



УКРАЇНА

(19) UA (11) 56974 (13) A

(51) 7 H04L9/08, H04L9/32

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВИНАХІДВидається під
відповідальність
власника
патенту

(54) СПОСІБ ЗАБЕЗПЕЧЕННЯ ЖИТТЄДІЯЛЬНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

1

2

(21) 2003032517

(22) 24 03 2003

(24) 15 05 2003

(46) 15 05 2003, Бюл. № 5, 2003 р.

(72) Артеменко Віктор Іванович, Бобовкін Віктор Тихонович, Воробйов Юрій Євгенович, Згуровський Михайло Захарович, Прокофев Валентин Якович, Серпінко Іван Васильович

(73) НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(57) 1 Спосіб забезпечення життєдіяльності комп'ютерних мереж, що включає запис в банк даних інформації, зашифрованої одним із криптографічних методів, установлення вірогідного зв'язку з користувачем шляхом сертифікації його криптографічного ключа, який відрізняється тим, що всю інформацію, що занесена в банк даних, записують на зовнішні носії інформації, а при кожному сеансі зв'язку користувача з системою при сертифікації типу разового криптографічного ключа, сформованого та наданого йому на етапі реєстрації, визначають ознаку пріоритетності доступу та ознаку типу каналу, по якому користувач зв'язується з системою, протоколюють всі операції користувача і в разі введення користувачем неправильних даних, неправильності яких визначають, порівнюючи їх з даними, що містяться у банку

даних, роботу користувача з системою припиняють, визначають обсяг даних, якими користувач обмінюється з системою, тривалість обміну та кількість сеансів зв'язку користувача з системою і при перевершенні обсягу даних і часу обміну, а також кількості сеансів зв'язку, в кожному з яких використовують визначений при реєстрації одно-разовий сеансовий ключ, роботу користувача з системою припиняють

2 Спосіб за п. 1, який відрізняється тим, що перед передачею даних в канал зв'язку проводять їх безперервний аналіз, а передачу виконують окремими записами з одночасним розшифруванням та зашифруванням їх на сеансовому ключі, який отримують за криптографічним протоколом обміну ключами

3 Спосіб за п. 1, який відрізняється тим, що на основі протоколювання всіх операцій користувачів визначають інтенсивність (частоту та тривалість) використання ними записів даних і при її відсутності такі записи переписують на зовнішні носії інформації

4 Спосіб за п. 1, який відрізняється тим, що кожний наступний запис в банк даних виконують тільки після занесення попереднього запису на зовнішні носії інформації

Винахід відноситься до інформаційних технологій, зокрема до області передачі даних по комп'ютерних мережах, переважно таких, що обслуговують, як мінімум, окрему державну галузь, таку, наприклад, як освіту, податкову систему і т.і. В таких системах з використанням інформаційних технологій та комп'ютерних мереж однією з найголовніших вимог є забезпечення високої життєдіяльності та безперебійності функціонування при будь-яких умовах та збереження інформації, що знаходиться в цих системах

До таких способів ставляться досить суперечливі вимоги: необхідність застосування простих прийомів при експлуатації системи з надійним та безперебійним її функціонуванням

Удосконалення та розповсюдження складної комп'ютерної техніки та систем розподіленої обробки інформації привело до швидкого збільшення

об'ємів інформації, що передається в цифровій формі. Ця інформація використовується в фінансовій та банківській сфері, електронній пошті, електронному обміні даними та в других системах обробки даних. Передача цієї інформації по необладнаним та незахищеним каналам зв'язку пов'язана з вірогідністю піддати передану інформацію ризику електронного перехвату або перекрученню. Криптографічні системи забезпечують секретність таких передач, не допускаючи перегляду та змін інформації, не уповноваженими на це особами. Такі системи забезпечують цілісність передачі, не допускаючи підробок документів з електронними підписами

Відомий спосіб, що передбачає забезпечення життєдіяльності вищевказаних систем (див. патент України №41387, 7H04L9/08, 9/32, "Спосіб установа-лення вірогідного перевірюваного зв'язку спосіб

(13) A

(11) 56974

(19) UA

захищеного зв'язку, спосіб оновлення мікропрограмного забезпечення, спосіб здійснення шифрованого зв'язку та спосіб надання перевіреному на справжність пристрою права на проведення електронної трансакції" заявник СЕРТІКО ІНК., US, пріоритет 13 01 1995 року) Цей спосіб передбачає забезпечення життєдіяльності шляхом установа-лення вірогідного перевіреного зв'язку серед численності користувачів і містить операцію депонування, при цьому депонують в довіреному центрі збереження множини секретних асиметричних криптографічних ключів, що використовуються користувачами, перевіряють кожний з множини ключів в центрі збереження, сертифікують кожний з множини ключів після перевірки та ініціюють зв'язок кожним з численності користувачів з використанням відповідного одного з множини ключів в залежності від результатів сертифікації. Цей спосіб передбачає забезпечення життєдіяльності також шляхом установа-лення вірогідного перевіреного зв'язку між користувачами з операцією депонування, при цьому депонують в довіреному центрі збереження секретний асиметричний криптографічний ключ, що зв'язаний з кожним з численності користувачів, перевіряють кожний з цих ключів в центрі збереження, сертифікують кожний з цих ключів після перевірки та ініціюють захищений зв'язок користувача, що ініціює, з користувачем, що приймає, в залежності від результатів сертифікації ключів як користувача, що ініціює, так і користувача, що приймає. Крім того, з метою забезпечення життєдіяльності передбачено в даному способі оновлення мікропрограмного забезпечення шляхом вбудуванням ключів, що пов'язані з джерелом мікропрограмного забезпечення в пристрої, що підлягають перевірці на достовірність. Вказані заходи в деякій мірі забезпечують життєдіяльність комп'ютерних мереж.

Але відомий спосіб має недостаток, який полягає в тому, що він, по-перше, є порівняно складним і, по-друге, не забезпечує в достатній мірі життєдіяльність комп'ютерних мереж тому, що він не передбачає таких операцій, як періодичне оновлення інформації, що розташована в банку даних та яка протягом певного часу не використовується. У відомому способі також відсутній систематичний аналіз вихідної інформації та відсутнє постійне протоколювання кожного сеансу користувача з системою.

В основу винаходу покладена задача створення способу забезпечення життєдіяльності, який завдяки введенню нових операцій дозволяє забезпечити високу життєдіяльність комп'ютерних мережних систем, як при аварійних ситуаціях чи ситуаціях несанкціонованого доступу до інформації, так і її життєдіяльність з невизначено довгим часом її експлуатації.

Поставлена задача вирішується способом забезпечення життєдіяльності комп'ютерних мережних систем, що передбачає запис в банк даних шифрованої одним із криптографічних методів інформації, установа-лення вірогідного зв'язку з користувачем шляхом сертифікації його криптографічного ключа, згідно з винаходом, всю інформацію, що занесена в банк даних, записують на зовнішні носії інформації, а при кожному сеансі

зв'язку користувача з системою при сертифікації типу разового криптографічного ключа, сформованого та наданого йому на етапі реєстрації, визначають признак пріоритетності доступу та признак типу каналу, по якому користувач має право зв'язуватись з системою, протоколюють всі операції користувача і в разі вводу користувачем неправильних даних, неправильності яких визначають порівнюючи їх з даними, що містяться у банку даних, роботу користувача з системою припиняють, визначають кількість сеансів зв'язку користувача з системою і при перевершенні цієї кількості сеансів, в кожному з яких використовують визначений при реєстрації одноразовий сеансовий ключ, роботу користувача з системою припиняють. Перед передачею даних в канал зв'язку проводять їх безперервний аналіз, а передачу виконують окремими записами з одночасним розшифруванням та зашифруванням їх на сеансовому ключі, який отримують за криптографічним протоколом обміну ключами. На основі протоколювання всіх операцій користувачів визначають інтенсивність (частоту та тривалість) використання ними записів даних і при її відсутності такі записи переписують на зовнішні носії інформації. Кожний наступний запис в банк даних виконують тільки після занесення попереднього запису на зовнішні носії інформації.

Суть - пропонуємого способу детально буде проілюстровано на інформаційно-виробничій системі (IBC) "Освіта". IBC "Освіта" - це система, яка забезпечує створення єдиного інтегрованого інформаційного середовища держави в галузі освіти з використанням сучасних інформаційних технологій, що дозволяє створити єдину інформаційну інфраструктуру щодо обробки даних про освіту, забезпечити їх достовірність та цілісність, створити надійні механізми захисту інформації та обмеження доступу до неї, підвищити ефективність і якісно покращити умови праці для співробітників підрозділів міністерств та навчальних закладів.

В IBC "Освіта" вирішені основні проблеми, що забезпечують життєдіяльність всієї системи в цілому, а саме

захист конфіденційної інформації у базі даних, захист конфіденційної інформації у каналі зв'язку під час передачі її користувачу чи отримання такої інформації від користувача,

управління доступом користувачів до інформації системи

Конфіденційна інформація у базі даних ІОС "Освіта" зберігається у зашифрованому вигляді, що забезпечує належний рівень її захисту без застосування спеціальних програмних чи апаратних засобів захисту інформації під час зберігання та незалежність від використовуваних програмних засобів.

В IBC "Освіта" передбачена можливість збереження інформації у випадку аварійних ситуацій. Для цього забезпечена наявність функцій резервного копіювання інформації на зовнішні засоби збереження інформації. Передбачені також операції скидання і відновлення даних із зовнішніх носіїв інформації.

Захист конфіденційної інформації у каналі зв'язку під час передачі її користувачу чи отримання такої інформації від користувача забезпечується

передачею її у зашифрованому вигляді та використанням спеціальних захищених каналів зв'язку у випадках роботи з особливо важливою інформацією. Для встановлення зв'язку користувачів з системою формують банк даних користувачів, для кожного з яких формують признак пріоритетності доступу та признак типу каналу, по якому користувач має право зв'язуватись з мережевою системою, записують також значення логіна та пароль користувача, припустимі мережеві адреси, з яких користувачеві дозволено доступ в комп'ютерну мережеву систему, створюють і записують у банк даних користувачів криптографічні ключі та параметри криптографічних протоколів користувача, які використовують при ідентифікації та отриманні значень сеансових ключів, установлюють зв'язок користувача з системою по результатах виконання даних криптографічних протоколів, а при визначенні пріоритетності та типу каналу формують спільний з користувачем сеансовий ключ обміну даними.

Визначення інформаційних ресурсів ІВС "Освіта" доступних користувачеві - це визначення того, яка інформація може бути надана даному користувачу системи, або та яку інформацію він може передавати до ІВС "Освіта". При реєстрації користувача визначають з якою саме інформацією користувач має право працювати у системі, тобто визначають як саме співвідносяться запитувані ним повноваження на доступ до інформації з тими повноваженнями, що забезпечуються системою, та те, чи має він взагалі до неї право доступу. Зміст інформації, з якою може працювати користувач, та порядок взаємодії користувача з системою під час отримання чи передачі цієї інформації визначають тип доступу, який має користувач.

Порядок взаємодії користувача та ІВС "Освіта" регламентує те, яким чином (наприклад, буде він лише отримувати дані від ІВС "Освіта", чи буде передавати в ІВС "Освіта" свої дані) та через які канали зв'язку (наприклад, по внутрішній локальній комп'ютерній мережі, через виділені канали, або через Internet) він буде взаємодіяти з ІВС "Освіта". Це вирішується визначенням признаку каналу для кожного користувача.

Користувач має право працювати у системі певний проміжок часу. Після чого його повноваження можуть бути поповнені (після отримання від користувача додаткової інформації, що є підмножиною інформації, що надається при реєстрації у ІВС "Освіта") або припинені. Користувач також має обмеження на кількість сеансів роботи з системою. Така організація роботи системи ІВС "Освіта" дозволяє запобігти тим атакам на роботу системи, що використовують помилки користувачів (втрату чи неправильне використання засобів безпечної взаємодії з ІВС "Освіта" - ключів, програмних за-

собів нечасне надання чи ненадання інформації у ІВС "Освіта" про зміни у порядку їх роботи з ІВС "Освіта") або недостатню стійкість елементів системи забезпечення інформаційної безпеки ІВС "Освіта" на довготривалі деструктивні дії (наприклад, перебір зловмисниками паролів, адрес вузлів мережі, параметрів протоколів зв'язку та ін.).

Обсяг даних, якими користувач може обмінюватись у процесі взаємодії з ІВС "Освіта" та кількість сеансів обміну даними з користувачем обмежений. Таке обмеження дозволяє запобігати користувачам (або зловмисникам, що діють від імені користувачів) отримувати надлишкову інформацію, до якої вони мають доступ, але яка не потрібна для роботи. Також це обмеження дозволяє запобігати перевантаженню каналів зв'язку та системи марними запитами користувачів або великими обсягами даних, що надходять від користувачів.

Робота ІВС "Освіта" детально протоколюється на кожному етапі. Протоколювання системи ведеться в цілях контролю технічного стану складових системи, контролю роботи адміністратора системи, для виявлення спроб атак на систему (ззовні та зсередини - зареєстрованими користувачами), для виявлення некоректної роботи системи (збої, крах системи) та отримання даних для аналізу її причини, для отримання даних що можуть бути необхідні при відновленні стану системи після збою або краху (до стану останнього робочого стану), для збереження налаштувань системи (необхідно для забезпечення можливості не взаємодіючої роботи з системою декількох осіб, що виконують функції адміністратора).

Модульна структура системи реєстрації дозволяє модифікувати окремі елементи системи незалежно від інших елементів. Завдяки цій якості можливе поступове оновлення системи без втрати нею функціональності та без погіршення характеристик з точки зору захищеності системи. Можливе також незалежне відлагодження модулів системи та швидке виправлення помилок у програмній реалізації модулів у разі їх виявлення. Модульна структура системи також дозволяє легко та без додаткових витрат тимчасово (на короткий термін - за надзвичайних обставин чи у випадку збоїв у роботі) змінювати характеристики системи.

Таким чином, вказані вище особливості ІВС "Освіта" дозволяють в значній степені забезпечити її життєдіяльність в різноманітних умовах, не стандартних ситуаціях, а також в аварійних випадках.

Виробничі випробовування запропонованого способу забезпечення життєдіяльності в ІВС "Освіта" показали велику надійність функціонування системи. Майже повністю виключена можливість виведення системи з нормального режиму роботи.