



УКРАЇНА

(19) UA (11) 95220 (13) C2
(51) МПК (2011.01)
G06F 21/00
H04L 12/06 (2006.01)

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(54) ГІБРИДНА АРХІТЕКТУРА ОБЛАСТІ ДОЗВОЛЕНОГО ВИКОРИСТАННЯ КОНТЕНТУ, ОРГАНІЗОВАНОЇ НА ОСНОВІ ЯК ПРИСТРОЇВ, ТАК І КОРИСТУВАЧІВ

1

2

(21) a200600528
(22) 14.07.2004
(24) 25.07.2011
(86) PCT/IB2004/051226, 14.07.2004
(31) 03102281.7
(32) 24.07.2003
(33) EP
(46) 25.07.2011, Бюл.№ 14, 2011 р.
(72) КАМПЕРМАН ФРАНЦИСКУС Л.А.Й., NL, КОСТЕР РОБЕРТ Л., NL, ШРЕЙЄН ГЕРТ Й., NL
(73) КОНІНКЛІЙКЕ ФІЛІПС ЕЛЕКТРОНІКС Н.В., NL
(56) US 2003076955; 24.04.2003
WO 03039155 A2; 08.05.2003
US 2002157002 A1; 24.10.2002
WO 03047204 A2; 05.06.2003
HEUVEL VAN DEN S A F A ET AL: "Secure Content Management in Authorised Domains" INTERNATIONAL BROADCASTING CONVENTION, XX, XX, 15 September 2002 (2002-09-15), pages 467-474, XP002273504
(57) 1. Спосіб організації області дозволеного використання контенту (AD), який включає такі операції:
- вибір ідентифікатора області, що унікально ідентифікує дану область дозволеного використання контенту (100);
- визначення щонайменше одного користувача та щонайменше одного пристрою належними до області дозволеного використання контенту, що ідентифікується згаданим ідентифікатором області, шляхом одержання або формування єдиного списку або сертифіката, що містить згаданий ідентифікатор області, унікальний ідентифікатор щонайменше одного користувача і унікальний ідентифікатор щонайменше одного пристрою, із визначенням у такий спосіб належності згаданих пристрою та користувача до даної області дозволеного використання контенту (100); і
- визначення щонайменше однієї одиниці контенту належною до області дозволеного використання контенту, що ідентифікується згаданим ідентифікатором області, шляхом здійснення таких операцій:
а) визначення одиниці контенту відповідною сертифікату прав користувача, який посилається на дану одиницю контенту та користувача, що нале-

жить до даної області дозволеного використання контенту; і/або
б) визначення одиниці контенту відповідною сертифікату прав пристрою, який посилається на дану одиницю контенту та пристрій, що належить до даної області дозволеного використання контенту;
с) визначення одиниці контенту відповідною сертифікату прав області, який посилається на дану одиницю контенту та дану область дозволеного використання контенту;
- з одержанням у такий спосіб певної кількості пристроїв і певної кількості користувачів, що мають повноваження здійснювати доступ до одиниці контенту, що належить до даної області дозволеного використання контенту;
- причому цей спосіб додатково включає контролювання доступу до певної одиниці контенту, що належить до даної області дозволеного використання контенту (100), що здійснюється певним користувачем та із використанням певного пристрою, яке передбачає:
- перевірку того, чи належить даний користувач до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту; або
- перевірку того, чи належить даний пристрій до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту;
- і уможливлення здійснення доступу до даної одиниці контенту даним користувачем із використанням даного і/або іншого пристрою у випадку, якщо даний користувач належить до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту;
- або уможливлення здійснення доступу до даної одиниці контенту даним і/або іншим користувачем із використанням даного пристрою у випадку, якщо даний пристрій належить до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту.
2. Спосіб за п. 1, який **відрізняється** тим, що контролювання доступу до певної одиниці контенту додатково передбачає перевірку того, чи визначає сертифікат прав користувача, який стосується даної одиниці контенту, що даний користувач має

(19) UA (11) 95220 (13) C2

право здійснювати доступ до даної одиниці контенту, і уможливлення доступу до даної одиниці контенту лише у разі позитивного результату перевірки.

3. Спосіб за п. 1 або п. 2, який **відрізняється** тим, що єдиний список або сертифікат містить згаданий ідентифікатор області, унікальний ідентифікатор одного користувача і унікальний ідентифікатор одного пристрою.

4. Спосіб за п. 1, який **відрізняється** тим, що сертифікат прав користувача або сертифікат прав пристрою, або сертифікат прав області включає в себе дані-права, що відображають права, наявні щодо щонайменше однієї одиниці контенту, визначеної відповідною даному сертифікату прав користувача або сертифікату прав пристрою, або даному сертифікату прав області.

5. Спосіб за п. 1, який **відрізняється** тим, що кожну одиницю контенту зашифровують, і кожній одиниці контенту, а також сертифікату прав користувача або сертифікату прав пристрою, або сертифікату прав області ставлять у відповідність право на контент, причому право на контент, що відповідає певній одиниці контенту, включає в себе дешифрувальний ключ для дешифрування даної одиниці контенту.

6. Система для організації області дозволеного використання контенту (AD), яка включає в себе:

- засіб для одержання ідентифікатора області, що унікально ідентифікує дану область дозволеного використання контенту (100);

- засіб для визначення щонайменше одного користувача та щонайменше одного пристрою належними до області дозволеного використання контенту, що ідентифікується згаданим ідентифікатором області, шляхом одержання або формування єдиного списку або сертифіката, що містить згаданий ідентифікатор області, унікальний ідентифікатор щонайменше одного користувача і унікальний ідентифікатор щонайменше одного пристрою, із визначенням у такий спосіб належності згаданих пристрою та користувача до даної області дозволеного використання контенту (100); і

- засіб для визначення щонайменше однієї одиниці контенту належною до області дозволеного використання контенту, що ідентифікується згаданим ідентифікатором області, шляхом здійснення таких операцій:

- а) визначення одиниці контенту відповідною сертифікату прав користувача, який посилається на дану одиницю контенту та користувача, що належить до даної області дозволеного використання контенту; і/або

- б) визначення одиниці контенту відповідною сертифікату прав пристрою, який посилається на дану одиницю контенту та пристрій, що належить до даної області дозволеного використання контенту;

- с) визначення одиниці контенту відповідною сертифікату прав області, який посилається на дану одиницю контенту та дану область дозволеного використання контенту;

- з одержанням у такий спосіб певної кількості пристроїв і певної кількості користувачів, що мають повноваження здійснювати доступ до одиниці кон-

тенту, що належить до даної області дозволеного використання контенту;

- причому ця система додатково включає в себе засіб для контролювання доступу до певної одиниці контенту, що належить до даної області дозволеного використання контенту (100), що здійснюється певним користувачем та із використанням певного пристрою, причому цей засіб виконаний з можливістю здійснювати:

- перевірку того, чи належить даний користувач до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту; або

- перевірку того, чи належить даний пристрій до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту; і

- уможливлення здійснення доступу до даної одиниці контенту даним користувачем із використанням даного і/або іншого пристрою у випадку, якщо даний користувач належить до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту; або

- уможливлення здійснення доступу до даної одиниці контенту даним і/або іншим користувачем із використанням даного пристрою у випадку, якщо даний пристрій належить до тієї самої області дозволеного використання контенту (100), до якої належить дана одиниця контенту.

7. Система за п. 6, яка **відрізняється** тим, що засіб для контролювання доступу до певної одиниці контенту виконаний з можливістю перевірки того, чи визначає сертифікат прав користувача, який стосується даної одиниці контенту, що даний користувач має право здійснювати доступ до даної одиниці контенту, і уможливлення доступу до даної одиниці контенту лише у разі позитивного результату перевірки.

8. Система за п. 6, яка **відрізняється** тим, що єдиний список або сертифікат містить згаданий ідентифікатор області, унікальний ідентифікатор одного користувача і унікальний ідентифікатор одного пристрою.

9. Система за п. 6, яка **відрізняється** тим, що сертифікат прав користувача або сертифікат прав пристрою, або сертифікат прав області включає в себе дані-права, що відображають права, наявні щодо щонайменше однієї одиниці контенту, визначеної відповідною даному сертифікату прав користувача, або даному сертифікату прав пристрою, або даному сертифікату прав області.

10. Система за п. 6, яка **відрізняється** тим, що кожна одиниця контенту зашифрована, і кожній одиниці контенту, а також сертифікату прав користувача або сертифікату прав пристрою, або сертифікату прав області поставлене у відповідність право на контент, причому право на контент, що відповідає певній одиниці контенту, включає в себе дешифрувальний ключ для дешифрування даної одиниці контенту.

11. Машиночитаний носій, на якому збережені команди, що зумовлюють виконання одним або декількома процесорами способу за одним із пп. 1-5.

Винахід стосується способу організації області дозволеного використання контенту. Винахід також стосується системи, призначеної для організації області дозволеного використання контенту. Крім того, винахід стосується машиночитного носія із збереженими на ньому командами, що зумовлюють виконання одним або декількома процесорами способу, запропонованого даним винаходом.

Як наслідок розвитку технологій передавання контенту (зокрема, змінні носії інформації та Інтернет-технології), обмін контентом став простим як ніколи. Швидке прийняття нових технологій споживачами свідчить про те, що такі технології дійсно відповідають їхнім потребам. Побічним ефектом є те, що такі технології також спрощують незаконне копіювання і розповсюдження контенту. Бізнесові кола, в основі бізнесу яких є інформаційні ресурси, убачають у ситуації, що створилася, загрозу своєму бізнесу. Відповідно, в останні роки швидкими темпами зростає кількість систем захисту контенту. Деякі з цих систем лише захищають контент від незаконного копіювання, тоді як інші ще й контролюють доступ користувача до контенту. Системи першої категорії називають системами захисту від копіювання (або CP-системи). Традиційно для індустрії користувацької електроніки (так звана CE-індустрія) основні зусилля були сконцентровані на системах захисту від копіювання, оскільки вважається, що цей тип захисту контенту може бути реалізований із невеликими витратами, і він не вимагає двосторонньої взаємодії з провайдером контенту. До прикладів таких систем належать система CSS, призначена для захисту дисків DVD-ROM, та система DTCP, призначена для захисту з'єднань за стандартом IEEE 1394.

Системи захисту контенту другого типу мають різні назви. У системах мовлення вони відомі під загальним терміном "системи умовного доступу" (так звані CA-системи), тоді як в Інтернет-індустрії вони відомі під загальним терміном "системи цифрового керування правами" (так звані DRM-системи).

Домашня мережа може бути визначена як група пристроїв, з'єднаних між собою за допомогою певної мережевої технології (наприклад, Ethernet, IEEE 1394, Bluetooth, 802.11b, 802.11g тощо). Хоч мережеві технології уможливають обмін даними між різними пристроями, їх ще недостатньо для того, щоб уможливити спільну роботу відповідних пристроїв. Для уможливлення цього необхідно, щоб пристрої могли виявляти функціональні можливості, наявні в інших пристроїв у даній мережі, і звертатися до цих функціональних можливостей. Такі можливості спільної роботи (що відомо фахівцям у даній галузі як "interoperability") забезпечуються сполучним програмним забезпеченням (так зване "middleware") домашніх мереж. Прикладами такого сполучного програмного забезпечення є Jini, HAVi, UPnP, AVC.

Концепція областей дозволеного використання контенту (поняття "область дозволеного використання контенту" також відоме фахівцям як "Authorized Domain", AD) - це спроба знайти рі-

шення, що відповідало б інтересам як власників контенту (що бажають захистити належні їм авторські права), так і споживачів контенту (що бажають використовувати контент без обмежень). Її суть полягає в тому, щоб утворити кероване мережеве середовище, в якому контент можна використовувати відносно вільно, але лише в межах області його дозволеного використання. Як правило, області дозволеного використання контенту утворюються в домашньому середовищі, що також іменується домашньою мережею. Зрозуміло, можливі й інші варіанти. Наприклад, користувач міг би взяти з собою у подорож переносний пристрій для відтворення аудіо- і/або відео з певною обмеженою кількістю контенту і використати його в готельному номері для здійснення доступу до додаткового контенту (або його завантаження), що зберігається на його особистій аудіо- і/або відео-системі вдома. Хоча переносний пристрій і знаходиться за межами домашньої мережі користувача, він є частиною його області дозволеного використання контенту. Таким чином, область дозволеного використання контенту (AD) являє собою систему, що уможливорює доступ до контенту пристроям, що належать до цієї області, але не дозволяє використовувати контент ніяким іншим пристроям.

Детальніше використання областей дозволеного використання контенту описано у S.A.F.A. van den Heuvel, W. Jonker, F.L.A.J. Kamperman, P.J. Lenoir, Secure Content Management in Authorised Domains, Philips Research, Нідерланди, матеріали конференції IBC 2000, стор. 467-474, що проводилася 12-16 вересня 2002 р.

Було запропоновано декілька рішень, що до певної міри реалізують концепцію області дозволеного використання контенту.

Відомі рішення одного типу пропонують області дозволеного використання контенту (AD), організовані на основі пристроїв. Прикладами таких систем є SmartRight (Thomson Multimedia), xCP і NetDRM (Matsushita). Ще один приклад області дозволеного використання контенту (AD), організованої на основі пристроїв, розкритий у нашій європейській патентній заявці № 02076998.0 (PHNL020455).

У типових областях дозволеного використання контенту (AD), організованих на основі пристроїв, область утворюється певним конкретним набором пристроїв і контентом. Тільки цьому конкретному набору пристроїв дозволені здійснення доступу, використання тощо контенту даної області. Ніякого розрізнення користувачів цього набору пристроїв або розмежування між ними не передбачається.

Недоліком таких систем, де області дозволеного використання контенту (AD) організовані на основі пристроїв, є те, що вони, як правило, не забезпечують того рівня гнучкості, який бажав би мати або потребував би користувач, оскільки користувач вимушений використовувати лише конкретний обмежений набір пристроїв. Відповідно, користувач не може скористатися придбаними ним правами в будь-який вибраний ним час і в будь-

якому вибраному ним місці. Наприклад, в гостях у товариша користувач не зможе здійснити доступ до контенту, чесно купленого цим користувачем, використовуючи пристрої цього товариша, оскільки ці пристрої, як правило, не входять у визначений і обмежений набір пристроїв області, до якої належить контент користувача.

Відомі рішення іншого типу розкривають області дозволеного використання контенту, організовані на основі користувачів, тобто область будується не на основі пристроїв, як це мало місце в областях дозволеного використання контенту (AD), організованих на основі пристроїв, а на основі людей. Прикладом такої системи є, наприклад, система, описана в нашій європейській патентній заявці № 02079390.7 (PHNL021063), в якій контент закріплюється за користувачами, яких потім об'єднують у групу для створення області дозволеного використання контенту.

У типовій області дозволеного використання контенту (AD), організованій на основі користувачів, здійснення доступу до контенту, що належить до даної області (AD), дозволене лише певному і обмеженому колу користувачів, які при цьому можуть використовувати будь-який сумісний пристрій. Як правило, області дозволеного використання контенту, організовані на основі користувачів, легше адмініструвати, порівняно з областями дозволеного використання контенту, організованими на основі пристроїв.

Однак організовані на основі користувачів системи вимагають ідентифікації особи користувача, що може виявитись незручним або небажаним для користувачів. Крім того, гість, що завітав до вашого дому, може захотіти здійснити доступ до вашого контенту. Але якщо у нього не буде пристрою для ідентифікації особи в цій області дозволеного використання контенту, він не зможе здійснити доступ до цього контенту. Було б добре, якби домашні пристрої, що належать до відповідної області дозволеного використання контенту, уможливили б здійснення гостем доступу до контенту даної області.

Відповідно, існує необхідність в області дозволеного використання контенту, що поєднує в собі переваги як систем, організованих на основі користувачів, так і систем, організованих на основі пристроїв.

Мета винаходу полягає у наданні способу і відповідної системи для побудови області дозволеного використання контенту, організованої на основі як пристроїв, так і користувачів. Ще одна мета полягає в наданні способу і системи, в яких би усувалися згадані вище недоліки попереднього рівня техніки. Ще одна мета полягає в тому, щоб зробити це просто, гнучко і ефективно.

Ці цілі, як і деякі інші, досягаються у способі (і відповідній системі) організації області дозволеного використання контенту (AD), що включає операції вибору ідентифікатора області, що унікально ідентифікує дану область дозволеного використання контенту, визначення щонайменше одного користувача відповідним згаданому ідентифікатору області і визначення щонайменше одного пристрою відповідним згаданому ідентифікатору об-

ласті, з одержанням у такий спосіб певної кількості пристроїв і певної кількості осіб, що мають повноваження здійснювати доступ до одиниці контенту, що належить до даної області дозволеного використання контенту.

Завдяки цьому забезпечується просте і ефективне об'єднання пристроїв і користувачів у область дозволеного використання контенту (AD). Крім того, утворюється гібридна область дозволеного використання контенту, яка організована як на основі пристроїв, так і на основі користувачів. Відповідно, здійснення доступу до одиниці контенту даної області дозволеного використання контенту дозволяється або за результатами перевірки належності до однієї і тієї самої області одиниці контенту і користувача, або за результатами перевірки належності до однієї і тієї самої області одиниці контенту і пристрою, що використовується користувачем. Завдяки цьому здійснення доступу до контенту даної області дозволеного використання контенту одним або декількома користувачами стає більш гнучким, із збереженням при цьому захищеності контенту. До того ж такий спосіб є простим, надійним і таким, що забезпечує ефективний захист контенту.

В одному варіанті здійснення способу додатково включає операцію визначення щонайменше однієї одиниці контенту належною до області дозволеного використання контенту, що ідентифікується згаданим ідентифікатором області.

В одному варіанті здійснення операція визначення щонайменше одного користувача відповідним згаданому ідентифікатору області передбачає одержання або формування списку користувачів області, що містить згаданий ідентифікатор області і унікальний ідентифікатор кожного користувача, із визначенням у такий спосіб належності користувача до даної області дозволеного використання контенту, і/або операція визначення щонайменше одного пристрою відповідним згаданому ідентифікатору області передбачає одержання або формування списку пристроїв області, що містить згаданий ідентифікатор області і унікальний ідентифікатор кожного пристрою, із визначенням у такий спосіб належності пристрою до даної області дозволеного використання контенту.

В одному варіанті здійснення операція визначення щонайменше однієї одиниці контенту належною до області дозволеного використання контенту передбачає:

- визначення одиниці контенту відповідною праву користувача, що відповідає користувачу, який належить до області дозволеного використання контенту, і/або
- визначення одиниці контенту відповідною праву пристрою, що відповідає пристрою, який належить до області дозволеного використання контенту.

В одному варіанті здійснення операція визначення щонайменше однієї одиниці контенту належною до області дозволеного використання контенту передбачає визначення одиниці контенту відповідною праву області, що відповідає області дозволеного використання контенту.

В одному варіанті здійснення право користувача, або право пристрою, або право області включає в себе дані-права, що відображають права, наявні щодо щонайменше однієї одиниці контенту, визначеної відповідною даному праву користувача, або даному праву пристрою, або даному праву області.

В одному варіанті здійснення спосіб додатково включає контролювання доступу до певної одиниці контенту, що належить до даної області дозволеного використання контенту, що здійснюється певним користувачем та із використанням певного пристрою, яке передбачає:

- перевірку того, чи належить даний користувач до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту, або

- перевірку того, чи належить даний пристрій до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту,

- і уможливлення здійснення доступу до даної одиниці контенту даним користувачем із використанням даного і/або іншого пристрою у випадку, якщо даний користувач належить до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту,

- або уможливлення здійснення доступу до даної одиниці контенту даним і/або іншим користувачем із використанням даного пристрою у випадку, якщо даний пристрій належить до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту.

В одному варіанті здійснення спосіб додатково включає контролювання доступу до певної одиниці контенту, що належить до даної області дозволеного використання контенту і має унікальний ідентифікатор контенту, що здійснюється певним користувачем та із використанням певного пристрою, яке передбачає:

- перевірку того, чи містить список пристроїв даної області дозволеного використання контенту ідентифікатор даного пристрою, з перевіркою у такий спосіб, чи належить даний пристрій до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту, і/або

- перевірку того, чи містить список користувачів даної області дозволеного використання контенту ідентифікатор даного користувача, з перевіркою у такий спосіб, чи належить даний користувач до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту,

- і уможливлення здійснення доступу до даної одиниці контенту будь-яким користувачем із використанням даного пристрою у випадку, якщо даний пристрій належить до тієї самої області дозволеного використання контенту, до якої належить дана одиниця контенту, до якої здійснюється доступ, і/або

- уможливлення здійснення доступу до даної одиниці контенту даним користувачем із використанням будь-якого (включно з даним) пристрою у випадку, якщо даний користувач належить до тієї самої області дозволеного використання контенту,

до якої належить дана одиниця контенту, до якої здійснюється доступ.

В одному варіанті здійснення контролювання доступу до певної одиниці контенту додатково передбачає перевірку того, чи визначає право користувача, яке стосується даної одиниці контенту, що даний користувач має право здійснювати доступ до даної одиниці контенту, і уможливлення доступу до даної одиниці контенту лише у разі позитивного результату перевірки.

В одному варіанті здійснення кожну одиницю контенту зашифровують, і кожній одиниці контенту, а також праву користувача, або праву пристрою, або праву області ставлять у відповідність право на контент, причому право на контент, що відповідає певній одиниці контенту, включає в себе дешифрувальний ключ для дешифрування даної одиниці контенту.

В одному варіанті здійснення

- список користувачів області реалізований як сертифікат користувачів області або міститься у ньому, і/або

- список пристроїв області реалізований як сертифікат пристроїв області або міститься у ньому, і/або

- право користувача реалізоване як сертифікат прав користувача або міститься у ньому, і/або

- право пристрою реалізоване як сертифікат прав пристрою або міститься у ньому, і/або

- право області реалізоване як сертифікат прав області або міститься у ньому.

Запропоновані цим винаходом варіанти здійснення системи, яким віддають перевагу, визначені у формулі винаходу. Варіанти здійснення системи відповідають варіантам здійснення способу і мають ті самі переваги з тих самих причин.

Крім того, винахід також стосується машиночитного носія із збереженими на ньому командами, що зумовлюють виконання одним або декількома процесорами способу, запропонованого даним винаходом.

Ці та інші аспекти винаходу стануть очевидними при ознайомленні з приведеними як приклади варіантами здійснення, що його ілюструють, з посиланнями на креслення, на яких:

Фіг. 1 - схема, що ілюструє об'єднання осіб, пристроїв, прав користувачів і контенту в одну область дозволеного використання контенту (AD) згідно з цим винаходом;

Фіг. 2 - схема, що ілюструє об'єднання осіб, пристроїв, прав користувачів і контенту в одну область дозволеного використання контенту (AD) згідно з альтернативним варіантом здійснення даного винаходу;

Фіг. 3 - схема, що ілюструє елементи сертифіката пристроїв області (DDC) і сертифіката користувачів області (DUC);

Фіг. 4a - приклад структури даних (фрагмент), що включає контейнер контенту, право на контент (CR) і сертифікат прав користувача (URC) відповідно до варіанта здійснення даного винаходу, показаного на фіг. 1;

Фіг. 4b - приклад структури даних (фрагмента), що включає контейнер контенту, право на контент (CR) і сертифікат прав області (DRC) відповідно до

варіанта здійснення цього винаходу, показаного на фіг. 2;

Фіг. 5 - схема, що ілюструє приклад системи, що об'єднує в собі пристрої і користувачів, які утворюють область дозволеного використання контенту (AD).

На всіх фігурах одними і тими самими номерами позицій позначені аналогічні або ідентичні елементи. Деякі з показаних на фігурах елементів звичайно реалізуються програмно, і як такі являють собою програмні сутності, наприклад, програмні модулі або об'єкти.

На фіг. 1 схематично представлено об'єднання осіб, пристроїв, прав користувачів і контенту в одну область дозволеного використання контенту (AD) відповідно до цього винаходу. Показана область дозволеного використання контенту (100), що пропонується цим винаходом; декілька пристроїв D1, D2, D3,..., DM (де M дорівнює або більше за 1), декілька одиниць контенту C1, C2, C3,..., CN₂ (де N₂ дорівнює або більше за 1) і декілька осіб-користувачів P1, P2, P3,..., PN₁ (де N₁ дорівнює або більше за 1) належать до області дозволеного використання контенту (AD) відповідно до одного варіанта здійснення цього винаходу. Належність цих пристроїв, осіб і одиниць контенту до даної області (100) визначена у спосіб, пояснений нижче. Також показані права користувачів (URC1, URCN₂), причому одній одиниці контенту за варіантом, якому віддають перевагу, ставиться у відповідність один сертифікат прав користувача, який визначає, які права відповідна особа (або, в альтернативному варіанті, відповідна група осіб і/або всі особи, закріплені за областю (100)) має щодо даної одиниці контенту (або, в альтернативному варіанті, декількох або всіх одиниць контенту області (100)).

Більш докладну інформацію про архітектуру області дозволеного використання контенту і способи її організації читач може одержати з наших європейських патентних заявок № 01204668.6 (PHNL010880) та № 02076998.0 (PHNL020455). У європейській патентній заявці № 02076998.0 (PHNL020455) докладніше розкрито варіант реалізації, в якому відповідними області дозволеного використання контенту визначають контент і пристрої. Крім того, в нашій європейській патентній заявці № 02079390.7 (PHNL021063) розкрито варіант реалізації, в якому визначають відношення між контентом і особами, і цих осіб потім групують в область дозволеного використання контенту.

Слід зазначити, що на практиці доступ до контенту і/або його використання можуть бути здійснені лише шляхом застосування користувачем певного пристрою. У подальшому тексті ми виходимо з припущення, що використовувані в системі пристрої є "сумісними" і "відкритими". Це означає, що пристрої функціонують із дотриманням певних правил роботи (наприклад, не виводять незаконно контент на незахищений цифровий інтерфейс) і право власності на пристрій не має значення (що означає "відкритість»). Будемо також виходити з припущення, що питання впорядкування сумісності пристроїв (тобто ідентифікація сумісних пристроїв, продовження повноважень пристроїв і скасування

повноважень пристроїв) вирішені (відомими з рівня техніки способами); відповідно, детально розглядати ці питання в цьому тексті не будуть.

Право користувача (URC1,..., URCN₂) являє собою один зв'язок, закріплення, відношення, одну прив'язку, відповідність тощо між одним користувачем і правом на контент (необхідним для дешифрування одиниці контенту). Ввівши право користувача, ми одержуємо в нашій системі п'ять основних компонентів; це все працює у такий спосіб:

- контент (C1, C2, C3,..., CN₂): одиниці контенту за варіантом, якому віддають перевагу, зашифровані (можливі різні варіанти - наприклад, за допомогою ключа, унікального для кожного найменування контенту) і можуть знаходитися в будь-якому місці системи; в даному варіанті здійснення визначається непряма відповідність (відношення) між одиницею контенту і сертифікатом прав користувача, через право на контент, як пояснюється з посиланням на фіг. 4а;

- право на контент (CR; на фіг. 1 не показано - див. фіг. 4а): містить криптографічний ключ (ключі) або інші відповідні засоби захисту для здійснення доступу до певної (зашифрованої/захищеної) одиниці контенту. Система демонструє гнучкість у тому, що права на контент можуть бути унікальними для кожного найменування контенту або навіть для кожного примірника (копії) контенту. Права на контент повинні надаватися тільки сумісним пристроям. У жорсткішому варіанті права на контент надаються тільки сумісним пристроям, які використовуються повноважними користувачами (тобто користувачами, що мають повноваження на певне право на контент, які впливають з їхніх прав користувача). Права на контент можна було б також зберігати разом із самим контентом, наприклад, на оптичному диску. Однак права на контент необхідно зберігати захищеними, оскільки вони містять ключ для дешифрування контенту;

- сертифікат прав користувача (URC1,..., URCN₂): сертифікат або щось подібне, виданий провайдером контенту; сертифікат надає певній особі повноваження використовувати певне право на контент (CR) (що відповідає певній одиниці контенту). У принципі, права користувача можуть знаходитися в будь-якому місці системи. За варіантом, якому віддають перевагу, сертифікат прав користувача містить також правила доступу до відповідної одиниці контенту (наприклад, обмеження кола глядачів особами у віці 18 років і старше, або лише європейським ринком тощо);

- пристрій (D1, D2, D3,..., DM): пристрій, що використовується для відтворення, обробки, записування, представлення, відображення, зміни тощо одиниці контенту. Додатково пристрій (сумісний) може також (за варіантом, якому віддають перевагу) ідентифікувати користувача за допомогою особистого ідентифікувального пристрою (наприклад, смарт-карти, мобільного телефону, біометричного датчика тощо) і збирати сертифікати (наприклад, зі смарт-карти, або з інших пристроїв), що підтверджують, що користувач має повноваження використовувати певне право на контент. Це право на контент можна було б одержувати зі

смарт-карти, де воно було збережене (якщо воно було там збережене), або (за умови захищеного передавання) з іншого сумісного пристрою через мережу;

- користувач-особа (P1, P2, P3,..., PN₁): користувач ідентифікується певним біометричним або - за варіантом, якому віддають перевагу - особистим ідентифікувальним пристроєм (наприклад, смарт-картою, мобільним телефоном, мобільним телефоном зі смарт-картою, або пристроями іншого типу, що унікально ідентифікують користувача), який він носить на собі, з собою або до якого має доступ. Перевагу віддають мобільному телефону зі смарт-картою або іншому пристрою, спорядженому засобом для зберігання даних, оскільки у цьому випадку користувач може носити права з собою (для доступу до контенту на пристроях, не підключених до мережі). Ідентифікувальний пристрій може бути захищений засобами біометричної ідентифікації, щоб ніхто крім законного власника не міг скористатися цим ідентифікувальним пристроєм. Користувач може також ідентифікуватися за допомогою криптографічної технології із відкритим ключем, або протоколів із "нульовим знанням" (відомі як "zero-knowledge protocol"), або їх поєднання.

За варіантом, якому віддають перевагу, повноважні пристрої визначаються належними до області дозволеного використання контенту (AD) (100) за допомогою сертифікатів. Аналогічно, повноважні особи/користувачі за варіантом, якому віддають перевагу, також визначаються належними до області дозволеного використання контенту (AD) (100) за допомогою сертифікатів. У цьому конкретному варіанті здійснення відповідності між одиницями контенту і користувачем за допомогою сертифіката прав користувача (URC). Цей сертифікат прав користувача дозволяє використання відповідного права на контент (CR), яке, за варіантом, якому віддають перевагу, включає в себе криптографічний ключ для здійснення доступу до контенту, як буде більш детально пояснено з посиланнями на фіг. 4а. Сертифікат прав користувача (URC), як правило, ставиться у відповідність до однієї одиниці контенту, але може ставиться у відповідність і декільком одиницям контенту. Приклад фрагмента структури даних з контейнером контенту (містить одиницю контенту), URC і CR показаний і більш детально пояснюється з посиланнями на фіг. 4а.

Сертифікати області за варіантом, якому віддають перевагу, видаються адміністратором області. В альтернативному варіанті адміністрування цих сертифікатів можуть здійснювати сумісні пристрої, що мають відповідні функціональні можливості.

У показаному на фіг. 1 прикладі кожній одиниці контенту C1, C2,..., CN₂ відповідає сертифікат прав користувача URC1, URC2,..., URCN₂. URC1 і URC2 відповідають особі P1, URC3 відповідає особі P2, URCN₂₋₂, URCN₂₋₁ і URCN₂ відповідають особі PN₁ а URC4-URCN₂₋₃ розподілені між особами P3-PN₁₋₁.

У такий спосіб конкретний контент C1 і C2 визначений відповідним ("закріплений") конкретній

особі P1, конкретний контент C3 визначений відповідним конкретній особі P2, конкретний контент CN₂₋₂, CN₂₋₁ і CN₂ визначений відповідним конкретній особі PN₁, конкретний контент C4-CN₂₋₃ розподілений між конкретними особами P3-PN₁₋₁ за допомогою відповідних URC.

У цьому варіанті здійснення однієї одиниці контенту може відповідати лише один URC (непрямо, через право на контент) і, відповідно, лише одна особа. Якщо декільком користувачам знадобиться копія тієї ж самої одиниці контенту, то відповідно до цього варіанту здійснення вона буде представлена в окремому екземплярі для кожного користувача і кожний такий екземпляр вважатиметься іншою одиницею контенту; адміністрування прав у цьому випадку полегшується. В альтернативному варіанті, залежно від конкретних робочих умов, одна одиниця контенту може ставитись у відповідність більш ніж одній особі, оскільки можна встановити зв'язок між CR та декількома URC.

Особи P1, P2, P3,..., PN₁ і пристрої D1, D2, D3,..., DM потім об'єднують у групу, утворюючи область дозволеного використання контенту (100).

Перевагу віддають здійсненню об'єднання - тобто групуванню і закріпленню - пристроїв, осіб і контенту із використанням сертифікатів. За варіантом, якому віддають перевагу, застосовуються сертифікат (або список) пристроїв даної області (DDC), сертифікат (або список) користувачів даної області (DUC) і сертифікат (або список) прав користувача (URC). У подальшому описі будуть згадуватися тільки сертифікати, хоч потрібно розуміти, що такі структури можуть, наприклад, реалізовуватися як списки і т.п.

У DDC наводиться перелік пристроїв, що належать до області (100), наприклад, із вказуванням у ньому для кожного пристрою унікального ідентифікатора. У DUC наводиться перелік користувачів, що належать до області (100), наприклад, із вказуванням унікального ідентифікатора, або криптографічного ключа (наприклад, відкритого), або його хеш-коду для кожного користувача. DUC і DDC показані на фіг. 3, і більш детально пояснюються нижче. За варіантом, якому віддають перевагу, сертифікат URC запроваджується для кожної одиниці контенту (так, в прикладі варіанта здійснення, показаному на фіг. 1, кількість таких URC становить N₂); в URC вказано, які права є (і/або яких немає) у користувача (за яким цей URC закріплений) в області (100) і, факультативно, в суміжній області (права X-AD), щодо тієї одиниці контенту, що відповідає даному URC. Як альтернатива, URC може ставитись у відповідність певному користувачу; тоді в ньому, наприклад, вказується кожна одиниця контенту, закріплена за даним користувачем, а також права, які даний користувач має щодо кожної такої одиниці контенту. Як альтернатива, для визначення прав кожного користувача застосовується лише один URC; тобто, у таких URC вказується, яка/які одиниця/одиниці контенту закріплені за кожним користувачем, і які права цей користувач має (і/або не має).

У варіанті здійснення, якому віддають перевагу, DDC і DUC взаємопов'язані за допомогою ідентифікатора області (Domain_ID), що включається в

кожний з цих сертифікатів. Завдяки цьому втілюється дуже простий спосіб встановлення зв'язку між користувачами (і, отже, одиницями контенту) і пристроями певної області (і тим самим - організація такої області).

Якщо певний пристрій (наприклад, пристрій D3) захоче одержати доступ до певної одиниці контенту (наприклад, контенту C1), необхідно буде пересвідчитись, перевірити тощо (із застосуванням сертифікатів), що дана одиниця контенту закріплена за певною особою (наприклад, особою P1), що належить до тієї самої області (100), що і даний пристрій. Це можна, наприклад, зробити, перевіривши, що:

- (унікальний) ідентифікатор даного конкретно-го пристрою (наприклад, пристрою D3) міститься у DDC,

- (унікальний) ідентифікатор даної конкретної особи (наприклад, особи P1) міститься у DUC,

- і DDC, і DUC містять один і той самий ідентифікатор області (наприклад, Domain_ID - 4- або 8-байтове число (наприклад, одержане за допомогою генератора випадкових чисел); не показано), і

- URC для даної конкретної особи (наприклад, URC1) визначає, що ця особа має право доступу до даного контенту (наприклад, якщо не закінчився термін дії дозволу на його використання, або контент був використаний не більше разів, ніж дозволено, наприклад, не більше трьох разів).

Це буде проілюстроване більш детально з посиланнями на фіг. 4а. Як альтернатива, замість того, щоб бути випадковим числом, ідентифікатор області (Domain_ID) може бути посиланням на певний об'єкт даних, наприклад, сертифікат області.

Шляхом встановлення зв'язків між одиницями контенту та особами (за допомогою URC) можна легко відображати, кому належить контент. Крім того, легше адмініструвати розділення області дозволеного використання контенту (AD), оскільки при розділенні осіб розділяються і відповідні одиниці контенту, оскільки одиниці контенту закріплені за цими особами.

Отже, один або декілька пристроїв, одна або декілька осіб і щонайменше одна одиниця контенту (для кожної особи) об'єднують в область дозволеного використання контенту, за варіантом, якому віддають перевагу, із застосуванням сертифікатів або, як альтернатива, із застосуванням списків, що містять такі самі елементи, які були описані для сертифікатів. Цілком можливо, що в певні моменти часу в певній області будуть відсутні особи, і/або пристрої, і/або одиниці контенту. Наприклад, у самому початку, при організації області, в ній може не бути одиниць контенту або пристроїв, належних до цієї області тощо.

Таким чином користувач, щодо якого встановлена його належність до тієї самої області, до якої належить одиниця контенту, до якої прагнуть здійснити доступ, може одержувати доступ до цього контенту із застосуванням будь-якого пристрою. Крім того, користувач, що застосовує пристрій, щодо якого встановлена його належність до тієї самої області, до якої належить одиниця контенту, до якої прагнуть здійснити доступ, може одержу-

вати доступ до цього контенту, застосовуючи даний пристрій. Більш того, всі користувачі можуть одержувати доступ до цієї одиниці контенту через даний пристрій.

Завдяки цьому забезпечується більша гнучкість при здійсненні доступу одного або декількох користувачів до контенту в області дозволеного використання контенту (AD), але із збереженням захищеності контенту.

Відповідно до альтернативного варіанту здійснення контент може "закріплюватися" за пристроями, що належать до області AD, а не за особами, що належать до неї. Замість сертифіката прав користувача застосовується сертифікат прав пристрою (DevRC) (не показаний). У цьому випадку зміст сертифіката прав пристрою (DevRC) був би таким самим, як зміст URC, тільки замість ідентифікатора особи (Person ID) в ньому був би ідентифікатор пристрою (Device ID); більше нічого б не змінилося.

Фахівцю буде ясно, що замість одного списку або сертифіката, що містить користувачів (тобто DUC), і одного списку або сертифіката, що містить пристрої (тобто DDC), і у вищезазначених випадках, і у випадках, що розглядаються нижче, можна застосувати й інші схеми. Як альтернатива, і пристрої, і користувачі можуть бути включені до одного списку/сертифіката. Також рівною мірою можна застосувати декілька списків/сертифікатів, що містять пристрої, і/або декілька списків/сертифікатів, що містять користувачів, і у будь-яких сполученнях.

На фіг. 2 схематично представлено об'єднання осіб, пристроїв, прав користувачів і контенту в область дозволеного використання контенту (AD) відповідно до альтернативного варіанта здійснення даного винаходу. Цей варіант здійснення відповідає варіанту, показаному на фіг. 1, але лише з тією відмінністю, що замість "закріплення" одиниць контенту C1, C2, ..., CN₂ за особами P1, P2, ..., PN₁ за допомогою сертифікатів прав користувача URC1, URC1, ..., URCN₂, одиниці контенту визначаються належними до області (100) за допомогою одного або декількох прав області (DRC). За варіантом, якому віддають перевагу, одній одиниці контенту ставлять у відповідність одне DRC. У варіанті здійснення, якому віддають перевагу, DRC реалізоване як сертифікат.

Якщо в даному варіанті здійснення певний пристрій (наприклад, пристрій D3) захоче здійснити доступ до певної одиниці контенту (наприклад, контенту C1), необхідно буде встановити, перевірити тощо (застосовуючи сертифікати), чи дана одиниця контенту належить до тієї самої області (100), що і даний пристрій, і що особа (наприклад, особа P1), що використовує даний пристрій, належить до цієї самої області. У даному варіанті здійснення це може бути виконане, наприклад, за допомогою перевірки того, чи включений (унікальний) ідентифікатор даного пристрою в DDC, або чи включений (унікальний) ідентифікатор цієї особи в DUC. Крім того, треба перевірити, чи DRC, поставлений у відповідність до даної одиниці контенту, належить до цієї самої області, і чи такий самий ідентифікатор області в DDC або DUC, і чи

визначає DRC для даного контенту, що особа, що належить до цієї області, має право доступу до даної одиниці контенту (наприклад, якщо не закінчився термін дії дозволу на його використання, або контент був використаний не більше разів, ніж дозволено, наприклад, не більше трьох разів). Відповідно, доступ до одиниці контенту здійснюється або через сумісний пристрій, що належить до даної області, або через дійсний ідентифікатор особи. Детальніше це пояснюється з посиланням на фіг. 4b.

На фіг. 3 схематично представлені сертифікат пристроїв області (DDC) і сертифікат користувачів області (DUC). Як можна бачити, сертифікат пристроїв області (DDC) містить перелік унікальних ідентифікаторів (Dev.ID1, Dev.ID2, ...) одного або декількох пристроїв, що належать до даної області, тобто пристроїв, що мають повноваження на здійснення доступу до контенту в даній області. У варіанті здійснення, якому віддають перевагу, ідентифікатор пристрою, наприклад, Dev.ID1, являє собою серійний номер, ідентифікаційний номер і т.ін., тобто номер, який не може бути змінений принаймні користувачем. Дана область AD ідентифікується значенням ідентифікатора області (Domain ID), що може бути, наприклад, 8-байтовим випадковим числом.

Сертифікати, що використовуються у даному винаході (DDC, DUC тощо), можуть, наприклад, являти собою відомі фахівцям сертифікати SPKI (прості інфраструктури відкритих ключів). Крім того, корисно було б вмістити Domain_ID у поле holder такого сертифіката SPKI, що служить як DDC, DUC і/або DRC.

Сертифікат користувачів області (DUC) містить перелік унікальних ідентифікаторів (Pers_ID1, Pers_ID2, ...) одного або декількох користувачів/осіб, що належать до даної області, тобто є користувачами, що мають повноваження на здійснення доступу до контенту в даній області. Дана область, в якій переліченим користувачам дозволено здійснювати доступ, ідентифікується значенням ідентифікатора Domain_ID, подібно до того, як описано вище для сертифіката пристроїв області (DDC). Сертифікат користувачів області (DUC) і сертифікат пристроїв області (DDC) зв'язані один з одним, оскільки містять однакові ідентифікатори Domain_ID; у такий спосіб визначається область дозволеного використання контенту (до якої належать і пристрої, і користувачі).

На фіг. 4a показаний приклад (фрагмент) структури даних з контейнером контенту, правом на контент (CR) і сертифікатом прав користувача (URC) відповідно до варіанта здійснення цього винаходу, показаного на фіг. 1. Контейнер (501) контенту містить захищені дані/контент, наприклад, одержаний від провайдера послуг. Контейнер контенту містить також ідентифікатор контенту Cont_ID, унікальний для цієї одиниці контенту. Відповідно, ідентифікатор контенту Cont_ID використовується для знаходження одиниці контенту у відповідній області, наприклад, шляхом перевірки кожного контейнера контенту, що належить до даної області, до виявлення потрібного Cont_ID.

Право на контент (CR) (502) містить ідентифікатор контенту Cont_ID і ключ шифрування контенту ContEncrK. Ідентифікатор контенту використовується для визначення зв'язку із зашифрованою одиницею контенту (що міститься у контейнері контенту), для якої призначається ключ шифрування контенту, тобто контенту, для розшифровки якого і, тим самим, для уможливлення доступу до якого цей ключ необхідний. У цьому варіанті здійснення ключ шифрування є симетричним ключем, тобто один і той самий ключ застосовується і для шифрування, і для дешифрування даних. Як альтернатива можуть використовуватися інші схеми захисту.

Крім того, показане право користувача (UR) або сертифікат прав користувача (URC) (503). URC містить ідентифікатор контенту (Cont_ID), призначений для визначення зв'язку певної одиниці контенту (і права на контент) із певним URC. URC також містить ідентифікатор особи/користувача (Pers_ID), що ідентифікує особу, зв'язок якої із даним контентом визначається. Цим ідентифікатором особи/користувача могли би бути, наприклад, ідентифікаційний номер даної особи, ім'я, значення хеш-коду відкритого ключа для даного користувача, або взагалі будь-який унікальний ідентифікатор особи.

Крім того, URC містить дані-права (RgtsDat), які визначають, які повноваження має даний користувач (визначений ідентифікатором Pers_ID) щодо даної одиниці контенту (що міститься в контейнері контенту, що містить такий самий ідентифікатор Cont_ID). Ці дані-права можуть визначати, наприклад, права щодо відтворення (наприклад, обмеження аудиторії особами, не молодшими 18 років, тільки європейським ринком тощо), права щодо створення копій першого покоління, термін дійсності, заборону на використання контенту більше трьох разів тощо. Крім того, дані-права (RgtsDat) можуть також визначати повноваження будь-якого користувача щодо даної одиниці контенту (які можуть як співпадати, так і відрізнятися від повноважень особи, що ідентифікується ідентифікатором Pers_ID).

Для реалізації такого URC можна було б застосовувати, наприклад, добре відомий сертифікат SPKI.

У варіанті здійснення, в якому зв'язок контенту з областю встановлюється через пристрої, а не через особи, URC був би не потрібен; натомість використовувався би сертифікат прав пристрою, який був би таким самим, як URC, за винятком того, що він містив би ідентифікатор пристрою замість ідентифікатора особи.

Для ілюстрації використання контейнера контенту, права на контент (CR) і сертифіката прав користувача (URC) відповідно до даного варіанта здійснення цього винаходу розглянемо нижченаведений простий приклад, що ілюструє здійснення користувачем доступу до одиниці контенту.

Спочатку одержують ідентифікатор контенту (Cont_ID) для тієї конкретної одиниці контенту, до якої користувач бажає здійснити доступ, і ідентифікатор особи (Pers_ID) цього користувача. Ідентифікатор особи може бути одержаний, напри-

клад, за допомогою особистого ідентифікувального пристрою (наприклад, смарт-карти, мобільного телефону, мобільного телефону зі смарт-картою, біометричного датчика тощо, або іншим чином). Ідентифікатор контенту може бути одержаний, наприклад, на основі імені файла, вибору файла, із заголовка контейнера контенту тощо.

Потім здійснюють перевірку того, чи належать одиниця контенту і користувач до однієї і тієї самої області дозволеного використання контенту. Перевірка того, чи належить користувача до певної області, здійснюється шляхом перевірки того, чи міститься ідентифікатор даної особи (Pers_ID) в сертифікаті користувачів області (DUC) (див. фіг. 1, 2 і 3). Якщо він там міститься, то належність користувача до області вважають встановленою, і йому дозволяється здійснювати доступ до контенту, що також належить до цієї області.

Потім перевіряється, чи належить дана одиниця контенту до тієї самої області, шляхом перевірки того, чи визначена відповідність ідентифікатора контенту даної одиниці контенту якійсь особі, що належить до даної області, тобто шляхом перевірки того, чи існує належний до даної області URC із таким самим ідентифікатором контенту. Якщо так, тоді одиниця контенту належить до тієї самої області, і отже згаданий користувач (за умови, що користувач і/або пристрій, що застосовується, були перевірені) має право здійснювати доступ до неї. Крім того, дані-права (Rights Dat), що містяться в URC, можуть також визначати обмежений доступ до одиниці контенту. Дані-права можуть визначати правила, права, умови для особи, що відповідає ідентифікатору Pers_ID, і/або правила, права, умови загалом. Наприклад, вони могли б визначати, що всі користувачі даної області мають право відтворення, тоді як користувач, якому відповідає ідентифікатор Pers_ID, додатково має виключні права створювати копії першого покоління.

Як правило, користувач здійснює доступ до одиниці контенту із застосуванням певного пристрою. Якщо користувач не належить до даної області, або неможливо одержати належний ідентифікатор особи користувача (наприклад, доступ до контенту прагне здійснити товариш), то необхідно перевірити, чи належить пристрій, використовуваний користувачем для здійснення доступу до даної одиниці контенту, до тієї самої області, що і дана одиниця контенту, для того щоб дозволити користувачу здійснення доступу до цієї одиниці контенту, оскільки або він не належить, або не можна встановити, чи він належить до тієї самої області, що і дана одиниця контенту. Це здійснюють шляхом одержання ідентифікатора області (Domain_ID) з DUC, з яким зв'язана (через особу) одиниця контенту. Цей Domain_ID застосовується для виявлення сертифіката пристроїв області (DDC) (див. фіг. 1, фіг. 2 і фіг. 3), що містить такий самий Domain_ID, і перевірки того, чи містить цей DDC ідентифікатор Dev.ID того пристрою, з використанням якого користувач намагається здійснити доступ до одиниці контенту. Якщо DDC містить ідентифікатор Dev.ID цього пристрою, то користувач (або будь-які інші користувачі) може викорис-

товувати даний пристрій для здійснення доступу до даного контенту (і всього іншого контенту цієї області).

Ці три етапи перевірки - прав доступу до одиниці контенту, користувача і пристрою - в альтернативних варіантах можуть здійснюватися в іншому порядку, відмінному від описаного, або, наприклад, паралельно, принаймні певною мірою.

Після того, як результати перевірки покажуть, що користувач або пристрій належать до тієї самої області, що і контент, одержаний ідентифікатор контенту застосовується для знаходження права на контент (CR), що відповідає тій одиниці контенту, до якої здійснюють доступ, щоб одержати криптографічний ключ, необхідний для дешифрування зашифрованої одиниці контенту. Потім, застосовуючи ідентифікатор контенту, знаходять також контейнер контенту, що містить цю зашифровану одиницю контенту.

Нарешті, ключ, що міститься у праві на контент, застосовують для дешифрування одиниці контенту, яка стає доступною, наприклад, для візуалізації, копіювання на оптичний диск, редагування тощо. Як альтернатива, одиниця контенту може бути дешифрована із використанням права на контент до передавання в пристрій, що використовується для здійснення доступу, так що передаватиметься лише одиниця контенту. Однак це вимагає вживання спеціальних заходів для захисту одиниці контенту під час її передавання, щоб унеможливити "витік" незахищеного контенту.

Цей процес ілюструється на фіг. 4а за допомогою стрілок, що показують зв'язок за полем Cont_ID різних структур.

Таким чином, якщо результати перевірки засвідчили, що конкретний користувач належить до тієї самої області, що і одиниця контенту, до якої здійснюється доступ, то тоді немає необхідності у перевірці того, чи належить пристрій, що використовується даним користувачем, до тієї самої області. Більш того, такий визнаний повноважним користувач може здійснювати доступ до цієї одиниці контенту із використанням будь-яких пристроїв. Аналогічно, якщо результати перевірки засвідчили, що певний пристрій належить до тієї самої області, то будь-які користувачі можуть здійснювати доступ до даної одиниці контенту із використанням цього пристрою, і необхідності перевіряти користувача немає.

Отже, підвищується гнучкість при здійсненні одним або декількома користувачами доступу до контенту в області дозволеного використання контенту (AD), і при цьому зберігається захищеність контенту.

На фіг. 4b зображена (як можливий приклад) структура даних (фрагмент) з контейнером даних, правом на контент (CR) і сертифікатом прав області (DRC), що використовується у варіанті здійснення даного винаходу, показаному на фіг. 2. У цьому варіанті здійснення одиниці контенту визначаються належними до області за допомогою DRC, а не відповідними користувачам (за допомогою URC) з відповідної області.

Контейнер контенту (501) і право на контент (CR) (502) відповідають відповідним контейнеру

контенту і праву на контент, показаним і описаним, наприклад, із посиланнями на фіг. 4а. Запроваджено також сертифікат прав області (DRC) 504, що містить ідентифікатор контенту (Cont_ID), який використовується для встановлення зв'язку між якоюсь конкретною одиницею контенту (і правом на контент) і якимось конкретним DRC. DRC містить також ідентифікатор області (Domain_ID), що визначає область, до якої визначається належним даний контент. Цей ідентифікатор області відповідає відповідному ідентифікатору з сертифікату пристроїв області (DCC) і сертифікату користувачів області (DUC), що були описані з посиланнями на фіг. 1, фіг. 2 і фіг. 3.

Крім того, DCR (504) містить дані-права (RghtDat), які визначають права і повноваження одного або декількох користувачів щодо відповідної одиниці контенту (тієї, що міститься у контейнері контенту з таким самим Cont_ID). Ці дані-права аналогічні даним-правам з URC, описаному з посиланнями на фіг. 4а.

Для ілюстрації використання контейнера контенту, права на контент і сертифіката прав області відповідно до цього варіанта здійснення цього винаходу розглянемо наведений нижче простий приклад, що ілюструє здійснення користувачем доступу до одиниці контенту з використанням якогось конкретного пристрою.

Спочатку одержують ідентифікатор контенту (Cont_ID) тієї одиниці контенту, до якої користувач прагне здійснити доступ, ідентифікатор особи (Pers_ID) даного користувача і ідентифікатор області (Domain_ID), до якої належить дана одиниця контенту. Ідентифікатор контенту і ідентифікатор особи можуть бути одержані так, як описано з посиланнями на фіг. 4а. Ідентифікатор області (Domain_ID) одержують із поля Domain_ID сертифіката DRC, з яким є зв'язок у даного контенту.

Після цього перевіряють, чи належать дані одиниця контенту і користувач до однієї і тієї самої області дозволеного використання контенту. Перевірка належності користувача до певної області виконується шляхом перевірки того, чи міститься його ідентифікатор особи (Pers_ID) у сертифікаті користувачів області (DUC) (показаний на фіг. 1, фіг. 2 і фіг. 3), що містить відповідний ідентифікатор області. Якщо міститься, то це означає, що підтверджені належність даного користувача до відповідної області і його права на здійснення доступу до контенту, що також належить до даної області.

Потім перевіряють, чи належить і дана одиниця контенту до тієї самої області, шляхом перевірки того, чи існує зв'язок між ідентифікатором контенту даної одиниці контенту і даною областю, тобто перевіряючи, чи є зв'язок між даною областю і DRC, що містить згаданий ідентифікатор контенту. Якщо є, то дана одиниця контенту належить до тієї самої області, і тому користувач (за умови, що користувач і/або пристрій, який їм використовується, вже були перевірені) має право здійснювати доступу до неї. Крім того, дані-права (RghtDat) можуть визначати обмежений доступ до відповідної одиниці контенту, як описано з посиланнями на фіг. 4а.

Як правило, користувач здійснює доступ до одиниці контенту із застосуванням певного пристрою. Якщо користувач не належить до даної області, або неможливо одержати належний ідентифікатор особи користувача (наприклад, доступ до контенту прагне здійснити товариш), то необхідно перевірити, чи належить пристрій, використовуваний користувачем для здійснення доступу до даної одиниці контенту, до тієї самої області, що і дана одиниця контенту, для того щоб дозволити користувачу здійснення доступу до цієї одиниці контенту, оскільки або він не належить, або не можна встановити, чи він належить до тієї самої області, що і дана одиниця контенту. Це здійснюють шляхом одержання ідентифікатора області (Domain_ID) з DRC, з яким зв'язана одиниця контенту. Цей ідентифікатор Domain_ID використовують для виявлення сертифіката пристроїв області (DDC) (див. фіг. 1, фіг. 2 і фіг. 3), що містить такий самий Domain_ID, і перевірки того, чи містить цей DDC ідентифікатор Dev.ID того пристрою, з використанням якого користувач намагається здійснити доступ до одиниці контенту. Якщо DDC містить ідентифікатор Dev.ID цього пристрою, то користувач (або будь-які інші користувачі) може використовувати даний пристрій для здійснення доступу до даного контенту (і всього іншого контенту цієї області).

Ці три етапи перевірки - прав доступу до одиниці контенту, користувача і пристрою - в альтернативних варіантах можуть здійснюватися в іншому порядку, відмінному від описаного, або, наприклад, паралельно, принаймні певною мірою.

Після того, як результати перевірки покажуть, що дані користувач, контент і пристрій належать до однієї області, доступ до одиниці контенту здійснюється так, як описано з посиланнями на фіг. 4а, тобто шляхом одержання права на контент, дешифрування контенту і т.д.

Цей процес ілюструється на фіг. 4b за допомогою стрілок, що показують зв'язок за полем Cont_ID різних структур.

На фіг. 5 схематично зображено приклад системи, що включає в себе пристрої і осіб, які разом утворюють область дозволеного використання контенту (AD). Мережа (501) робить можливим обмін даними між декількома пристроями, наприклад, у будинку або квартирі. Пристроями в цьому прикладі є телевізор (504), цифрова відеосистема (503), музичний центр (502) і переносний пристрій (507), підключений до мережі (501) за допомогою бездротового зв'язку через точку бездротового доступу (506). Також на фіг. 5 показано користувача/особу (505).

Розглянемо приклад, в якому до області дозволеного використання контенту (100) належать телевізор (504), цифрова відеосистема (503), музичний центр (502) і користувач (505), а також декілька одиниць контенту (не показані) (визначених належними до даної області через осіб/користувачів або через пристрої - як показано на фіг. 1, або через сертифікати прав області - як показано на фіг. 2).

У даному прикладі користувач прагне здійснити доступ до певної одиниці контенту, використо-

вуючи переносний пристрій (507). Користувач може знаходитися як у тому самому місці, що і пристрої, так і в іншому місці (наприклад, в готельному номері). Для того щоб користувач зміг здійснити доступ до одиниці контенту, відповідно до даного винаходу необхідно пересвідчитися у тому, що дана особа (505) належить до області (100), оскільки переносний пристрій (507) до неї не належить. Це може бути виконане шляхом однозначної ідентифікації користувача, наприклад, за допомогою пристрою зчитування смарт-карт, наприклад, передбаченого в переносному пристрої (507), який може потім передати ідентифікатор користувача (User ID) в мережу (501). Будемо вважати, що право на контент і одиниця контенту знаходяться на переносному пристрої (507) (в іншому випадку вони можуть бути туди передані). Після цього користувач перевіряється, як описано вище з посиланнями на фіг. 4a або фіг. 4b. Після підтвердження повноважень користувача може бути здійснений доступ до даної одиниці контенту.

Розглянемо тепер інший приклад, в якому до області дозволеного використання контенту (100) належать телевізор (504), цифрова відеосистема (503), музичний центр (502) і переносний пристрій (507), а також декілька одиниць контенту (не показані) (визначених належними до даної області через осіб/користувачів або через пристрої - як показано на фіг. 1, або через сертифікати прав області - як показано на фіг. 2). У цьому прикладі користувач (505) не належить до області дозволеного використання контенту (100); наприклад, він може бути сусідом або товаришем, що зайшов в гості. У цьому прикладі користувач також прагне здійснити

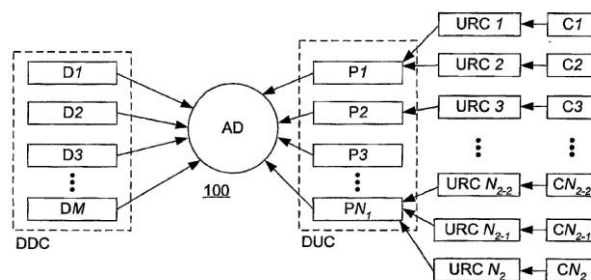
доступ до даної одиниці контенту з використанням переносного пристрою (507).

Для того щоб такий користувач зміг здійснити доступ до даної одиниці контенту, відповідно до даного винаходу необхідно пересвідчитися у тому, що переносний пристрій (507) належить до області (100), оскільки особа (505) до неї не належить.

Це може бути виконане шляхом перевірки того, чи належить переносний пристрій (507) до тієї самої області, до якої належить одиниця контенту, як описано з посиланнями на фіг. 4a або фіг. 4b. Після підтвердження повноважень пристрою згаданий користувач зможе здійснити доступ до даної одиниці контенту, використовуючи переносний пристрій (507).

У формулі винаходу будь-який номер позиції в дужках не повинен тлумачитися як такий, що обмежує обсяг охорони, що визначається формулою винаходу. Вирази "містить", "включає", "належить" тощо не виключають наявності інших елементів або етапів, крім перелічених. Вживання однини не повинно тлумачитися як таке, що виключає можливість наявності декількох відповідних елементів.

Винахід може бути реалізований за допомогою апаратних засобів, які включають в себе декілька окремих засобів, і за допомогою відповідним чином запрограмованого комп'ютера. У пункті формули винаходу, що стосується пристрою, де перелічені декілька засобів, деякі з цих засобів можуть бути реалізовані одним і тим самим апаратним засобом. Той факт, що певні заходи, що згадуються у непов'язаних залежних пунктах формули винаходу, не повинен тлумачитися так, що сполучення цих заходів не може бути здійснене або є небажаним.



ФІГ. 1

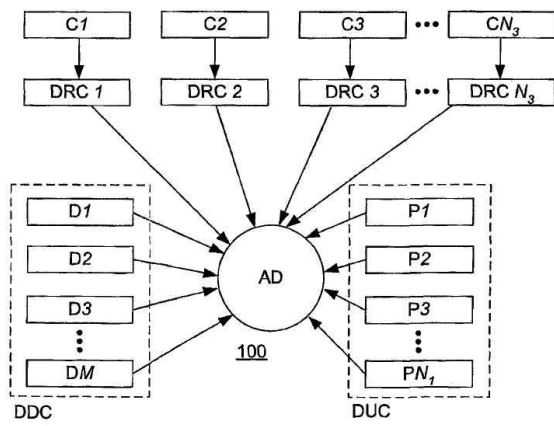


FIG. 2

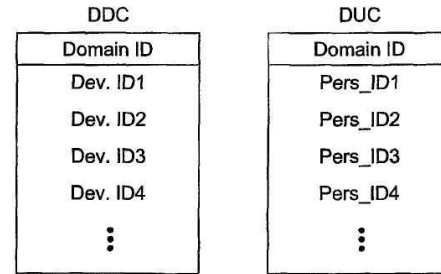


FIG. 3

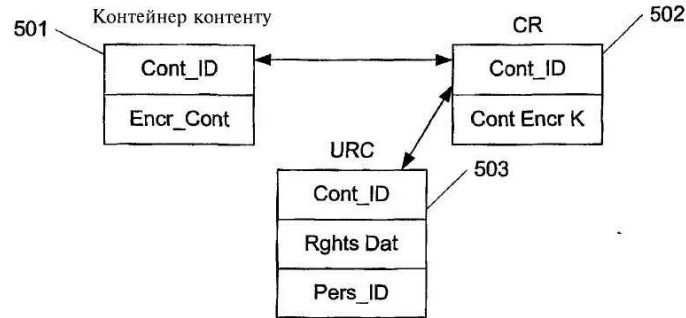


FIG. 4a

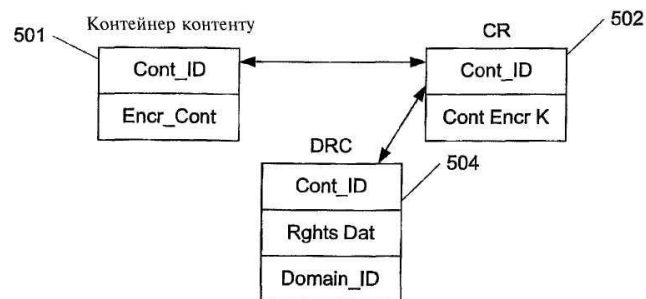
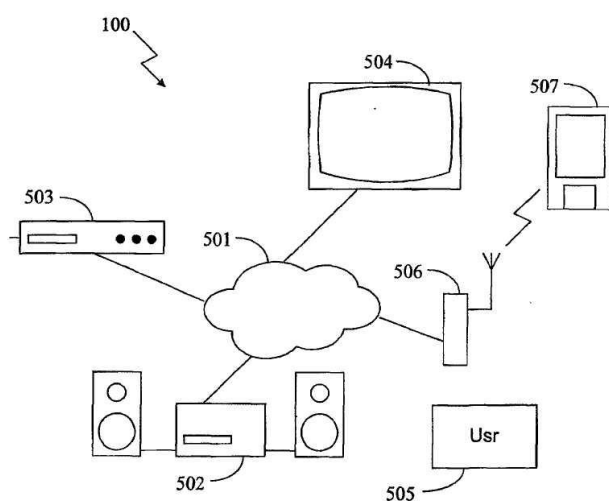


FIG. 4b



ФІГ. 5