



УКРАЇНА

(19) UA

(11) 58414

(13) A

(51) 7 H04L9/08, H04L9/32

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС

ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВИНАХІДВидається під
відповідальність
власника
патенту

(54) СПОСІБ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ВИРОБНИЧОЇ СИСТЕМИ

1

2

(21) 2003043543

(22) 18 04 2003

(24) 15 07 2003

(46) 15 07 2003, Бюл. № 7, 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 функціонування інформаційно-виробничої системи, що передбачає 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, при цьому з вказаних даних виділяють ототожнювальні дані, які використовують для виготовлення та ідентифікації стандартизованих обов'язкових для даної галузі документів, з ототожнювальних даних виділяють інформаційні дані, які наносять на документ при його виготовленні, 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 має право зв'язуватись з системою, протоколюють всі операції користувача і в разі вводу користувачем неправильних даних, неправильність яких визначають, порівнюючи їх з даними, що містяться у банку даних, роботу користувача з системою припиняють, визначають обсяг даних, якими кори-

стувач 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 одноразовий сеансовий ключ, роботу користувача з системою припиняють

2 Спосіб по п. 1, який відрізняється тим, що при виготовленні документа на нього наносять інформаційну частину даних одним із відомих технологічних процесів

3 Спосіб по п. 1 який відрізняється тим, що ідентифікацію документа проводять шляхом зчитування його інформаційної частини та порівняння її з інформаційною частиною даних, що міститься у відповідній ототожнювальній частині даних даного документа, записаній в банку даних системи

4 Спосіб по 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

5 Спосіб по 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

6 Спосіб по 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 управління окремими державними галузями, наприклад, освітою, податковою системою і т.п., за допомогою комп'ютерних систем, в яких крім збору, запису, обробки та передачі даних по комп'ютерних мережах, передбачено ще й виготовлення встановлених для цієї чи іншої галузі стандартизованих обов'язкових доку-

ментів, наприклад, документів про освіту, посвідчень працівників податкової служби, посвідчень водіїв транспортних засобів і т.п.

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,

(13) A

(11) 58414

(19) UA

що знаходиться в цих системах, виключення можливості несанкціонованого доступу до інформації, що зберігається в банках даних таких систем, забезпечення безпомилкової ідентифікації виготовлених документів та їх володарів, правомірність використання цих документів. Важливою вимогою є також встановлення надійного зв'язку між системою та користувачами, надійна передача інформації як до користувача, так і від користувача в систему.

Відомо, що 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 необладнаному та незахищеному каналу 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 функціонування системи зв'язку (див. патент України № 46055, 6Н04L 12/64, "Спосіб функціонування системи зв'язку (варіанти)" заявник СПРІНТ КОМ'ЮНІКЕЙШНЗ КОМПАНІ ЛП УС, пріоритет 08 09 1995 року, бюл. № 5, 2002 рік) для забезпечення викликів з використанням віртуального з'єднання, при якому користувач поміщає виклик шляхом передачі сигналізації для виклику до системи зв'язку і передача інформації користувача в систему конкретним з'єднанням за викликом, при цьому система містить АТМ (режиму асинхронної передачі) мультиплексор, що забезпечує міжмережовий обмін та процесор сигналізації, зв'язаний з АТМ мультиплексором, що забезпечує міжмережовий обмін, при цьому приймають сигналізацію для виклику у процесорі сигналізації, обробляють сигналізацію для виклику у процесорі сигналізації для вибору віртуального з'єднання, передають нову сигналізацію до АТМ мультиплексора, що забезпечує мережовий обмін, приймають інформацію користувача для виклику з конкретного з'єднання в АТМ мультиплексорі, перетворюють інформацію користувача з конкретного з'єднання на АТМ елементи даних, що ідентифікують вибране віртуальне з'єднання в АТМ мультиплексорі у відповідь на нову сигналізацію, та передають АТМ елементи з АТМ мультиплексора вибраним віртуальним з'єднанням.

Як видно з опису вказаного способу функціонування в ньому виконуються тільки функції прийому, обробки та передачі інформації і не передбачено виготовлення стандартизованих обов'язкових документів, які б характеризували б діяльність цієї системи в галузі управління, наприклад, областю зв'язку.

Відомий також спосіб функціонування інформаційної системи, що передбачає забезпечення життєдіяльності вищевказаних систем (див. патент

України № 41387, 7Н04L 9/08, 9/32, "Спосіб установавлення вірогідного перевірюваного зв'язку, спосіб захищеного зв'язку, спосіб оновлення мікропрограмного забезпечення, спосіб здійснення шифрованого зв'язку та спосіб надання перевірному на справжність пристрою права на проведення електронної транзакції" заявник СЕРТІКО ІНК, УС, пріоритет 13 01 1995 року) Цей спосіб передбачає забезпечення життєдіяльності шляхом установавлення вірогідного перевірюваного 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 чисельності користувачів з використанням відповідного одного з множини ключів в залежності від результатів сертифікації. Цей спосіб передбачає забезпечення життєдіяльності також шляхом установавлення вірогідного перевірюваного зв'язку між користувачами з операцією депонування, при цьому депонують в довіреному центрі збереження секретний асиметричний криптографічний ключ, що зв'язаний з кожним з чисельності 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 також недостаток, який полягає в тому, що він, по-перше, не має можливості виготовляти стандартизованих обов'язкових документів, які належать до тієї чи іншої галузі управління, не має можливості також ідентифікувати такі документи та визначати їх приналежність тому чи іншому володарю та їх правомірне використання, по-друге, не забезпечує в достатній мірі життєдіяльність системи 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. У відомому способі присутні тільки операції прийому, обробки та передачі інформації між користувачами. Все вищесказане обмежує функціональні можливості систем для використання їх в управлінні тією чи іншою галуззю.

В основу винаходу покладена задача створення способу функціонування інформаційно-виробничої системи, який завдяки введенню нових операцій дозволяє забезпечити високу життєдіяльність системи, як при аварійних ситуаціях чи

ситуаціях несанкціонованого доступу до інформації, так і її життєдіяльність з невизначено довгим часом її експлуатації, забезпечити можливість виготовлення стандартизованих обов'язкових документів для цієї чи іншої галузі, їх ідентифікацію, визначення власників таких документів та контролювати правильність їх використання, при цьому цей спосіб забезпечує інваріантність до виду виготовлених документів, що дозволяє використання систем з таким способом функціонування в різних галузях управління.

Поставлена задача вирішується способом функціонування інформаційно-виробничої системи, що передбачає запис в банк даних шифрованої одним із криптографічних методів інформації, установлення відповідного зв'язку з користувачем шляхом сертифікації його криптографічного ключа, всю інформацію, що занесена в банк даних, записують на зовнішні носії інформації, при цьому з вказаних даних виділяють ототожнюючі дані, які використовують для виготовлення та ідентифікації стандартизованих обов'язкових для даної галузі документів, з ототожнюючих даних виділяють інформаційні дані, які наносять на документ при його виготовленні, 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. Виготовлення документу виконують шляхом нанесення на нього інформаційної частини даним одним із відомих технологічних процесів ідентифікацію документу проводять шляхом зчитування його інформаційної частини та порівняння її з інформаційною частиною даних, що міститься у відповідній ототожнюючій частині даних даного документу, записаний в банку даних системи.

Сутність пропонуваного 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 технопо-

гій, 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 отриманні такої інформації від користувача,
- управління доступом користувачів до інформації системи.

Конфіденційна інформація у базі даних IBC "Освіта" зберігається у зашифрованому вигляді, що забезпечує належний рівень її захисту без застосування спеціальних програмних чи апаратних засобів захисту інформації під час зберігання та незалежності 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 отриманні 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 паролі 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 IBC "Освіта" доступних користувачеві - це визначення того, яка інформація може бути надана даному користувачу системи, або/та яку інформацію він може передавати до IBC "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 засобів, 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 обмінюватися 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 (збоїв, 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 взаємовиключної 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

Виготовлення документу виконують спідуючим чином. На підготовлену картку однією з відомих технологій наносять інформаційну частину даних. Інформаційна частина даних має для різних документів різну розмірність та зміст, але відповідає вимогам, що пред'являються до даного типу документів. Наприклад, інформаційна частина даних для документу "Студентський квиток" включає такі дані, як прізвище, ім'я та по-батькові, фотографію власника, назву вищого навчального закладу, курс навчання, назву групи, термін дії

Ототожнюючу частину даних, що містить в собі інформаційну частину (в тому числі цифрову фотографію) та додаткову частину даних заносять в банк даних системи. Додаткова частина даних формується під час виготовлення документів (заповнювач, час виготовлення документу та інш.)

Ідентифікацію документу проводять шляхом зчитування його інформаційної частини та порівняння її з інформаційною частиною даних, що міститься у відповідній ототожнюючій частині даних даного документу. 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 випробування запропонованого способу забезпечення життєдіяльності в ІВС "Освіта" показали велику надійність функціонування системи. Майже повністю виключена можливість виведення системи з нормального режиму роботи