



УКРАЇНА

(19) UA

(11) 53651

(13) C2

(51) 7 H04L9/08

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

(54) СПОСІБ КРИПТОГРАФІЧНОГО ОБМІНУ КОДАМИ МІЖ ПЕРШИМ КОМП'ЮТЕРНИМ ПРИСТРОЄМ ТА ДРУГИМ КОМП'ЮТЕРНИМ ПРИСТРОЄМ

1

(21) 98126427  
(22) 16 05 1997  
(24) 17 02 2003  
(86) PCT/DE97/01002, 16.05.1997  
(31) 196 22 631 7  
(32) 05 06 1996  
(33) DE  
(46) 17 02 2003, Бюл. № 2, 2003 р  
(72) Ойхнер Мартін, DE, Кесслер Фолкер, DE  
(73) СІМЕНС АКЦІЕНШЕЗЕЛЬШАФТ, DE  
(56) DE, 3915262, 30 11 1989  
CHORLEY B J ET AL "The definition and implementation of a secure communications protocol" PROCEEDINGS OF THE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, ZURICH, SWITZERLAND, 4-6 OCT 1983  
(57) 1 Спосіб криптографічного обміну кодами між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2), згідно з яким  
- між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) здійснюється автентифікація,  
- між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) відбувається підбір алгоритмів захисту від несанкціонованого доступу (SP), який відрізняється тим, що  
- під час автентифікації між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) відбувається обмін автентифікаторами (AR<sub>A</sub>, AR<sub>B</sub>), за допомогою яких забезпечується автентичність комп'ютерних пристроїв (C1, C2),  
- під час відбору алгоритму захисту від несанкціонованого доступу (SP) застосовується принаймні один з автентифікаторів (AR<sub>A</sub>, AR<sub>B</sub>)  
2 Спосіб за п 1, який відрізняється тим, що  
- між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) відбувається обмін кодами (SA), а також  
- під час обміну кодами застосовується принаймні один з автентифікаторів (AR<sub>A</sub>, AR<sub>B</sub>)  
3 Спосіб за п 1 або 2, який відрізняється тим, що  
- перший комп'ютерний пристрій (C1) підпорядкований першому домену захисту (S1),  
- другий комп'ютерний пристрій (C2) підпорядкований другому домену захисту (S2),

2

- інші комп'ютерні пристрої (Ci) першого домену захисту (S1) або другого домену захисту (S2) здійснюють підбір іншого алгоритму захисту від несанкціонованого доступу (SPi), а також  
- при підборі застосовуються автентифікатори (AR<sub>A</sub>, AR<sub>B</sub>)  
4 Спосіб за одним з п 1 або 2, який відрізняється тим, що  
- перший комп'ютерний пристрій (C1) підпорядкований першому домену захисту (S1),  
- другий комп'ютерний пристрій (C2) підпорядкований другому домену захисту (S2),  
- інші комп'ютерні пристрої (Ci) першого домену захисту (S1) або другого домену захисту (S2) здійснюють інший обмін кодами (SAi), а також  
- при обміні кодами (SAi) застосовуються автентифікатори (AR<sub>A</sub>, AR<sub>B</sub>)  
5 Спосіб за п 1 або 2, який відрізняється тим, що  
- перший комп'ютерний пристрій (C1) підпорядкований першому домену захисту (S1),  
- другий комп'ютерний пристрій (C2) підпорядкований другому домену захисту (S2),  
- інші комп'ютерні пристрої (Ci) першого домену захисту (S1) або другого домену захисту (S2) здійснюють підбір іншого алгоритму захисту від несанкціонованого доступу (SPi),  
- інші комп'ютерні пристрої (Ci) першого домену захисту (S1) або другого домену захисту (S2) здійснюють інший обмін кодами (SAi),  
- при підборі застосовують автентифікатори (AR<sub>A</sub>, AR<sub>B</sub>),  
- при обміні кодами (SAi) застосовують автентифікатори AR<sub>A</sub>, AR<sub>B</sub>)  
6 Спосіб за одним з пп 1 - 5, який відрізняється тим, що  
в межах способу застосовуються геш-функції (h ()), що базуються на симетричних криптоалгоритмах  
7 Спосіб за одним з пп 1-5, який відрізняється тим, що  
в межах способу застосовуються цифрові сигнатури (SIG ())  
8 Спосіб за одним з пп 1 - 7, який відрізняється тим, що здійснюється інтенсивна автентифікація за способом X 509  
9 Спосіб за одним з пп 1-7, який відрізняється тим, що  
- для обміну кодами здійснюється автентифікація

(13) C2

(11) 53651

(19) UA

за способом Diffie-Hellman, а також - коди, обмін якими здійснювався за способом Diffie-Hellman, застосовуються як автентифікатори ( $AR_A$ ,  $AR_B$ )

10 Спосіб за одним з пп 1 - 9, який відрізняється тим, що здійснюється фаза переривання з'єднання

(Disconnect), у межах якої стираються розділені секретні дані, наприклад коди, обмін якими відбувся, або автентифікатори ( $AR_A$ ,  $AR_B$ )

11 Спосіб за п 10, який відрізняється тим, що стираються коди, обмін якими відбувся

12 Спосіб за п 11, який відрізняється тим, що послідовно стираються інші секретні дані

У багатьох галузях техніки є необхідним забезпечення захисту акту комунікації між партнерами від будь-яких зловживань за допомогою криптографічних способів. При цьому витрати, необхідні для забезпечення криптографічного захисту акту комунікації в цілому, залежать від галузі застосування. Так, наприклад, за деяких обставин під час приватних розмов не дуже важливо, щоб для захисту акту комунікації було вжито всіх можливих криптографічних заходів. Проте, надійний захист актів комунікації, зміст яких є вельми конфіденційним, набуває великого значення.

Процес вибору служб безпеки, а також механізмів, алгоритмів і параметрів, що використовуються для захисту актів комунікацій, називають алгоритмом захисту від несанкціонованого доступу, якого дотримуються під час актом комунікації між партнерами.

Проте, оскільки рівень необхідного захисту від несанкціонованого доступу і зв'язаний з ним відповідний алгоритм є різними для різних актів комунікації та галузей застосування, і оскільки партнери за актом комунікації фактично не мають у своєму розпорядженні всі криптографічні способи захисту, у разі частішої зміни партнерів за актом комунікації це може призвести до значних розбіжностей між необхідними або можливими алгоритмами захисту від несанкціонованого доступу, що підтримуються відповідним комп'ютерним пристроєм партнера за актом комунікації, тобто, можуть бути реалізовані.

Необхідно, щоб під час кожного акту комунікації у межах однієї групи, що бере участь в акті комунікації, було встановлено єдиний алгоритм захисту від несанкціонованого доступу для відповідного з'єднання.

У разі застосування великої кількості різних прикладних протоколів, що описані, між іншим, у документі "M. Altenhofen et al, The BERKOM Multimedia Collaboration Service, ACM Multimedia 93, ACM 0-89791-596-8/93/0457, CA, IUSA 1993", наприклад CMAP, CDAP тощо, виникає проблема, яка полягає у тому, що різні прикладні протоколи однакових або різних комп'ютерних пристроїв потребують різних алгоритмів захисту від несанкціонованого доступу. У залежності від обставин для забезпечення логічного зв'язку між відповідними протоколами різних комп'ютерних пристроїв застосування виникає необхідність також у застосуванні власних, спеціальних криптографічних кодів для кожного прикладного протоколу. Оскільки на одному комп'ютерному пристрої можуть бути встановлені різні прикладні протоколи, у залежності від обставин виникає потреба в обміні кількома криптографічними кодами між двома комп'ютерними

пристроями. З цієї причини може також виникнути потреба в обміні між двома комп'ютерними пристроями різними алгоритмами захисту від несанкціонованого доступу.

Надійний обмін кодами або підбір надійного алгоритму захисту від несанкціонованого доступу ґрунтується на взаємній автентифікації комп'ютерних пристроїв, що беруть участь у підборі або в обміні кодами перед процедурою обміну кодами або підбору алгоритму захисту від несанкціонованого доступу.

Зазвичай перед кожним підбором алгоритму захисту від несанкціонованого доступу або перед кожним обміном кодами здійснюється фаза автентифікації, під час якої відбувається взаємна автентифікація (тобто розпізнавання) комп'ютерних пристроїв.

При великій кількості процесів підбору алгоритмів захисту від несанкціонованого доступу або обміну кодами це призводить до виконання великої кількості автентифікацій, що пов'язано з великими витратами на акти комунікації і збільшенням потрібної потужності EOM.

Ця проблема додатково загострюється також у тому разі, коли акт комунікації відбувається не лише між двома комп'ютерними пристроями, а передбачається кілька комп'ютерних пристроїв, підпорядкованих різним доменам захисту. Під поняттям доменів захисту слід розуміти у цьому зв'язку певну кількість комп'ютерних пристроїв, що використовують спільні алгоритми захисту від несанкціонованого доступу.

У цьому разі автентифікація здійснюється зазвичай на рівні доменів захисту.

Огляд звичайних криптографічних методів, якими можна користуватись у цьому способі, поданий, наприклад, у документі "S. Muftic, Sicherheitsmechanismen für Rechnernetze (Механізми захисту від несанкціонованого доступу до обчислювальних мереж), Видавництво Carl Hanser Verlag, Мюнхен, ISBN 3-446-16272-0, с 34 - 70, 1992р."

Відомий варіант підбору алгоритмів захисту від несанкціонованого доступу під час акту комунікації між двома партнерами, проте при цьому підбір, що описується у цьому документі, обмежується лише незначною кількістю заздалегідь визначених параметрів "T. Kipp et al, The SSL Protocol (Протокол SSL), Internet Draft, Червень 1995р."

У документі "CHORLEY B. J. ET AL "The definition and implementation of a secure communications protocol" PROCEEDINGS OF THE INTERNATIONAL CARNAHAN CONFERENCE ON

SECURITY TECHNOLOGY, ZURICH, SWITZERLAND, 4-6 OCT 1983, ISBN 0-89779-057-X, 1983, LEXINGTON, KY, USA, UNIV KENTUCKY, USA", який за сукупністю ознак є найближчим аналогом, описується протокол, згідно з яким захищений запит між двома терміналами установлюється шляхом передавання множини параметрів, що визначають спосіб кодування, джерело ключа та будь-які зв'язані змінні. Це передавання реалізується шляхом надсилання терміналом, який запитує, початкового повідомлення з необхідними параметрами до терміналу, якому передбачений запит. Термінал, якому передбачений запит може просто прийняти параметри та увійти в режим закодованого тексту шляхом повернення Закодованого З'єднувального повідомлення Запиту або відхилити їх та закрити запит шляхом надсилання Запиту про Закриття. Альтернативно, параметри можуть бути прийнятими і повертаються деякі додаткові параметри (наприклад, коли в кожному напрямі використовується різний ключ). Навіть, альтернативна множина параметрів може повертатися завдяки тому, що початкова множина параметрів була деяким чином непринятною. В разі, коли додаткові параметри повертаються, термінал, який запитує може прийняти їх тільки шляхом повернення Закодованого З'єднувального Запиту або відхилити їх шляхом надсилання Запиту про Закриття. Окрім того є можливість приймати тестовий шаблон. Тестові шаблони використовуються для перевірки ідентичності терміналів, який запитує та якому передбачений запит. Тестовий шаблон зберігається, а відповідь надсилається після узгодження нових параметрів.

В основу винаходу покладено проблему створення способу для обміну кодами між двома комп'ютерними пристроями, у якому потрібні витрати на акт комунікації та потужність ЕОМ, необхідна для реалізації методу, є меншими, ніж для відомих способів.

Ця проблема вирішується за допомогою способу для криптографічного обміну кодами між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2),

у якому між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) здійснюється автентифікація,

у якому між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) відбувається підбір алгоритмів захисту від несанкціонованого доступу (SP),

який відрізняється тим, що

під час автентифікації між першим комп'ютерним пристроєм (C1) та другим комп'ютерним пристроєм (C2) відбувається обмін автентифікаторами ( $AR_A$ ,  $AR_B$ ), за допомогою яких забезпечується автентичність комп'ютерних пристроїв (C1, C2),

під час відбору алгоритму захисту від несанкціонованого доступу (SP) застосовується принаймні один з автентифікаторів ( $AR_A$ ,  $AR_B$ ).

У цьому способі здійснюється взаємна автентифікація двох комп'ютерних пристроїв, у межах якої відбувається обмін автентифікаторами між комп'ютерними пристроями. За допомогою автентифікаторів здійснюється обмін секретними даними між комп'ютерними пристроями, що дозволяє

здійснити автентифікацію комп'ютерних пристроїв. Після цього підбір алгоритму захисту від несанкціонованого доступу та/або обмін кодами між комп'ютерними пристроями здійснюється із застосуванням автентифікаторів.

Завдяки цьому способу немає потреби у проведенні явних фаз автентифікації між комп'ютерними пристроями для кожного нового процесу обміну кодами та/або відбору алгоритму захисту від несанкціонованого доступу. Наприклад, при використанні кількох прикладних протоколів значно зменшується кількість необхідних фаз автентифікації, оскільки автентифікацію між комп'ютерними пристроями слід виконувати лише один раз, а для усіх наступних операцій автентифікація комп'ютерних пристроїв відбувається неявно за допомогою автентифікаторів, що передаються.

Внаслідок цього суттєво зменшуються витрати, необхідні для обміну кодами між комп'ютерними пристроями, а також необхідний час обчислень ЕОМ.

Переважні варіанти втілення винаходу пояснюються у додаткових пунктах формули винаходу.

У разі групування кількох комп'ютерних пристроїв у домену захисту та автентифікації комп'ютерних пристроїв на рівні доменів захисту, яким підпорядкований відповідний комп'ютерний пристрій, досягається додаткова економія витрат, необхідних для здійснення акту комунікації, а також потрібна потужність ЕОМ. Це є можливим завдяки модульній структурі способу, оскільки явну фазу автентифікації слід здійснювати лише для одного відповідного пристрою комп'ютера одного домену захисту. Якщо здійснюється підбір іншого алгоритму захисту від несанкціонованого доступу та/або інший обмін кодами між іншими комп'ютерними пристроями відповідних доменів захисту, для яких вже відбувся двосторонній процес автентифікації, автентифікатори, обмін якими вже відбувся, при наступному підборі та/або наступному обміні кодами можуть використовуватися для неявної автентифікації інших комп'ютерних пристроїв.

Крім того, перевага іншого варіанту способу полягає у застосуванні геш-функцій, що базуються на симетричних криптоалгоритмах, оскільки утворювати геш-значення із застосуванням подібних геш-функцій можна дуже швидко. Завдяки цьому значно прискорюється процес виконання способу.

Завдяки використанню цифрових сигнатур, можна надійно та достовірно реалізувати цей спосіб.

Крім того, доцільно здійснювати фазу переривання з'єднання, у якій здійснюється стирання розділених секретних інформацій, наприклад, кодів, обмін якими відбувся, або автентифікаторів. При цьому додатково підвищується надійність способу, оскільки для інших комп'ютерних пристроїв не застосовуються жодні секретні інформації, які можна було б використати пізніше для зловживань. Крім того, фаза переривання з'єднання використовується для синхронізації комп'ютерних пристроїв, що беруть участь в акті комунікації. Іншим варіантом способу доцільним є послідовне стирання секретних інформацій, так що існує можливість повторного ієрархічного використання секретних даних, обмін якими вже відбувся,

наприклад, для іншого процесу обміну кодами. Це означає, наприклад, що на початку фази переривання з'єднання стираються коди з'єднання, обмін якими здійснюється для утворення логічного зв'язку під час акту комунікації, а алгоритми захисту від несанкціонованого доступу, що підбираються для прикладних протоколів, ще залишаються записаними. Тому при утворенні нового логічного зв'язку між прикладними протоколами комп'ютерних пристроїв потрібно лише здійснити обмін новими кодами між комп'ютерними пристроями. Секретні дані, обмін якими вже був здійснений, наприклад автентифікатори або застосований алгоритм захисту від несанкціонованого доступу, крім того, можна використовувати для нового логічного зв'язку.

Нижче спосіб пояснюється більш детально на прикладі варіанту способу за допомогою креслень. На фіг. 1 наведена схема послідовності операцій із зазначенням окремих етапів способу.

На фіг. 2 схематично зображений формат повідомлень, у якому доцільно передавати повідомлення, обмін якими відбувається у цьому способі.

У межах цього винаходу поняття криптографічного способу слід розуміти так, що поняття криптографічного способу охоплює всі способи для перевірки цілісності пакету даних DP, як некриптографічні, так і криптографічні, наприклад, Cyclic-Redundancy Check (CRC) (контроль за допомогою циклічного надлишкового коду).

На фіг. 1 наведений приклад реалізації способу, що пояснює суть винаходу. Як пояснюється далі, цей варіант способу ні в якому разі не слід розуміти як єдину можливість втілення винаходу. Варіанти окремих етапів наведеного способу відомі фахівцям і пояснюються далі.

На початку реалізації способу між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2 здійснюється автентифікація. Автентифікація відбувається у фазі автентифікації A.

Автентифікацію можна здійснювати, наприклад, згідно з стандартом X 509 для підвищення ефективності. При цьому процес автентифікації відбувається, наприклад, таким чином.

Від першого комп'ютерного пристрою C1 перший сертифікат Cert<sub>A</sub>, який включає у себе надійний, сертифікований надійною третьою інстанцією, захищений блоком сертифікації, відкритий код першого комп'ютерного пристрою C1, передається на другий комп'ютерний пристрій C2.

Далі перший комп'ютерний пристрій C1 додатково до першого сертифікату Cert<sub>A</sub> генерує перше повідомлення-сигнатура S1, яке утворюється з цифрової сигнатури і першого повідомлення N1 за допомогою секретного коду SK<sub>A</sub> першого комп'ютерного пристрою C1.

Перше повідомлення N1 включає у себе, наприклад, перша часова мітка та, перше випадкове число R<sub>A</sub>, яке у межах цього способу є однозначним, ідентифікатор I<sub>B</sub> другого комп'ютерного пристрою C2, у разі застосування механізму автентифікації X 509, наприклад, однозначного ідентифікатора другого комп'ютерного пристрою C2, у разі використання алгоритму захисту, що застосовується в описаному далі процесі підбору алгоритму захисту від несанкціонованого доступу, який по-

ширюється на весь домен захисту, специфікацію домену SDID, який підпорядкований другий комп'ютерний пристрій C1, а також автентифікатор AR<sub>A</sub> першого комп'ютерного пристрою, закодований відкритим кодом PK<sub>B</sub> другого комп'ютерного пристрою C2, що відповідає псевдокоду першого комп'ютерного пристрою C1.

Перший сертифікат Cert<sub>A</sub>, а також перше повідомлення-сигнатура S1 передаються на другий комп'ютерний пристрій C2.

Після оцінки (верифікації) першого повідомлення-сигнатури S1, що служить для запобігання різним спробам криптографічного злому, у другому комп'ютерному пристрої C2 генерується друге повідомлення-сигнатура S2 і передається на перший комп'ютерний пристрій C1.

Друге сигнатурне повідомлення S2 складається, наприклад, з таких компонентів:

другої часової мітки T<sub>B</sub>,

другого однозначного випадкового числа R<sub>B</sub>,

ідентифікатора I<sub>A</sub> першого комп'ютерного пристрою C1,

першого випадкового числа R<sub>A</sub>,

автентифікатора AR<sub>B</sub> другого комп'ютерного пристрою C2, закодованого відкритим кодом PK<sub>A</sub> першого комп'ютерного пристрою C1.

Із зазначених вище компонентів формується друге повідомлення N2, що визначається формуванням цифрової сигнатури із застосуванням секретного коду SK<sub>B</sub> другого комп'ютерного пристрою C2.

Секретні псевдокоди як автентифікатори AR<sub>A</sub> першого комп'ютерного пристрою C1 та AR<sub>B</sub> - другого комп'ютерного пристрою C2 у подальшому процесі виконання протоколу використовуються для забезпечення криптографічного з'єднання подальших фаз протоколу і протокольних повідомлень з фазою автентифікації. У разі застосування стандарту X 509 автентифікатор AR<sub>A</sub> першого комп'ютерного пристрою C1 може бути перенесений у поле, передбачене для "секретного біт-ряда".

Після прийому та оцінки, тобто верифікації другого повідомлення-сигнатури S2 у першому комп'ютерному пристрої C1 у першому комп'ютерному пристрої C1 генерується третє повідомлення-сигнатура S3, що передається на другий комп'ютерний пристрій C2.

Третє повідомлення-сигнатура S3 генерується із застосуванням секретного коду SK<sub>A</sub> першого комп'ютерного пристрою C1, за допомогою якого кодується третє повідомлення N3. Третє повідомлення N3 включає у себе принаймні один ідентифікатор I<sub>B</sub> другого комп'ютерного пристрою C2, а також друге випадкове число R<sub>B</sub>.

Проте, автентифікацію між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2 можна здійснювати будь-яким іншим способом, наприклад, із застосуванням принципу експоненціального обміну кодами, наприклад, так званого обміну Diffie-Hellmann. У разі застосування обміну кодами Diffie-Hellmann коди, обмін якими відбувається, використовуються безпосередньо як автентифікатори AR<sub>A</sub>, AR<sub>B</sub>, що використовуються у наступних фазах способу.

У фазі автентифікації A потрібно лише, щоб

між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2 відбувається надійний обмін автентифікаторами  $AR_A$ ,  $AR_B$ . Це означає, що необхідно тільки, щоб в обох комп'ютерних пристроях C1, C2 після фази автентифікації A в іншому відповідному комп'ютерному пристрої C1, C2 були присутні характеристичні секретні дані.

Після закінчення процесу автентифікації між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2 здійснюється підбір алгоритму захисту від несанкціонованого доступу, що використовується у наступному акті комунікації, та/або відбувається заміна криптографічного коду.

Далі детально пояснюється фаза підбору  $S_P$  алгоритму захисту від несанкціонованого доступу, а також фаза обміну кодами  $S_A$ . Проте, у варіантах способу передбачається виконання лише фази підбору  $S_P$  алгоритму захисту від несанкціонованого доступу або лише фази обміну кодами  $S_A$ . Спільне представлення обох фаз  $S_P$ ,  $S_A$  у наведеному варіанті способу використовується лише для більш наочного пояснення суті винаходу.

Фаза підбору алгоритму захисту від несанкціонованого доступу  $S_P$  може характеризуватись, наприклад, такими етапами:

За допомогою цього побудованого за модульним принципом протоколу можна здійснювати взаємну автентифікацію першого комп'ютерного пристрою C1 і другого комп'ютерного пристрою C2 для подальшого підбору алгоритму захисту від несанкціонованого доступу між першим комп'ютерним пристроєм C1 і другим комп'ютерним пристроєм C2, причому немає потреби у повторному проведенні фази автентифікації A. Це можливо завдяки застосуванню автентифікаторів  $AR_A$ ,  $AR_B$  у фазі підбору алгоритму захисту від несанкціонованого доступу  $S_P$  для неявної автентифікації комп'ютерних пристроїв C1, C2.

В іншому варіанті втілення способу алгоритм захисту від несанкціонованого доступу може поширюватись, наприклад, на всі домени захисту  $S1$ ,  $S2$ , причому визначається група EOM, підпорядкованих спільним алгоритмам захисту від несанкціонованого доступу.

Проте, алгоритм захисту від несанкціонованого доступу може поширюватись тільки на актуальне з'єднання між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2.

У першому комп'ютерному пристрої C1 генерується пропозиція алгоритму захисту від несанкціонованого доступу  $SP_A$ , що підлягає застосуванню, яка включає у себе алгоритм захисту від несанкціонованого доступу, що пропонується першим комп'ютерним пристроєм C1.

Пропозиція алгоритму захисту від несанкціонованого доступу  $SP_A$  кодується відкритим кодом  $HR_D$  другого комп'ютерного пристрою C2, завдяки чому дуже вразлива пропозиція алгоритму захисту від несанкціонованого доступу  $SP_A$  захищається від несанкціонованого прослуховування.

Крім того, принаймні для пропозиції алгоритму захисту від несанкціонованого доступу  $SP_A$ , ідентифікатора  $I_B$  другого комп'ютерного пристрою C2, а також автентифікатора  $AR_B$  другого комп'ютерного пристрою C2 застосовується геш-функція  $h$  ( ), за допомогою якої утворюється перше геш-

значення  $h$  ( $SP_A$ ,  $I_B$ ,  $AR_B$ ).

За допомогою першого геш-значення  $h$  ( $SP_A$ ,  $I_B$ ,  $AR_B$ ) гарантується автентичність першого комп'ютерного пристрою C1, а також пропозиції алгоритму захисту від несанкціонованого доступу  $SP_A$  для другого комп'ютерного пристрою.

Замість цього можна застосовувати асиметричну цифрову сигнатуру, внаслідок чого забезпечується достовірність повідомлення із відповідною цифровою сигнатурою.

Генерування геш-значення на базі симетричного криптографічного способу забезпечує перевагу, яка полягає у тому, що визначати геш-значення за допомогою симетричного криптографічного способу можна значно скоріше, ніж формувати цифрову сигнатуру.

У межах цього способу можна використовувати будь-які геш-функції, наприклад, спосіб MD4, MD5 або геш-алгоритм ISO10118. Застосування геш-алгоритму ISO10118 є особливо доцільним у разі наявності апаратного забезпечення для так званого симетричного способу кодування DES (Data Encryption Standard).

Закодована пропозиція алгоритму захисту від несанкціонованого доступу  $SP_A$ , а також перше значення  $h$  ( $SP_A$ ,  $I_B$ ,  $AR_B$ ) передаються на другий комп'ютерний пристрій C2, у якому здійснюється верифікація.

У відповідь на це на перший комп'ютерний пристрій передається підтвердження алгоритму захисту від несанкціонованого доступу  $SP_{AB}$ , закодоване відкритим кодом  $PK_A$  першого комп'ютерного пристрою C1. Далі, друге геш-значення  $h$  ( $SP_{AB}$ ,  $I_A$ ,  $AR_A$ ) генерується у другому комп'ютерному пристрої C2 і передається на перший комп'ютерний пристрій C1, причому друге геш-значення  $h$  ( $SP_{AB}$ ,  $I_A$ ,  $AR_A$ ) генерується принаймні за допомогою підтвердження алгоритму захисту від несанкціонованого доступу  $SP_{AB}$ , ідентифікатора  $I_A$  першого комп'ютерного пристрою C1, а також автентифікатора  $AR_A$  першого комп'ютерного пристрою C1.

Підтвердження алгоритму захисту від несанкціонованого доступу  $SP_{AB}$  включає у себе, наприклад, підтвердження акцептування надісланого першим комп'ютерним пристроєм C1 пропозиції алгоритму захисту від несанкціонованого доступу  $SP_A$ , або генерованої другим комп'ютерним пристроєм C2 власної пропозиції алгоритму захисту від несанкціонованого доступу. Якщо генерована другим комп'ютерним пристроєм C2 пропозиція алгоритму захисту від несанкціонованого доступу відрізняється від пропозиції алгоритму захисту від несанкціонованого доступу  $SP_A$  першого комп'ютерного пристрою C1, комп'ютерний пристрій C1 має належним чином переробити наступну пропозицію алгоритму захисту від несанкціонованого доступу, верифікувати її, перевірити і надіслати наступне підтвердження алгоритму захисту від несанкціонованого доступу на другий комп'ютерний пристрій C2.

Зміст повідомлень відповідає описаному вище способу. Фаза застосування  $S_P$  алгоритму захисту від несанкціонованого доступу може повторюватись ітеративно, поки перший комп'ютерний пристрій C1 і другий комп'ютерний пристрій C2 не "по-

годяться" з варіантом алгоритму захисту від несанкціонованого доступу, що підтримується обома комп'ютерними пристроями C1, C2

Фаза обміну кодами SA може бути реалізована, наприклад, за допомогою таких етапів

Від першого комп'ютерного пристрою C1 перше повідомлення про обмін кодами SA1 передається на другий комп'ютерний пристрій C2

Перше повідомлення про обмін кодами SA1 складається, наприклад, з таких компонентів

даних P про з'єднання, що застосовується, за допомогою якого репрезентується одне з кількох одночасно активних з'єднань,

числове значення  $C_{AB}$  першого комп'ютерного пристрою C1 для розподілу кодів та/або повідомлення про переривання з'єднання,

закодованого відкритим кодом PK\_B другого комп'ютерного пристрою C2 коду з'єднання k, який має застосовуватись у наступному способі, причому код з'єднання k є переважно симетричним кодом з'єднання, що застосовується у межах з'єднання P,

третього геш-значення  $h(k, P, C_{AB}, I_B, AR_B)$ , яке генерується принаймні за допомогою коду з'єднання k, даних з'єднання P, числового значення  $C_{AB}$ , ідентифікатора  $I_B$  другого комп'ютерного пристрою C2, а також автентифікатора  $AR_B$  другого комп'ютерного пристрою C2

У наступному варіанті способу також передбачається, що код з'єднання k представляє собою асиметричну пару кодів

Числове значення  $C_{AB}$  між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2 використовується для того, щоб розрізнити перший комп'ютерний пристрій C1 та другий комп'ютерний пристрій C2 для різних прогонів протоколу для одного з'єднання P. Внаслідок того що відповідне числове значення  $C_{AB}$ , що приймається, постійно має перевищувати останнє записане числове значення  $C_{AB}$ , можна розпізнавати спроби злому шляхом повторного відтворення даних, що прослуховуються

Перше повідомлення про обмін кодами SA1 верифікується другим комп'ютерним пристроєм C2 за допомогою третього геш-значення  $h(k, P, C_{AB}, I_B, AR_B)$ , код з'єднання k декодується за допомогою секретного коду SK\_B другого комп'ютерного пристрою C2, і генерується друге повідомлення про обмін кодами SA2, за допомогою якого підтверджується прийом та подальше застосування коду з'єднання k для з'єднання P першого комп'ютерного пристрою C1

Друге повідомлення про обмін кодами SA2 складається, наприклад, з таких компонентів

даних про з'єднання P,

четвертого геш-значення  $h(P, k, C_A, I_A)$ , що генерується принаймні за допомогою даних з'єднання P, коду з'єднання k, першого числового значення  $C_A$ , а також ідентифікатора  $I_A$  першого комп'ютерного пристрою C1

Таким чином можна просто і надійно здійснювати обмін кодами з'єднання, потрібними для реалізації способу, між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2, причому немає потреби повторювати фазу взаємної автентифікації і підбору алгоритму захисту від

несанкціонованого доступу Sp

Це можливо лише завдяки модульній структурі описаного вище способу, оскільки при модульній структурі можна відмовитись від окремих етапів або комбінувати їх між собою будь-яким чином

Крім того, у наступному варіанті способу за винаходом передбачено також можливість забезпечення криптографічного захисту переривання з'єднання Це можна здійснювати, наприклад, шляхом генерування у першому комп'ютерному пристрої C1 повідомлення про переривання з'єднання VAN і його передачі на другий комп'ютерний пристрій C2

Повідомлення про переривання зв'язку VAN включає у себе, наприклад, такі компоненти

дані про з'єднання P,

дані для ідентифікації повідомлення про переривання з'єднання VAN,

числове значення  $C_{AB}$ ,

п'яте геш-значення  $h(P, DR, C_{AB}, I_B, AR_B)$ , що може бути утворене, наприклад, за допомогою даних про з'єднання P, даних DR повідомлення про переривання з'єднання VAN, числового значення  $C_{AB}$ , ідентифікатора  $I_B$  другого комп'ютерного пристрою C2, а також автентифікатора  $AR_B$  другого комп'ютерного пристрою C2

Повідомлення про переривання з'єднання VAN верифікується другим комп'ютерним пристроєм C2, з'єднання переривається, і генерується, наприклад, повідомлення-підтвердження переривання з'єднання VACKN (сигнал підтвердження) у другому комп'ютерному пристрої C2, що передається на перший комп'ютерний пристрій C1

Повідомлення-підтвердження переривання з'єднання VACKN (сигнал підтвердження) включає у себе, наприклад, такі компоненти

дані про з'єднання P,

дані DA для ідентифікації повідомлення-підтвердження переривання з'єднання VACKN,

шосте геш-значення  $h(P, DA, C_{AB}, I_A, AR_A)$ , що може бути утворене, наприклад, за допомогою даних про з'єднання P, даних DA для ідентифікації повідомлення-підтвердження переривання з'єднання VACKN, числового значення  $C_{AB}$ , ідентифікатора  $I_A$  першого комп'ютерного пристрою C1, а також автентифікатора  $AR_A$  першого комп'ютерного пристрою C1

За допомогою даних DR, DA для ідентифікації повідомлення про переривання з'єднання VAN або повідомлення-підтвердження переривання з'єднання VACKN можна запобігти іншому використанню геш-значень при наступному вдосконаленні цього описаного вище способу Повідомлення про переривання з'єднання VAN та/або повідомлення-підтвердження переривання з'єднання VACKN додатково включають у себе дані про з'єднання P, яке використовується

Описані вище і представлені на фіг 1 фази A способу для автентифікації, процедури підбору SP пропозиції алгоритму захисту, обміну кодів SA, а також переривання з'єднання можна виконувати у будь-яких комбінаціях

В іншому варіанті способу передбачено, що на етапі переривання з'єднання стираються не всі секретні дані, обмін якими відбувся, але спочатку стирається тільки відповідний код з'єднання k, об-

мін яким відбувся, а, наприклад, обраний алгоритм захисту від несанкціонованого доступу та/або автентифікатори  $AR_A$ ,  $AR_B$  залишаються записаними у комп'ютерних пристроях C1, C2

Далі, у наступному варіанті способу передбачено послідовне стирання розділених секретних даних, тобто після стирання коду з'єднання к спочатку стирається відповідний обраний алгоритм захисту від несанкціонованого доступу і лише після цього - автентифікатори  $AR_A$ ,  $AR_B$

Спосіб може бути реалізований на етапі встановлення з'єднання або на етапі з'єднання між першим комп'ютерним пристроєм C1 та другим комп'ютерним пристроєм C2

В іншому варіанті способу передбачена передача окремих повідомлень у форматі повідомлень, структура якого зображена на фіг 2

У разі використання такого формату перед повідомленням, що підлягає передачі, розміщується поле заголовка KF

Описаний далі формат повідомлень у жодному разі не обмежується описаним вище способом, навпаки, його можна застосовувати в усіх криптографічних протоколах

Поле заголовка KF складається переважно з таких елементів

прапорця захисту (Security-Flag) SF довжиною принаймні один біт,

даних про з'єднання P,

даних про фазу PT фази A, SP, SA, яких стоїть відповідна інформація повідомлення,

числового поля Z, за допомогою якого повідомлення однозначно ідентифікується у межах відповідної фази A, SP, SA,

даних D, наприклад, адреси, який підпорядко-

ваний комп'ютерний пристрій C1, C2, що приймає повідомлення, та/або даних про домени захисту S1, S2, яким підпорядкований відповідний комп'ютерний пристрій C1, C2

Крім того, у полі заголовка KF в іншому варіанті способу, наприклад, на ділянці PT, задаються відповідні фази A, SP, SA, може бути розміщена принаймні одна інформація про алгоритми, що підлягають застосуванню у фазі A, SP, SA, наприклад RSA, MD5, MD4, DES, еліптичні характеристики-алгоритми та/або параметри, що слід використовувати в алгоритмах

Для цього достатніми є дані, розміщені у прапорці захисту SF, з першим логічним значенням для повідомлення, що підлягає криптографічній обробці, і другим логічним значенням для повідомлення, що не підлягає криптографічній обробці

З цієї причини в іншому варіанті способу передбачено, що прапорець захисту SF має довжину, що дорівнює тільки точно одному біту

Перевага числового поля Z полягає у тому, що у фазі A, SP, SA у принципі можна здійснювати обмін будь-якою кількістю повідомлень, і відповідне повідомлення у фазі A, SP, SA може бути однозначно ідентифіковане за допомогою числового поля Z

Перевага даних про фазу PT фази A, SP, SA у полі заголовка KF полягає у дуже простій можливості розширення усього способу за рахунок введення нових фаз, причому у дані про фазу PT потрібно ввести лише одне нове позначення. За допомогою даних про фазу PT можна також просто замінювати та/або стирати вже введені фази

Повідомлення розміщується у полі VL змінної довжини

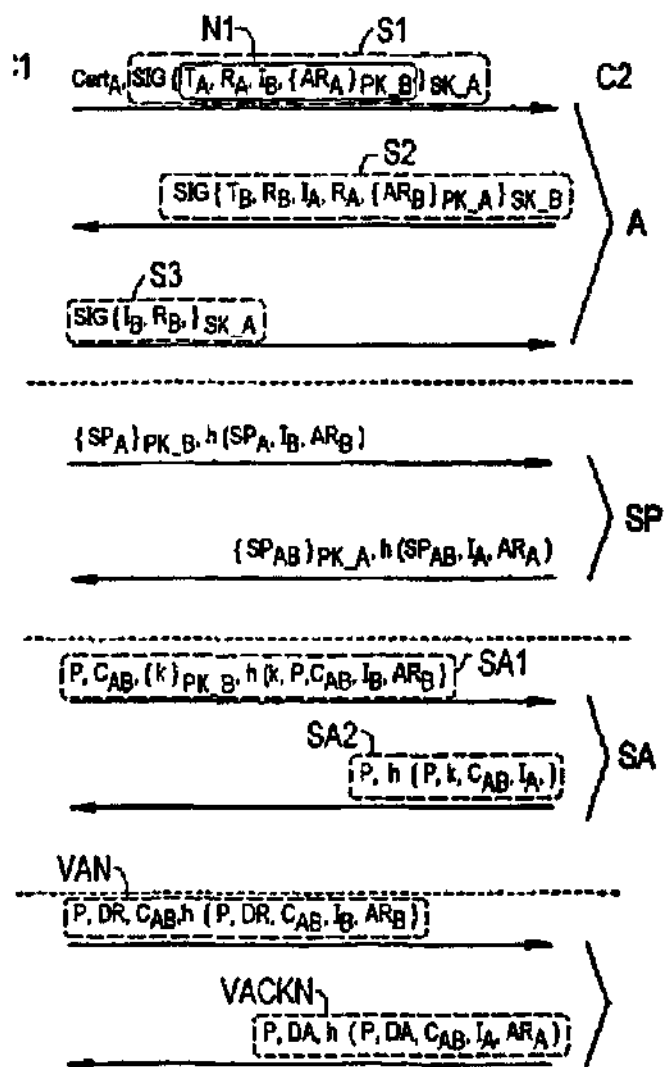


Fig 1

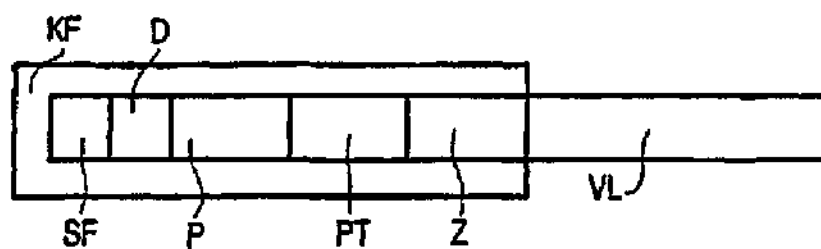


Fig.2