдера, що привласнює потокам контенту унікальні адреси базового Інтернет-протоколу (IP) для керованої оператором комп'ютерної мережі (УКС), доступ до яких можливий через безліч мережевих терміналів (СТ), що містять в собі програвач контенту, дескремблер, модуль запиту доступу до контенту, зв'язаний через комп'ютерну мережу з сервером управління доступом підписчика (СУД) в комп'ютерну мережу і сервером-валідатором, що надає для СТ сесійні ключі (SK), що захищають слова (CW), що управляють, для даних контенту провайдера, причому САП забезпечує виконання процесу адаптації захищеного (скрембльованого) потоку контенту провайдера для ретрансляції в УКС, при ретрансляції на САП відбувається перекапсуляція потоку біт контенту у формат, придатний для передачі за допомогою IP адресації; при цьому блоки скрембльованих/зашифрованих даних потоків контенту провайдера не видозмінюються, а слова, що управляють (CW), необхідні для дескремблювання/розшифровки даних контенту, зашифровуються за допомогою SK, що передаються на САП від сервера-валідатора, і поміщаються в потік повідомлень управління правами (ЕСМ), процедура формування доступу до контенту полягає в тому, що за допомогою інтерактивної взаємодії з електронним програмним гідом (EPG), функціонально пов'язаним з СУД, СТ генерує запит ініціалізації доступу до вибраного потоку по IP адресі сервера-валідатора, що містить в собі ідентифікатор (ID) СТ і умовний номер вибраного потоку контенту, у відповідь на який сервер-валідатор для СТ підписчика генерує запит на підтвердження повноважень Доступу до контенту, у відповідь СТ посилає повідомлення з персональною ключовою фразою, при успішній авторизації СТ сервер-валідатор генерує повідомлення для СУД, що містить ID СТ і умовний номер потоку контенту, що вирішує доступ для даного СТ до вибраного контенту підписчика, далі СУД посилає повідомлення для СТ, що містить, IP адресу вибраного потоку контенту, одночасно з цим формується захищений канал зв'язку між СТ і сервером-валідатором по якому сервер-валідатор у відповідь на запити посилає повідомлення з поточними SK, процедури відтворення потоку контенту СТ, що полягає в тому, що СТ з прийнятих від САП по IP адресі даних вибраного потоку провайдера демультіплексирує ЕСМ, дешифрує CW за допомо-

гою SK, дескремблює за допомогою CW дані контенту і відтворює їх програвачем, при цьому відтворення потоку може бути зупинене або оператором комп'ютерної мережі шляхом відмови доступу для даного терміналу до IP адресі контенту в УКС на абонентському порту, або за ініціативою сервера-валідатора, при його відмові видати, запрошуваний терміналом SK.

- Де як термінал використовується комп'ютерна приставка сет топ бокс (STB).

- Як термінал використовується персональний комп'ютер зі встановленим на ньому відповідним програмним забезпеченням.

- Модуль електронного програмного гіда (EPG), вбудований до СУД.

- Модуль EPG виконаний у вигляді одного або декількох серверів.

- У складі САП присутній один або більш офіційний модуль умовного доступу (CAM) провайдера контенту.

- У складі сервера-валідатора присутній один або більш офіційний САМ провайдера контенту.

- Допускається функціонування безлічі серверів-валідаторів, що належать різним провайдерам контенту.

- У її складі є модуль білінга.

- Модуль білінга поєднаний з сервером-валідатором.

- Модуль білінга поєднаний з СУД.

- Сервер-валідатор містить базу даних що має не менш одного з наступних полів: PIN код, мережева апаратна адреса (MAC) СТ підписчика, IP адреса СТ підписчика, лічильник тимчасового ліміту, що залишився, термін дії для використання PIN коду даного запису.

- Сервер-валідатор містить у складі бази даних як обов'язкове поле - записи PIN коду, причому безлічі PIN кодів відповідає безліч карт оплати.

- Карти оплати представлені на матеріальному носіїві з їх записом, захищеним захисним шаром і поширюються в торгівельній мережі.

- Карти оплати представлені у вигляді записів PIN кодів на серверах електронної комерції.

- Сервер-валідатор розташовується на території провайдера контенту.

- Сервер-валідатор і СУД мають спільну адресу IP.

Перераховані вище ознаки є новими і за їх рахунок досягається наступний технічний результат - з'являється можливість ретрансляції захищеного провайдером контенту в комп'ютерній мережі при збереженні контролю за підписчиками з боку провайдера контенту.

Для подолання недоліків рівня техніки, що наведені вище, запропонований спосіб функціонування системи умовного доступу для вживання в „комп'ютерних мережах, що полягає у взаємодії серверів адаптації потоків (САП) контенту провайдера, керованій оператором комп'ютерної мережі (УКС)

мережевих терміналів (СТ), сервером управління доступом підписчика (СУД) в комп'ютерну мережу і сервера-валідатора, що забезпечує контроль прав провайдера контенту. Аспекти взаємо-

дії вказаних пристроїв справжнього винаходу будуть показані на кресленнях, де:

Фіг. 1 схематично показує варіант здійснення системи згідно винаходу, що заявляється;

Фіг. 2 показує діаграму обміну повідомленнями в процедурах формування доступу до контенту і відтворення потоку контенту;

Фіг. 3 показує діаграму обміну повідомленнями при спрощеній процедурі формування доступу.

Високу економічну ефективність реалізації запропонованого способу забезпечує вживання (див. Фіг. 1) САП 2, на якому реалізований процес адаптації потоків провайдеру контенту 1 до ретрансляції в УКС 3. Процес адаптації захищеного (скрембльованого) потоку контенту провайдеру полягає в перекапсуляції потоку біт контенту у формат, придатний для передачі за допомогою ІР адресації, при цьому блоки скрембльованих даних потоку контенту провайдеру не видозмінюються, а слова, що управляють (CW), необхідні для їх дескремблювання/розшифровки, зашифровуються за допомогою сесійних ключів (SK), що передаються на САП від сервера-валідатора і поміщаються в потік повідомлень управління правами (ECM).

САП призначає потокам контенту унікальні адреси базового інтернет-протоколу (IP).

Можливість забезпечити захист для доступу до контенту в комп'ютерних мережах спосіб досягає використанням процедур формування доступу до контенту і відтворення потоку контенту. У вказаних процедурах беруть (див. Фіг.1) участь СУД 5, функціонально пов'язаний з модулем електронного програмного гіда (EPG) 6, сервер-валідатор 7, СТ 4, модуль білінга 8.

Процедура формування доступу до контенту, при якій за допомогою інтерактивної взаємодії з електронним програмним гідом (EPG) при обміні повідомленнями (див. Фіг.2) М1 і М2, СТ генерує запит М3 для ініціації доступу до вибраного потоку по ІР адресі сервера-валідатора, що містить в собі ідентифікатор (ID) СТ і умовний номер вибраного потоку контенту, у відповідь на який сервер-валідатор для СТ підписчика генерує запит для підтвердження повноважень доступу до контенту М4 у відповідь СТ посилає повідомлення з персональною ключовою фразою М5, при успішній авторизації підписчика сервер-валідатор генерує повідомлення для СУД М6, що містить, ID СТ і умовний номер потоку контенту, що вирішує доступ для даного СТ до вибраного контенту підписчика, далі СУД посилає повідомлення для СТ М7, що містить ІР адресу вибраного потоку контенту. Одночасно з цим, формується захищений канал зв'язку між СТ і сервером-валідатором, використований в процедурі відтворення потоку контенту.

Процедура відтворення потоку контенту СТ (див. Фіг. 2), полягає в тому, що термінал приймає потік контенту по його ІР адресу, демультимплексує з нього ECM, дешифрує С W за допомогою SK, дескремблює за допомогою CW дані контенту і відтворює їх програвачем. При цьому поточні SK СТ отримує по запитах М8 через захищений канал зв'язку від сервера-валідатора в повідомленнях М9. Контроль прав провайдеру контенту полягає в

даному випадку в тому, що відтворення потоку може бути зупинене як оператором комп'ютерної мережі шляхом відмови доступу для даного терміналу до ІР адреси контенту в УКС на абонентському порту, так і за ініціативою сервера-валідатора, при його відмові видати запрошуваний терміналом SK.

Посилення захисту контенту в даному способі досягається тим що САП видаляє у вихідному потоці контенту оригінальні ECM і повідомлення управління наданням прав (EMM) провайдеру контенту. Перешкоджаючи тим самим безпосередньому використанню технологій, відпрацьованих піратами контенту провайдеру для одно направлених каналів зв'язку, таких як DVB-S і DVB-C.

Запропонований спосіб адаптації на САП зручний для використання такою широко поширеною в технології комп'ютерних мереж, як інкапсуляція потоку контенту провайдеру в форматі транспортного потоку (TS) в пакети протоколу дейтаграм користувача (UDP) для широкомовних (multicast) або точка-крапка (unicast) ІР адрес.

Поряд з цим, можлива реалізація механізму мовлення, широко поширеного в Internet, використовуючи протокол управління передачею (TCP), наприклад через протоколи пересилки гіпертекстових файлів (http), протокол реального часу (RTP), протокол реального часу для медіа потоків (RTSP), протокол передачі файлів (FTP). При цьому можлива інкапсуляція потоку контенту провайдеру в один з форматів MPEG1, MPEG2, MPEG4, WM, RA, RV, AVI, OGG, MP3, PCM, WAV, AIFF, ADPCM.

Реалізації потоків контенту провайдеру технічно можуть вдавати із себе різні варіанти, найпоширенішою з яких є трансляція по DVB специфікаціям (DVB-S, DVB-T, DVB-C, DVB-H), при цьому можливе створення функціональної і економічно ефективної реалізації САП при інтеграції на його базі модулів для прийому модульованих DVB потоків контенту або для прийому по асинхронному послідовному (ASI) або синхронному паралельному (SPI) інтерфейсам.

У певних випадках може виявитися зручною реалізація САП з інтегрованими платами захоплення аналогового медіа при якій потік контенту представляє аналогові (відео, аудіо) сигнали.

Потік контенту провайдеру може бути вже сформованими пакетами телебачення по ІР протоколу (IPTV) в UDP пакетах для multicast і unicast ІР адрес, при цьому виходить проста реалізація САП.

Часто контент передається провайдерами у вигляді файлів у форматах TS, MPEG1, MPEG2, MPEG4, WM, RA, RV, AVI, OGG, MP3, PCM, WAV, AIFF, ADPCM як по комп'ютерній мережі, так і на твердих носіях (DVD, CD, Flash карті, жорсткому диску), що також допускає ефективну реалізацію САП. При цьому провайдер має можливість захистити свої права, передаючи не відкритий, а вже скрембльований контент. Максимальний захист досягатиметься в тому випадку, якщо CW передаватимуться окремо від файлів контенту.

Найбільш поширеним способом скремблювання потоку контенту провайдеру є реалізація

спільного алгоритму скремблювання (CSA), проте для процесу адаптації придатні і інші способи криптографічного захисту контенту провайдера, наприклад за допомогою алгоритмів шифрування RC4, AES-128, ГОСТ 28147-89, DES, HC-128. В окремих випадках такий захист - скремблювання/шифрування даних може виконуватися на САП.

Запропонований спосіб допускає створення простих і інтуїтивно зрозумілих інтерфейсів для взаємодії підписників з системою через СТ. Для підтвердження повноважень СТ, сервер-валідатор може генерувати гіпертекстову (html) сторінку де пропонується вибір варіантів підтвердження умов доступу до контенту (наприклад список з номерів вже активованих карт передоплати на різні пакети каналів) або якщо такий вибір був обумовлений підписником раніше, можливість прийняти варіант підписки за умовчанням. Для активізації підписки з такої сторінки можливо запропонувати введення PIN коду.

Глибина інтерактивної взаємодії підписника з CAS в запропонованому способі може бути зменшена при спрощеній процедурі формування доступу (див.Фіг.3). Модифікація способу в даному випадку відрізняється тим, що при виборі варіанту контенту при інтерактивній взаємодії з EPG, пропонується ввести PIN код або ключову фразу, яка далі у складі повідомлення запиту поступає на сервер-валідатор.

Запропонований спосіб роботи CAS для комп'ютерної мережі при перевірці повноважень доступу до контенту як критерій порівняння, в сервер-валідаторе зручно використовувати як ідентифікатор СТ (ID) мережеву апаратну адресу (MAC), призначену для СТ IP адреса, серійний номер терміналу, ключову фразу, PIN код або їх комбінацію. Які далі і передаються на СУД, при успішній авторизації СТ. Крім того можлива реалізація посилення захисту засобами УКС, якщо сервер-валідатор формуватиме повідомлення для СУД про заборону доступу до контенту для неавторизованого терміналу, при цьому для даного СТ СУД конфігурує заборону доступу до IP адресу контенту в УКС на абонентському порту.

Для захисту інтерактивного діалогу між сервером-валідатором і СТ бажано використовувати технології і протоколи передачі пароля (PIN коду) використовуючі алгоритми MD5, SHA1, ГОСТ Р 34.11-94 або використовуючі захищене з'єднання по протоколах SSL/TLS, IPSec, Point-to-Point Protocol (PPTP). Інтерактивна взаємодія підписника з СУД зручно виконати у вигляді html сторінок передаваних по протоколах http/https.

Сформовані в сервері-валідаторі SK поступають на САП, де за допомогою алгоритмів шифрування таких як AES-128 ГОСТ 28147-89, DES, HC-128 зашифровують CW перед їх приміщенням в ЕСМ. Для досягнення необхідного рівня захисту сесійні ключі SK будуть динамічно оновлюватися протягом деяких проміжків часу, при цьому можливе створення гнучких і таких, що легко адмініструються політик безпеки, якщо SK будуть представлені наборами ключів, що діють одночасно але з різним часом дії (наприклад набір ключів з часом дії 1, 3, 5, 15, хвилин, 1, 3, 5, 12 годин). SK техніч-

но можуть генеруватися або вибиратися з попереднього запису в сервері-валідаторі, а так само поступати від провайдера контенту.

У УКС оператора обмеження доступу до потоку контенту провайдера на абонентському порту при multicast IP адресації пропонується використовувати протокол підтримки членства в групах (IGMP). Додатково для доступу абонента до порту комп'ютерної мережі пропонується використовувати протокол RADIUS, описаний в специфікаціях RFC 2058 і RFC 2059, протокол мережевого управління SNMP, протокол відображення адрес ARP або їх комбінацію.

Необхідні для роботи запропонованого способу CW провайдера можуть бути отримані при дешифруванні демультіплексированного потоку ЕСМ в офіційному модулі умовного доступу (CAM) провайдера контенту або поставлятися безпосередньо від сервера провайдера контенту через захищений канал зв'язку. Модуль для екстракції CW входить в складяк сервера-валідатора, так і САП, що диктується конкретними умовами побудови системи. В окремих випадках допускається передавати CW на СТ у відкритому вигляді, але по захищеному каналу зв'язку.

З метою локалізації авторизованого підписника, провайдера, що нелегально тиражує контент, спосіб допускає на САП в окремі пакети даних потоку контенту провайдера вводити спеціальні малопомітні спотворення — водяні знаки.

Для забезпечення прозорих взаєморозрахунків між операторами УКС і провайдерами потоків контенту в способі передбачена інтеграція з системою білінга, в якій, СУД генерує повідомлення для початку/закінчення тарифікації доступу мережевого терміналу до потоку контенту провайдера. У запропонованому способі сервер-валідатор так само має можливість генерувати повідомлення для системи білінга оператора УКС, що унеможливило зловживань.

У способі пропонується використовувати для авторизації і визначення ліміту використання контенту вбудовану в сервер-валідатор базу даних, що містить не менш одного з наступних полів: PIN код, мережева апаратна адреса терміналу, IP адреса терміналу, лічильник тимчасового ліміту, що залишився, і термін дії для використання PIN коду даного запису. При цьому можливе одночасне використання для визначення прав підписника відразу декількох записів цієї бази, для яких він може бути авторизований.

Спосіб передбачає, що доступ до модуля білінга можливий лише для провайдера контенту (бажано щоб вказаний провайдер навіть був власником сервера-валідатора) при цьому модуль білінга оператора комп'ютерної мережі через сервер-валідатор надає звіти для провайдера контенту.

Опис роботи запропонованої системи.

Для реалізації вищеописаного способу умовного доступу, запропонована система умовного доступу (CAS) для вживання в комп'ютерних мережах (див. Фіг.1), що містить не менше одного сервера адаптації потоків (САП) 2 для контенту провайдера 1, що привласнює потокам контенту

унікальні адреси базового Інтернет-протоколу (IP) для керованої оператором комп'ютерної мережі (УКС) 3, доступ до яких можливий через безліч мережевих терміналів (СТ) 4, що містять в собі програвач контенту, дескремблер, модуль запиту доступу до контенту, зв'язаний через комп'ютерну мережу з сервером управління доступом підписчика (СУД) 5 в комп'ютерну мережу і сервером-валідатором 7, що надає для СТ сесійні ключі (SK), що захищають слова що управляють (CW), для даних контенту провайдера, причому САП забезпечує виконання процесу адаптації захищеного, (скрембльованого) потоку контенту провайдера для ретрансляції в УКС, при ретрансляції на САП відбувається перекапсуляція потоку біт контенту у формат, придатний для передачі за допомогою IP адресації, при цьому блоки скрембльованих/зашифрованих даних потоків контенту провайдера не видозмінюються, а слова, що управляють (CW), необхідні для дескремблювання/розшифровки даних контенту, зашифровуються за допомогою SK, що передаються на САП від сервера-валідатора, і поміщаються в потік повідомлень управління правами (ECM), процедура формування доступу до контенту полягає в тому, що за допомогою інтерактивної взаємодії з електронним програмним гідом (EPG) 6, функціонально пов'язаним з СУД, СТ генерує запит ініціалізації доступу до вибраного потоку по IP адресі сервера-валідатора, ідентифікатор (ID) СТ і умовний номер вибраного потоку контенту, що містить в собі, у відповідь на який сервер-валідатор для СТ підписчика генерує запит на підтвердження повноважень доступу до контенту, у відповідь СТ посилає повідомлення з персональною ключовою фразою, при успішній авторизації СТ сервер-валідатор генерує повідомлення для СУД, що містить ID СТ і умовний номер потоку контенту, що вирішує доступ для даного СТ до вибраного контенту підписчика, далі СУД посилає повідомлення для СТ, що містить IP адресу вибраного потоку контенту, одночасно з цим формується захищений канал зв'язку між СТ і сервером-валідатором по якому сервер-валідатор у відповідь на запити посилає повідомлення з поточними SK, процедури відтворення потоку контенту СТ, що полягає в тому, що СТ з прийнятих від САП по IP адресу даних вибраного потоку провайдера демультимплексирує ECM, дешифрує CW за допомогою SK, дескремблює за допомогою CW дані контенту і відтворює їх програвачем, при цьому відтворення потоку може бути зупинене або оператором комп'ютерної мережі шляхом відмови доступу для даного терміналу до IP адресі контенту в УКС на абонентському порту, або за ініціативою сервера-валідатора, при його відмові видати, запрошуваний терміналом SK.

У запропонованій CAS можливо як СТ використовувати як комп'ютерні приставки - сет топ бокси

(STB) так і персональні комп'ютери зі встановленим на них відповідним програмним забезпеченням.

Для інтерактивної взаємодії з СУД в системі пропонується використовувати модуль електронного програмного гіда (EPG), який може бути як вбудований до СУД, так і виконаний у вигляді одного або декількох серверів.

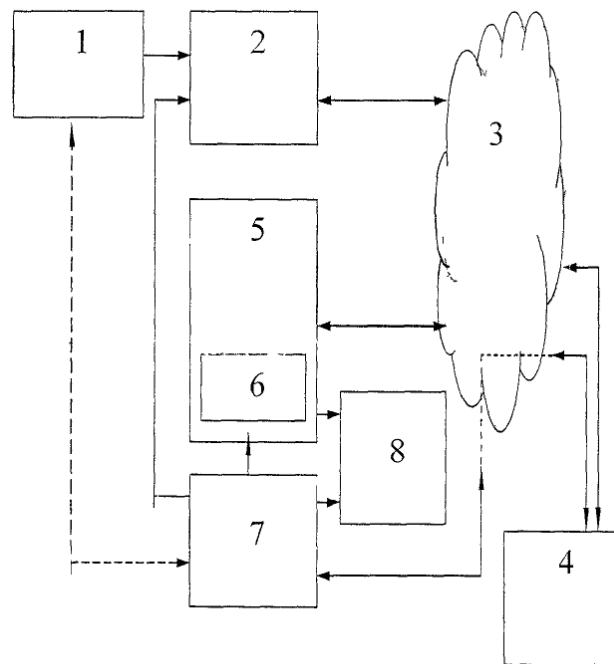
Для екстракції слів, що управляють (CW), в системі можуть використовуватися один або більш офіційні модулі умовного доступу (CAM) провайдера контенту, при цьому вони можуть розміщуватися як в САП так і в сервері-валідаторі.

Запропонована система відрізняється можливістю одночасно використовувати декілька різних провайдерів контенту, що допускається при інсталяції в системі декілька серверов-валідаторов, що належать різним провайдерам контенту.

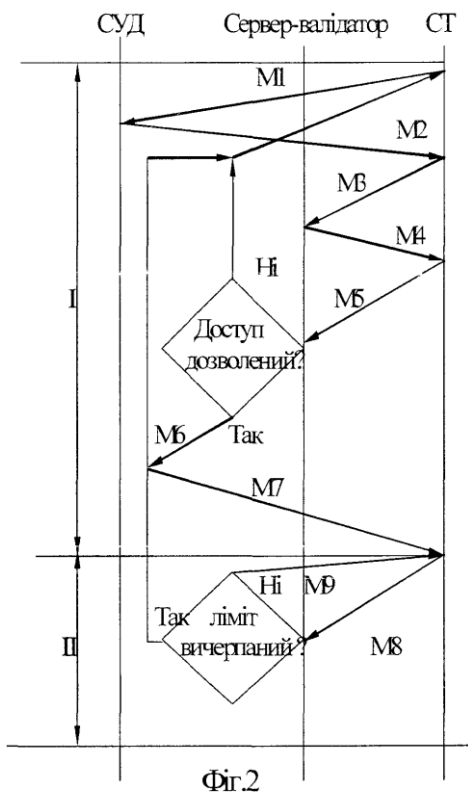
Для забезпечення вимоги до CAS про можливість забезпечення прозорості звітності для провайдера контенту в її складі є модуль білінгу, який може поєднуватися як з сервером-валідатором так і СУД.

Для даних, згідно яких відбувається авторизація СТ, сервер-валідатор містить базу даних що має не менш одного з наступних полів: PIN код, мережева апаратна адреса мережевого терміналу підписчика, лічильник тимчасового ліміту, що залишився, і термін дії для використання PIN коду даного запису. При цьому у складі бази даних як обов'язкове поле використовується запис PIN коду, причому безлічі PIN кодів відповідає безліч карт оплати. У свою чергу карти оплати можуть бути представлені як на матеріальному носіїві з їх записом, захищеним захисним шаром і поширюваних в торгівельній мережі, так і у вигляді записів PIN кодів на серверах електронної комерції. При цьому можливо реалізувати і гнучкість по тарифних планах не досягнути при використанні чіп карт умовного доступу поширених CAS, наприклад можливо організувати перегляд для підписчика після введення певного PIN коду будь-якого каналу з обумовленого для нього пакету програм з сумарним часом перегляду декілька хвилин і терміном придатності умови підписки декілька місяців/років.

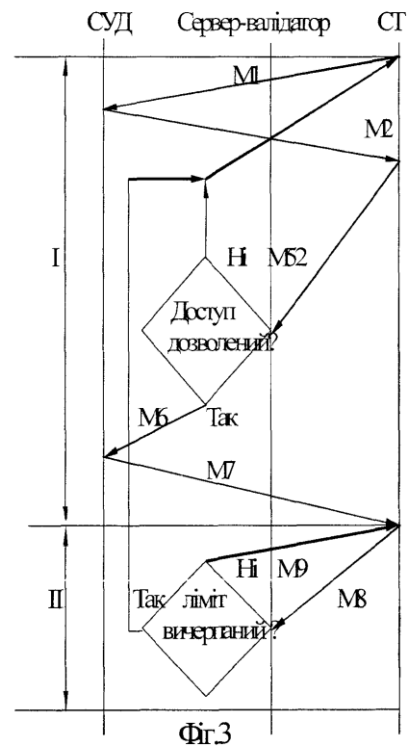
Запропонована система допускає варіанти реалізації, коли сервер-валідатор розташовується на території провайдера контенту, що може дозволити провайдеру контенту повністю контролювати всіх підписників, не побоюючись, маніпуляцій із звітністю сторони операторів комп'ютерної мережі. З іншого боку при довірчих стосунках між оператором УКС і провайдером контенту, можливе об'єднання сервера-валідатора і СУД коли вони можуть мати спільну адресу IP, що може привести деякому спрощенню запропонованої CAS.



Фіг.1



Фіг.2



Фіг.3