



УКРАЇНА

(19) UA (11) 85178 (13) C2

(51) МПК (2006)

H04Q 7/38

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

(54) СПОСІБ ОБРОБКИ ПОВІДОМЛЕННЯ ЗАХИСТУ В СИСТЕМІ МОБІЛЬНОГО ЗВ'ЯЗКУ

1

2

(21) а200508628

(22) 29.12.2003

(24) 12.01.2009

(86) PCT/KR03/02877, 29.12.2003

(31) 10-2003-0008512

(32) 11.02.2003

(33) KR

(46) 12.01.2009, Бюл.№ 1, 2009 р.

(72) ЧУН СУНГ ДАК, ЙІ СЕУНГ ДЗУН, ЛІ ЯНГ ДАЕ

(73) ЕЛ ДЖІ ЕЛЕКТРОНІКС ІНК.

(56) WO 02454531 A1, 06.06.2002

EP 0977452 A2, 02.02.2000

3rd Generation Partnership Project: "Technical Specification Group Services and System Aspects; 3G Security, Security Architecture (Release 5)" - 3GPP TS 33.102 v5.0.0 (2002-06), pages 1-61 [retrieved on 10.03.2004]

(57) 1. Спосіб обробки повідомлення захисту в системі мобільного зв'язку, який полягає в тому, що приймають повідомлення захисту, здійснюють перевірку цілісності прийнятого повідомлення захисту за допомогою створення очікуваного значення аутентифікації з використанням змінних захисту, включених у прийняте повідомлення захисту, і порівнюють очікуване значення аутен-

тифікації з прийнятим кодом аутентифікації, прийнятим спільно з повідомленням захисту, який відрізняється тим, що відкидають прийняте повідомлення захисту і залишають значення щонайменше однієї змінної захисту, збереженої у приймаючій стороні незмінною, якщо прийняте повідомлення захисту не пройшло перевірку цілісності, і значення щонайменше однієї змінної захисту, збереженої у приймаючій стороні, оновлюють новою інформацією захисту, отриманою прийнятим повідомленням захисту, якщо прийняте повідомлення захисту пройшло перевірку цілісності.

2. Спосіб за п. 1, в якому повідомлення захисту є повідомленням KPP (керування радіоресурсами).

3. Спосіб за п. 1, в якому повідомлення захисту є повідомленням сигналізації.

4. Спосіб за п. 1, який додатково полягає в тому, що зберігають значення щонайменше однієї змінної захисту, збереженої у приймаючій стороні, оновлене новою інформацією захисту.

5. Спосіб за п. 1, який додатково полягає в тому, що повторно зберігають збережене значення щонайменше однієї змінної захисту, якщо прийняте повідомлення захисту пройшло перевірку цілісності.

Даний винахід відноситься до способів обробки повідомлень, що застосовуються в мобільному зв'язку, і конкретніше до способу обробки повідомлення захисту в рівні РУР (RRC).

UMTS (UMTS) (універсальна мобільна телекомунікаційна система) включає в себе ОК (UE) (обладнання користувача), УНМРД (UTRAN) (наземну мережу радіодоступу UMTS) та БМ (CN) (базову мережу). Крім того, УНМРД містить множину ПРМ (RNS) (підсистем радіомережі). Кожна ПРМ містить КРМ (RNC) (контролер радіомережі) і множину вузлів В, керованих КРМ. Вузол В приймає сигнали, передані по каналу висхідної лінії зв'язку з ОК, і передає сигнали по каналу низхідної лінії зв'язку в ОК. КРМ відповідає за виділення і керування радіо ресурсами і відіграє роль пункту доступу для з'єднання вузла В з БМ. Кожне ОК, з'єднане з UMTS, керується конкретним КРМ в УНМРД, і конкретний КРМ називається ОКРМ (SRNC) (обслуговуючим КРМ).

УНМРД конфігурує, підтримує та керує КРД (RAB) (каналами радіодоступу) для зв'язків між ОК та БМ. БМ застосовує вимоги крізної ЯО (QoS) (якість обслуговування) до КРД, і КРД підтримує вимоги ЯО, встановлені БМ. УНМРД крім того конфігурує, підтримує і керує КРД, дозволяючи задовольняти вимогам крізної ЯО.

Радіо інтерфейсний протокол по вертикалі містить фізичний рівень, рівень ліній передачі даних і мережний рівень, а по горизонталі містить площину користувача для забезпечення передачі інформації і площину керування для забезпечення передачі сигналізації. Рівні протоколу групуються в L1 (рівень 1), L2 (рівень 2) та L3 (рівень 3) на основі трьох нижніх рівнів ВВС (OSI) (взаємодія відкритих систем) еталонної моделі. L1 забезпечує верхні рівні з обслуговуванням передачі інформації за допомогою різних методів радіопередачі. L1 з'єднується з рівнем КДС (MAC) (керування доступом до середовища) верхнього рівня через транс-

(13) C2

(11) 85178

(19) UA

портні канали.

Рівень керування лінією радіозв'язку КЛР (RLC) підтримує надійну передачу даних і виконує сегментацію і з'єднання СБД (SDU) (сервісні блоки даних) КЛР, переданих з верхніх рівнів. СБД КЛР, передані з верхніх рівнів, розділяються на блоки даних КЛР, які можуть оброблятися в рівні КЛР, і до розділених блоків даних КЛР додається інформація заголовка для перенесення на рівень КДС в формі ПБД (PDU) (протокольного блока даних).

Рівень ПППД (PDCP) (протокол поєднання пакетних даних) розташовується поверх рівня RLC. Рівень ПППД забезпечує для даних, які передаються по мережному протоколу, ефективну передачу по радіоінтерфейсу, смуга пропускання якого відносно обмежена. Рівень КРГД (BMC) (керування радіомовленням/груповою доставкою) планує ОК, на які буде передаватися повідомлення CP (CB) (стільникового радіомовлення), передане з БМ, і передає повідомлення CP на відповідні ОК, розташовані в конкретному стільнику(ах) на основі планування.

За запитом від верхніх рівнів рівень KPP (RRC) (керування радіоресурсами) керує передачею і фізичними каналами для виконання встановлення, реконфігурації та роз'єднання ОРК (RB) (однонаправлені радіоканали). У цьому випадку ОРК означає обслуговування, що забезпечується рівнем L2 для передачі даних між ОК та УНМРД.

Тим часом різні канали для прийому/передачі даних визначаються між ОК та УНМРД для використання. Дані відправляються і приймаються між фізичним рівнем ОК і рівнем УНМРД за допомогою фізичного каналу. У доповнення до фізичного каналу визначаються канали передачі даних між рівнями протоколів як канали передачі і логічні канали в мережі радіо доступу УМТС. Логічні канали забезпечуються для обміну даними між рівнем RLC і рівнем КДС, тоді як між рівнем КДС і рівнем КЛР передбачаються канали передачі для обміну даними. Здійснюється встановлення відповідності між каналами передачі в рівні КДС, тоді як відповідність встановлюється в фізичному рівні між транспортним рівнем і фізичним рівнем.

Різні види повідомлень приймаються/передаються між терміналом та УНМРД. «Перевірка захищеності» в основному виконується для захисту даних, що містяться в повідомленнях. Така «перевірка захищеності» включає в себе «шифрування» і «перевірку цілісності». Шифрування додає конкретну маску, яка відома тільки передавальній та приймальній сторонам, до повідомлення так, що третя сторона, якщо не знає маски, нездатна розпізнати зміст повідомлення.

Перевірка цілісності використовується для перевірки того, чи змінила неуповноважена третя сторона зміст повідомлення, або чи зроблена передача неуповноваженою стороною. А саме, перевірка цілісності здійснюється для захисту цілісності і є процедурою, необхідною для перевірки того, чи змінений раніше та умисно третьою стороною зміст прийнятого повідомлення.

В УМТС одночасно виконуються шифрування і перевірка цілісності для більшості повідомлень, що передаються на рівень KPP, і більшості повід-

омлень керування, що передаються на верхні рівні рівня KPP. А шифрування виконується тільки для інших основних даних користувача. Така перевірка цілісності може виконуватися в рівні KPP.

Таким чином, якщо приймається повідомлення, зміст якого змінений третьою стороною між передавальною і приймальною сторонами, або для фільтрації повідомлення, переданого від неуповноваженої передавальної сторони, приймальною стороною виконується перевірка цілісності для прийнятого повідомлення. У результаті прийняте повідомлення звичайно обробляється або відкидається відповідно до того, чи пройшло прийняте повідомлення перевірку цілісності чи ні.

Наприклад, одне з прийнятих повідомлень може бути повідомленням керування встановлення захисту. При зв'язку між ОК та мережею (наприклад, УНМРД) повідомлення керування встановлення захисту використовується для ініціювання захисту повідомлень, які потім будуть передаватися. Крім того, повідомлення керування встановлення захисту може використовуватися для керування змінними середовища, що відноситься до захисту, яке використовується для з'єднання, по якому виконується процес захисту.

Інформація, яка відноситься до керування змінними середовища, що відноситься до захисту, серед змістів, що містяться в повідомленні керування встановлення захисту, називається інформацією встановлення середовища, що відноситься до захисту. Ще, інформація, що відноситься до захисту середовища, яка міститься в повідомленні керування встановлення захисту, сама може бути змінена неуповноваженою третьою стороною або може бути передана неуповноваженою передавальною стороною, через що не можна довіряти такій інформації, що відноситься до захисту.

Відповідно, даний винахід направлений на спосіб обробки повідомлення захисту в системі мобільного зв'язку, який по суті усуває одну або більше проблем, що належать обмеженням та недолікам відповідного рівня техніки.

Задачею даного винаходу є створення способу обробки повідомлення керування встановлення захисту, що включає в себе перевірку захищеності самого повідомлення захисту.

Додаткові переваги, задачі та ознаки винаходу будуть сформульовані далі частково в описі, який наведений нижче, а частково стануть очевидні для фахівців при вивченні нижченаведеного або можуть бути перевірені при застосуванні винаходу. Задачі та інші переваги винаходу можуть здійснюватися і досягатися конкретною структурою, детально вказаною в написаному описі та наведений тут формулі винаходу, а також в прикладених кресленнях.

Для вирішення цих цілей та досягнення інших переваг і відповідно до призначення винаходу, що реалізовується і широко описаний тут, спосіб обробки повідомлення захисту в системі мобільного зв'язку відповідно до даного винаходу включає в себе етапи прийому повідомлення захисту, збереження попередніх змінних, що відносяться до захисту, виконання перевірки захисту в повідомленні захисту, відкидання або обробки повідомлення

захисту відповідно до результатів перевірки захисту та оновлення змінних, що відносяться до захисту.

Даний винахід характеризується тим, що перевірка захищеності самого повідомлення захисту здійснюється для захищеності захисту цілісності.

Потрібно розуміти, що вищезазначений загальний опис і подальший докладний опис даного винаходу є зразковими та пояснювальними і призначаються для забезпечення додаткових пояснень заявленого винаходу.

Супроводжуючі креслення, які включені сюди для забезпечення подальшого розуміння винаходу, і включені в цю заяву і складають частину цієї заявки, ілюструють варіант(и) здійснення винаходу і спільно з описом служать для пояснення принципів винаходу. На кресленнях:

Фіг.1 показує блок-схему алгоритму способу обробки загального повідомлення;

Фіг.2 показує блок-схему алгоритму способу обробки повідомлення керування встановленням захисту відповідно до першого варіанту здійснення даного винаходу;

Фіг.3 показує блок-схему способу обробки повідомлення керування встановленням захисту відповідно до другого варіанта здійснення даного винаходу;

Фіг.4 показує схему одного варіанту здійснення, що представляє РАХУНОК-I (COUNT-I) в змінних, що відносяться до захисту середовища; і

Фіг.5 показує схему для пояснення одного варіанту здійснення створення значення аутентифікації в перевірці цілісності.

Тепер буде зроблене докладне посилання на переважні варіанти здійснення винаходу, приклади яких показані на супроводжуючих кресленнях. Де можливо, одні і ті самі посилальні позиції будуть використовуватися на кресленнях для посилання на одні і ті самі елементи або подібні частини.

Фіг.1 показує блок-схему способу обробки загального повідомлення.

На Фіг.1 ОК (UE) (обладнання користувача) спочатку приймає основне повідомлення (S11) і потім виконує перевірку цілісності його (S12). Відповідно до результату перевірки цілісності повідомлення звичайно обробляється або відхиляється. Тобто, якщо повідомлення проходить перевірку цілісності, то воно звичайно обробляється (S13). Якщо повідомлення не відповідає контролю цілісності, воно відкидається оскільки існує проблема захисту (S14).

Фіг.2 показує блок-схему алгоритму способу для обробки повідомлення керування встановленням захисту відповідно до першого варіанту здійснення даного винаходу.

На Фіг.2 ОК (обладнання користувача) приймає повідомлення керування встановленням захисту (S21). І змінні захисту, що відносяться до захисту, оновлюються за допомогою інформації встановлення середовища, що відноситься до захисту, яка міститься в прийнятому повідомленні керування встановленням захисту (S22). ОК (наприклад, термінал) саме виконує перевірку захищеності (безпеки) для повідомлення керування встановленням захисту за допомогою оновлених

змінних, що відносяться до захисту середовища (S23). Перевірка захищеності включає в себе перевірку цілісності. Якщо повідомлення керування встановленням захисту проходить перевірку цілісності, то повідомлення обробляється звичайним чином (S24). Ще, якщо повідомленню керування встановленням захисту не вдається пройти перевірку цілісності, то повідомлення вважається ненормальним, тому прийняте повідомлення керування встановленням захисту відкидається (S25). Крім того, не можна покладатися на інформацію встановлення, що відноситься до захисту середовища, включену в повідомлення керування встановленням захисту. Отже, не можна використовувати інформацію встановлення, що відноситься до захисту середовища.

У першому варіанті здійснення даного винаходу коли приймальна сторона приймає повідомлення керування встановленням захисту, попередньо встановлені змінні, що відносяться до захисту середовища, оновлюються інформацією встановлення, що відноситься до захисту середовища, включеною в повідомлення, і попередні заздалегідь встановлені змінні, що відносяться до захисту середовища, відкидаються. Отже, змінні приймальної сторони, що відносяться до захисту середовища, не співпадають з цими змінними передавальної сторони, не можна далі обмінюватися повідомленнями, і приймальної сторони не можуть бути надані додаткові запитані послуги.

Фіг.3 показує блок-схему алгоритму способу обробки повідомлення керування встановленням захисту відповідно до другого варіанта здійснення даного винаходу.

На Фіг.3 спосіб обробки повідомлення керування встановленням захисту виконується таким чином.

Спочатку ОК (обладнання користувача) приймає повідомлення керування встановленням захисту (S31). До того, як ОК виконає перевірку безпеки на самому повідомленні керування встановленням захисту, змінні, що відносяться до захисту середовища, які були раніше встановлені, тимчасово зберігаються (S32). І змінні, що відносяться до захисту середовища, оновлюються за допомогою інформації встановлення, що відноситься до захисту середовища, включеною в прийняте повідомлення керування встановленням захисту (S33).

ОК (наприклад, термінал) виконує перевірку безпеки на самому повідомленні керування встановленням захисту за допомогою оновлених змінних, що відносяться до захисту середовища (S34). І перевірка безпеки включає в себе перевірку цілісності. Якщо повідомлення керування встановленням захисту проходить результат перевірки цілісності, тимчасово збережені змінні, що відносяться до захисту середовища, видаляються (S35). Після цього перевірка цілісності виконується для повідомлення, прийнятого пізніше, за допомогою оновлених змінних, що відносяться до захисту середовища, і повідомлення обробляється звичайним чином (S36).

Однак якщо повідомленню керування встановленням захисту не вдається пройти перевірку

цілісності, то воно обробляється так, що повідомлення керування встановленням захисту не приймається. А саме, якщо вважається, що повідомлення ненормальне, то прийняте повідомлення керування встановленням захисту відкидається (S31). Крім того, інформація встановлення, що відноситься до захисту середовища, включена в повідомлення керування встановленням захисту, не буде використовуватися, оскільки воно не надійне. Таким чином, у випадку, коли повідомлення керування встановленням захисту нездатне пройти перевірки цілісності, це повідомлення керування встановленням захисту відкидається, а також повторно зберігаються (відновлюються) тимчасово збережені змінні, що відносяться до захисту середовища (S38). І повідомлення, прийняті пізніше, обробляються за допомогою повторно збережених (відновлених) змінних, що відносяться до захисту середовища.

Відповідно до другого варіанта здійснення даного винаходу, навіть якщо повідомлення, зміст якого змінений в середині передачі з УНМРД в ОК, приймається, або навіть якщо повідомлення керування встановленням захисту, передане від неуповноваженої сторони, приймається, воно здатне підтримувати змінні, що відносяться до захисту середовища, однаковими для цього терміналу за допомогою попередньо встановлених змінних, що відносяться до захисту середовища, шляхом їх збереження та їх повторного збереження (відновлення). Отже, якщо змінні встановлення, що відносяться до захисту середовища, видаляються замість збереження, це може запобігти випадку, коли повідомлення не може бути пізніше оброблене через відмінності між змінними ОК та УНМРД, що відносяться до захисту середовища.

Спосіб здійснення перевірки цілісності детально пояснюється далі. Для такого пояснення роз'яснюються параметри, необхідні для здійснення перевірки цілісності. Для здійснення перевірки цілісності потрібні такі параметри, як КЦ (ІК) (ключ цілісності), РАХУНОК-І, ПОВІДОМЛЕННЯ, НАПРЯМОК (ідентифікатор напрямку, 1 біт) та ОНОВЛЕННЯ.

Фіг.4 показує схему одного з варіантів здійснення, що представляє РАХУНОК-І в змінних, які відносяться до захисту середовища.

РАХУНОК-І є однією з змінних, що відносяться до захисту середовища. Тобто РАХУНОК-І є значенням, відповідним послідовному числу для перевірки цілісності.

На Фіг.4 РАХУНОК-І включає в себе дві області. Одна область з цих двох областей включає в себе НГК КРР (RRC HFN) (номер гіперкадру) з 28 біт, в той час як інша область з цих двох областей включає в себе ПН КРР (RRC SN) (порядковий номер) з 4 біт.

Процедура оновлення змінних, що відносяться до захисту середовища, виконується таким чином, що переустановлюється НГК як значення старших 28 біт РАХУНОК-І. Тобто переустановлене значення НГК може бути значенням ПОЧАТОК, нещодавно переданим терміналом, 0 або конкретним значенням. І ОК виконує перевірку захисту на прийнятому повідомленні керування встановлен-

ням захисту за допомогою оновлених змінних, що відносяться до захисту середовища.

КЦ серед параметрів для здійснення перевірки цілісності вказує ключ цілісності, який генерується в процедурі аутентифікації у верхньому рівні рівня КРР для сповіщення рівня КРР. Значення КЦ не передається по радіоінтерфейсу, але верхній рівень рівня КРР в терміналі і мережі (наприклад, УНМРД) обчислює значення КЦ для використання на основі конкретних вхідних значень, відповідно.

Значення ПОЧАТОК зчитується з SIM карти системи, коли термінал ініціює з'єднання між рівнями КРР УНМРД і терміналом, і передається в УНМРД. Значення ПОЧАТОК, яке включене в повідомлення, що передається з верхнього рівня в рівень КРР терміналу, може бути передане в УНМРД. Коли активується з'єднання між рівнями КРР УНМРД і терміналом, значення ПОЧАТОК визначається як найбільше число верхніх 20 біт поточного використовуваного значення РАХУНОК-І або РАХУНОК-С (яке використовується для шифрування і відіграє роль, подібну до РАХУНОК-І). І значення ПОЧАТОК, що використовується в поточний момент між рівнями КРР терміналу та УНМРД, зберігається в SIM карті, коли з'єднання між рівнями КРР терміналу та УНМРД закінчується.

ПОВІДОМЛЕННЯ означає повідомлення, яке передається саме. НАПРЯМОК є дискримінатором напрямку, і його значення змінюється відповідно до висхідної лінії зв'язку або низхідної лінії зв'язку. НАПРЯМОК може бути встановлений як «0» або «1» на висхідній лінії зв'язку або низхідній лінії зв'язку. ОНОВЛЕННЯ є значенням, даним незалежно для кожного терміналу, і є значенням, яке УНМРД передає в ОК на початковому стані з'єднання КРР. Тобто значення ОНОВЛЕННЯ є довільним числом, яке УНМРД передає на ОК, яке призначене для забезпечення безпеки УНМРД від терміналу, що повторно використовує значення РАХУНОК-І та КСА-І (MAC-І) таким чином, що УНМРД забезпечує ОК новим значенням на кожному з'єднанні КРР. Значення КСА-І (MAC-І) (код-І повідомлення аутентифікації) є кодом повідомлення аутентифікації, який обчислюється за допомогою АЦУ (UIA) (алгоритму цілісності УМТС) із значеннями, що відносяться до захисту середовища, яке є контрольною сумою, вставленою в КРР PDU.

Якщо немає процедури оновлення значення ОНОВЛЕННЯ, порушник захисту легко робить захист УНМРД вразливим за допомогою запитання, що значення ПОЧАТОК, яке буде використовуватися як найвище значення РАХУНОК-І, повинне бути встановлене в дуже маленьке значення, коли запитане нове з'єднання між рівнями КРР, і потім за допомогою використання пари значень ПЧ та КСА-І, які були використані для попередніх з'єднань між рівнями КРР. Все ж така вразливість захисту може бути відвернена призначенням нового значення ОНОВЛЕННЯ в УНМРД кожний раз, коли знову встановлюється з'єднання між рівнями КРР.

Фіг.5 показує схему для пояснення одного варіанту створення значення аутентифікаційного значення в перевірці цілісності, в якому «f9» є стандартизованим алгоритмом створення перевірки

цілісності аутентифікації, визнаним 3GPP.

На Фіг.5 УНМРД і термінал використовують значення параметрів як вхідні значення, тим самим створюючи значення КСА-І та ХКСА-І за допомогою такого алгоритму як «f9». КСА-І є аутентифікаційним значенням перевірки цілісності, створеним в УНМРД, а ХКСА-І є аутентифікаційним значенням перевірки цілісності, створеним в терміналі. Якщо всі вхідні значення УНМРД і терміналу дорівнюють одне одному, то значення КСА-І та ХКСА-І, створені в процедурі на Фіг.3, будуть дорівнювати одне одному. Якщо ж повідомлення змінюється в середині обробки, вхідні значення ПОВІДОМЛЕННЯ приймальної сторони і передавальної сторони відрізняються одне від одного, так що значення ХКСА-І не дорівнює КСА-І.

Отже, якщо значення КСА-І та ХКСА-І не дорівнюють одне одному за результатом порівняння, термінал приймає рішення, що зміст прийнятого повідомлення керування встановленням захисту навмисно змінений під час передачі, або що прийняте повідомлення керування встановленням захисту передано неуповноваженою стороною. У такому випадку повідомлення керування встановленням захисту вважається недійсним через невдале проходження перевірки цілісності. УНМРД змінює частину вхідних значень, що використовуються для процедури на Фіг.3, кожен раз, коли відправляє нове повідомлення. І УНМРД створює новий КСА-І кожний раз за допомогою часткової зміни вхідних значень. Це здійснюється для запобігання тому, щоб неуповноважена сторона не використала повторно значення КСА-І для проходження перевірки цілісності.

Для цього УНМРД збільшує значення ПН РАХУНОК-І за допомогою приросту «1» кожен раз, коли відправляє повідомлення. Як згадано вище в попередньому описі, значення ПН складає молодші 4 біти РАХУНКУ-І. Значення ПН, яке дорівнює 4 бітам, може мати значення в діапазоні між 0 та 15 і послідовно збільшується на «1» від «0». Коли значення ПН стає «15», наступне значення ПН стає «0» і потім знову збільшується приростом на «1». Таким чином, значення НТК, яке відповідає найвищому значенню РАХУНКУ-І, збільшується на «1» кожен раз, коли ПН стає знову «0» з «15».

Отже, такий спосіб викликає той ефект, що РАХУНОК-І збільшується на «1» кожний раз, за допомогою чого вхідні значення частково змінюються в процедурі обчислення зашифрованого значення аутентифікації.

Тим часом, якщо термінал розпізнає значення ПН прийнятого повідомлення і вирішує, що значення ПН завершує один цикл, термінал збільшує це значення НТК на «1». Таким чином, РАХУНОК-І може співпадати з цим значенням передавальної сторони. Якщо такий спосіб використовується, термінал та УНМРД можуть мати однакову інформацію РАХУНОК-І, навіть якщо інформація ПН тільки відправлена. Крім цього, може бути відвер-

нена витік інформації захисту до третьої сторони, що може трапитися, коли відправляється весь РАХУНОК-І. Отже, УНМРД дозволяє приймальній стороні точно обчислювати значення ХКСА-І, а також додає значення ПН як нижче значення РАХУНКУ-І до повідомлення при кожній передачі повідомлення для запобігання проходження неуповноваженою третьою стороною перевірки цілісності. І значення КСА-І, яке буде використовуватися як еталон для терміналу для здійснення перевірки цілісності, додається до повідомлення при передачі.

Коли ОК приймає повідомлення керування встановленням захисту, необхідно виконати перевірку безпеки значення ПН. Для цього ОК керує своїм локальним параметром ПН тільки за допомогою значення ПН, прийнятого раніше. Якщо значення ПН, передане спільно з повідомленням керування встановленням захисту, дорівнює значенню ПН локального параметра терміналу, можна передбачити, що третя сторона відправляє повідомлення за допомогою однієї і тієї самої інформації захисту передавальної сторони, або що одне і те саме повідомлення передається знову з даного УНМРД. У цьому випадку термінал негайно відкидає це повідомлення керування встановленням захисту.

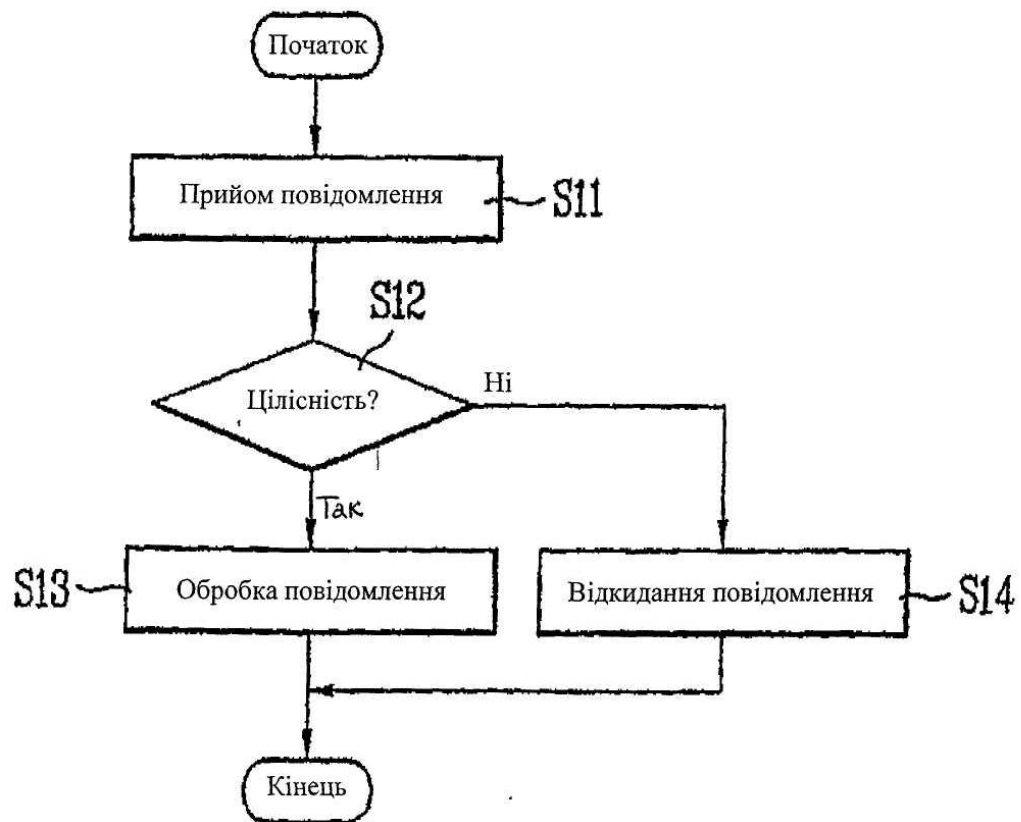
Термінал складає РАХУНОК-І за допомогою значення ПН, прийнятого спільно з повідомленням керування встановленням захисту, і обчислює ХКСА-І за допомогою параметрів, раніше встановлених в РАХУНОК-І та ОК. Параметри, раніше встановлені в ОК, включають в себе ПОВІДОМЛЕННЯ, НАПРЯМОК, ОНОВЛЕННЯ.

За допомогою порівняння значення КСА-І, переданого спільно з повідомленням керування встановленням захисту, зі значенням ХКСА-І, обчисленим ОК, ОК здійснює перевірку цілісності повідомлення керування встановленням захисту.

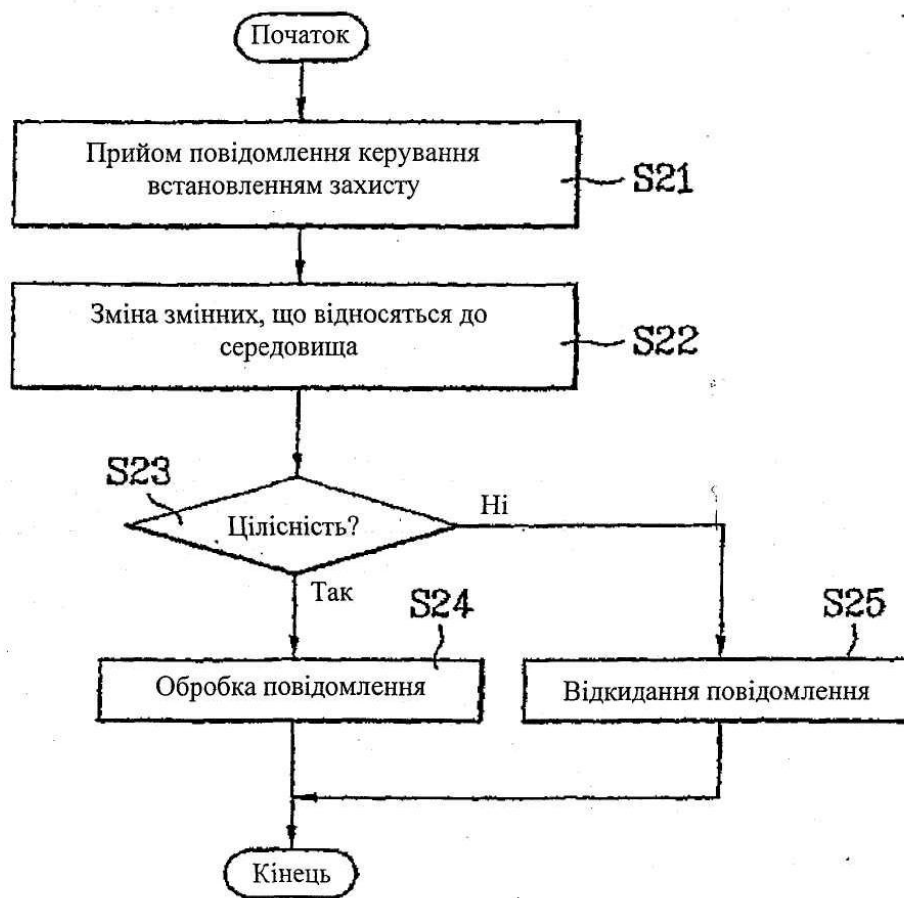
Коли прийняте повідомлення керування встановленням захисту проходить перевірку цілісності, приймальна сторона зберігає значення ПН, включене в повідомлення, в локальному параметрі ПН і використовує його для перевірки значення ПН наступного повідомлення.

Відповідно, спосіб згідно з даним винаходом реалізовується у вигляді програми і може бути збережений на записуючому носії інформації (CD-ROM, гнучкий диск, жорсткий диск, оптичний магнітний диск тощо) - в формі, яка може бути зчитана комп'ютером. Такий процес є очевидним для фахівця в цій галузі техніки, внаслідок чого це пояснення пропускається в цьому описі.

Буде очевидно для фахівця в цій галузі техніки, що різні модифікації та зміни можуть бути зроблені в даному винаході. Таким чином, мається на увазі, що даний винахід охоплює модифікації та зміни цього винаходу при умові, що вони попадають в обсязі прикладеної формули та її еквівалентів.



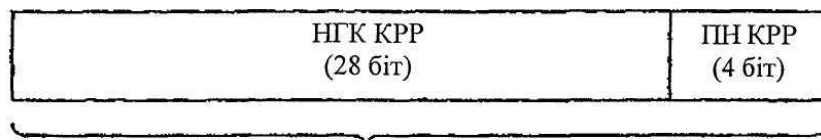
Фіг. 1



Фіг. 2

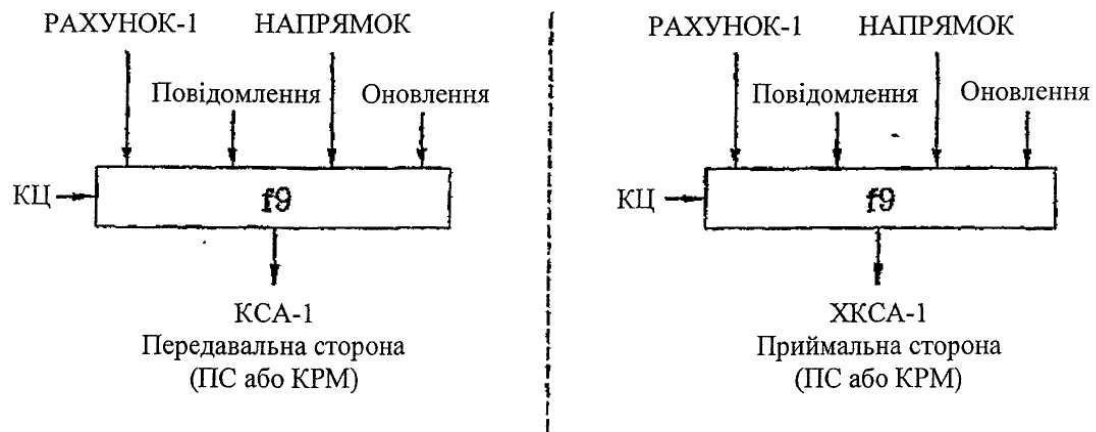


Фіг. 3



РАХУНОК-1

Фіг. 4



Фіг. 5