



УКРАЇНА

(19) **UA** (11) **51101** (13) **U**
(51) МПК (2009)
H04L 9/08
H04L 9/32

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СПОСІБ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ВИРОБНИЧОЇ СИСТЕМИ

1

(21) u201004047

(22) 06.04.2010

(24) 25.06.2010

(46) 25.06.2010, Бюл. № 12, 2010 р.

(72) ПРОКОФ'ЄВ ВАЛЕНТИН ЯКОВИЧ, БОБОВКІН
ВІКТОР ТИХОНОВИЧ, ЗГУРОВСЬКИЙ МИХАЙЛО
ЗАХАРОВИЧ, ВОРОБІЙОВ ЮРІЙ ЄВГЕНОВИЧ,
СЕРГІЄНКО ІВАН ВАСИЛЬОВИЧ, АРТЕМЕНКО
ВІКТОР ІВАНОВИЧ

(73) ЗАКРИТЕ АКЦІОНЕРНЕ ТОВАРИСТВО "НАУ-
КОВО-ДОСЛІДНИЙ ІНСТИТУТ ПРИКЛАДНИХ ІН-
ФОРМАЦІЙНИХ ТЕХНОЛОГІЙ"

(57) 1. Спосіб функціонування інформаційно-виробничої системи, який полягає в тому, що користувач інформаційно-виробничої системи реєструють, при цьому користувач генерує ключову пару, відкритий криптографічний ключ користувача розміщують в блоці банку даних користувачів, встановлюють з'єднання між робочою станцією користувача та блоком банку даних інформації, інформацію зашифровують та розшифровують сеансовим ключем, який змінюють при кожному сеансі обміну інформацією, інформацію підписують електронним цифровим підписом, який створюють особистим криптографічним ключем користувача, в блок банку даних інформації записують інформацію, що надійшла від робочої станції користувача, протоколюють всі операції користувача, із зазначеної інформації виділяють ототожнюючу частину, яку використовують для виготовлення та ідентифікації стандартизованих обов'язкових для даної галузі документів, з ототожнюючої частини інформації виділяють інформаційну частину, яку наносять на картку документа при її виготовленні однією з відомих технологій, проводять вхідний та вихідний аналіз інформації на наявність суперечливої інформації, при виявленні суперечливої інформації, суперечливість якої визначають, порівнюючи її з інформацією того ж користувача, що

2

міститься у блоці банку даних інформації, сеанси обміну інформацією робочої станції користувача з блоком банку даних інформації припиняють, який **відрізняється** тим, що при реєстрації користувачу надають ідентифікатор доступу та пароль для роботи з інформацією його робочої станції, кожному користувачу надають особистий носій для зберігання особистого ключа, ключа шифрування, пароля та ідентифікатора доступу, при кожному сеансі зв'язку робочої станції користувача з блоком банку даних інформації по ідентифікатору доступу визначають ознаку пріоритетності доступу користувача, сеансовий ключ при передачі зашифровують ключем шифрування, суперечливу інформацію, виявлену при вхідному чи вихідному аналізі, відокремлюють, при перереєстрації користувача оперативно змінюють його особистий ключ, ключ шифрування, пароль та ідентифікатор доступу на особистому носії користувача у блоці актуалізації доступу.

2. Спосіб за п. 1, який **відрізняється** тим, що як особистий носій користувача використовують носій, який є незалежним автоматизованим пристроєм смарт-карткою.

3. Спосіб за п. 2, який **відрізняється** тим, що автоматизований пристрій смарт-картка має вбудовані засоби захисту інформації, що знаходяться на ньому.

4. Спосіб за п. 1, який **відрізняється** тим, що як ключ шифрування використовують відкритий ключ користувача.

5. Спосіб за п. 1, який **відрізняється** тим, що використовують зв'язок між логічно пов'язаними документами, при цьому перед виробленням картки певного документа перевіряють наявність в блоці банку даних інформації певної історії відповідних цьому документу та логічно пов'язаних з ним інших документів.

Корисна модель належить до галузі інформаційних технологій, зокрема до області передачі даних по комп'ютерних мережах, переважно таких, що обслуговують, як мінімум, окрему суспільну

галузь, таку, наприклад, як освіту, органи міського самоврядування і т.п.

З рівня техніки відомий спосіб функціонування інформаційно-виробничої системи [декларативний

(19) **UA** (11) **51101** (13) **U**

патент України на винахід №58414 А, H04L9/08, H04L9/32 «СПОСІБ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ВИРОБНИЧОЇ СИСТЕМИ», опубліковано 15.07.2003, бюл. № 7/ 2003 р.), обраний за найближчий аналог. Вказаний спосіб полягає у наступному:

Користувача інформаційно-виробничої системи реєструють, при цьому користувач генерує ключову пару. Відкритий криптографічний ключ користувача розміщують в блоці банку даних користувачів. Встановлюють з'єднання між робочою станцією користувача та блоком банку даних інформації, інформацію зашифровують та розшифровують сеансовим ключем, який змінюють при кожному сеансі обміну інформацією, інформацію підписують електронним цифровим підписом, який створюють особистим криптографічним ключем користувача. В блок банку даних інформації записують інформацію, що надійшла від робочої станції користувача, протоколюють всі операції користувача. Із зазначеної інформації виділяють ототожнюючу частину, яку використовують для виготовлення та ідентифікації стандартизованих обов'язкових для даної галузі документів. З ототожнюючої частини інформації виділяють інформаційну частину, яку наносять на картку документа при її виготовленні однією з відомих технологій, проводять вхідний та вихідний аналіз інформації на наявність суперечливої інформації. При виявленні суперечливої інформації, суперечливість якої визначають, порівнюючи її з інформацією того ж користувача, що міститься у блоці банку даних інформації, сеанси обміну інформацією робочої станції користувача з блоком банку даних інформації припиняють.

Недоліками вказаного способу є:

неможливість надання різних ознак пріоритетності доступу, недостатня захищеність сеансового ключа, недостатня надійність зберігання пароля та закритого ключа користувача, недостатня надійність зберігання суперечливої інформації, недостатня оперативність зміни особистого ключа, ключа шифрування, пароля та ідентифікатора доступу при перереєстрації користувача що призводить до зниження рівня захисту, достовірності та цілісності інформації банку даних інформації.

В основу корисної моделі, що заявляється покладена технічна задача створити такий спосіб функціонування інформаційно-виробничої системи, при якому за рахунок надання кожному користувачу ідентифікатора доступу, додаткового шифрування сеансового ключа ключем шифрування, зберігання особистого ключа, ключа шифрування, пароля та ідентифікатора доступу на особистому носії, відокремлення суперечливої інформації, виявленої при вхідному чи вихідному аналізі, оперативної зміни особистого ключа, ключа шифрування, пароля та ідентифікатора доступу при перереєстрації користувача у блоці актуалізації доступу досягається можливість зменшити вірогідність нанесення на картки документів невірної чи недостовірної інформації та, як наслідок підвищити рівень захисту, достовірності та цілісності інформації банку даних інформації.

Поставлена технічна задача досягається шляхом створення способу функціонування інформаційно-виробничої системи наприклад, при користуванні загальнодержавною інформаційно-виробничою системою в галузі освіти ІВС «ОСВІТА», який полягає в тому, що

Користувача інформаційно-виробничої системи реєструють, при цьому користувач генерує ключову пару. Відкритий криптографічний ключ користувача розміщують в блоці банку даних користувачів. Встановлюють з'єднання між робочою станцією користувача та блоком банку даних інформації, інформацію зашифровують та розшифровують сеансовим ключем, який змінюють при кожному сеансі обміну інформацією, інформацію підписують електронним цифровим підписом, який створюють особистим криптографічним ключем користувача. В блок банку даних інформації записують інформацію, що надійшла від робочої станції користувача, протоколюють всі операції користувача. Із зазначеної інформації виділяють ототожнюючу частину, яку використовують для виготовлення та ідентифікації стандартизованих обов'язкових для даної галузі документів. З ототожнюючої частини інформації виділяють інформаційну частину, яку наносять на картку документа при її виготовленні однією з відомих технологій, проводять вхідний та вихідний аналіз інформації на наявність суперечливої інформації. При виявленні суперечливої інформації, суперечливість якої визначають, порівнюючи її з інформацією того ж користувача, що міститься у блоці банку даних інформації, сеанси обміну інформацією робочої станції користувача з блоком банку даних інформації припиняють, згідно із запропонованою корисною моделлю, при реєстрації користувачу надають ідентифікатор доступу та пароль для роботи з інформацією його робочої станції. Кожному користувачу надають особистий носій для зберігання особистого ключа, ключа шифрування, пароля та ідентифікатора доступу. При кожному сеансі зв'язку робочої станції користувача з блоком банку даних інформації по ідентифікатору доступу визначають ознаку пріоритетності доступу користувача. Сеансовий ключ при передачі зашифровують ключем шифрування. Суперечливу інформацію, виявлену при вхідному чи вихідному аналізі відокремлюють. При перереєстрації користувача оперативно змінюють його особистий ключ, ключ шифрування, пароль та ідентифікатор доступу на особистому носії користувача у блоці актуалізації доступу.

Крім того, як особистий носій користувача переважно використовують носій, який є незалежним автоматизованим пристроєм смарт-карткою. Ця смарт-картка має вбудовані засоби захисту інформації, що знаходяться на ній.

Корисною моделлю також передбачено, що в деяких випадках як ключ шифрування використовують відкритий ключ користувача.

Крім того, в деяких випадках реалізації корисної моделі використовують зв'язок між логічно пов'язаними документами, при цьому перед виробленням картки певного документа перевіряють наявність в блоці банку даних інформації певної

історії відповідних цьому документу та логічно пов'язаних з ним інших документів.

Перераховані ознаки складають суть корисної моделі та забезпечують досягнення технічного результату - зменшення вірогідності нанесення на картки документів невірної чи недостовірної інформації та, як наслідок підвищення рівня захисту, достовірності та цілісності інформації банку даних інформації.

Причинно-наслідковий зв'язок ознак корисної моделі та технічного результату полягає в тому, що за рахунок надання кожному користувачу ідентифікатора доступу, додаткового шифрування сеансового ключа ключем шифрування, зберігання особистого ключа, ключа шифрування, пароля та ідентифікатора доступу на особистому носії, відокремлення суперечливої інформації, виявленої при вхідному чи вихідному аналізі, оперативної зміни особистого ключа, ключа шифрування, пароля та ідентифікатора доступу при перереєстрації користувача у блоці актуалізації доступу забезпечується можливість зменшити вірогідність нанесення на картки документів невірної чи недостовірної інформації та, як наслідок підвищити рівень захисту, достовірності та цілісності інформації банку даних інформації.

Запропонована корисна модель проілюстрована доданим кресленням, на якому зображено структурну схему системи, яка реалізує спосіб функціонування інформаційно-виробничої системи.

Запропонована корисна модель може бути реалізована за допомогою системи, що складається з:

блоку банку даних інформації 1, поєднаного з робочою станцією користувача 2, яка під час сеансу зв'язку поєднана з персональним носієм користувача (наприклад смарт-карткою) та блоком банку даних користувачів 3, який під час роботи пов'язаний з блоком банку даних інформації 1 та робочою станцією користувача 2. Блок банку даних користувачів 3 поєднаний з блоком актуалізації доступу 4. Блок банку даних інформації 1, крім того поєднаний з блоком виробництва документів 5.

Можливість здійснення способу функціонування інформаційно-виробничої системи буде проілюстровано на прикладі загальнодержавної системи в галузі освіти «ІВС «ОСВІТА»

Користувач ІВС «ОСВІТА», реєструє та розміщують відкритий криптографічний ключ цього користувача в блоці банку даних користувачів 3. Кожному користувачу ІВС «ОСВІТА» надають особистий носій, який є незалежним автоматизованим пристроєм смарт-карткою. При реєстрації користувача на його особистий носій старт-картку записують особистий ключ, ключ шифрування, пароль та ідентифікатор доступу. Сеансовий ключ створюється апаратно засобами особистого носія смарт-картки користувача. Це підвищує рівень захисту, достовірності та цілісності інформації банку даних інформації 1, оскільки перехоплення сеансового ключа та алгоритму його створення в цьому випадку неможливе. Смарт-картка має вбудовані засоби захисту інформації, що знаходяться на ній та які захищають інформацію картки (особистий

ключ, ключ шифрування, пароль та ідентифікатор доступу). Користувачу ІВС «ОСВІТА» надають пароль для роботи з програмними засобами його робочої станції 2, які призначені для збору інформації ІВС «ОСВІТА». При роботі із зазначеними програмними засобами користувач ІВС «ОСВІТА» вставляє свою смарт-картку в зчитувач робочої станції 2. Зчитувач автоматично розпізнає пароль користувача і його ознаку пріоритетності доступу. При встановленні зв'язку між робочою станцією користувача 2 та блоком банку даних інформації 1, інформацію зашифровують та розшифровують сеансовим ключем при кожному сеансі обміну інформацією. Сеансовий ключ при прийомі-передачі інформації додатково зашифровують відкритим ключем користувача як ключем шифрування для підвищення рівня захисту, достовірності та цілісності інформації банку даних інформації 1. Користувач підписує інформацію електронним цифровим підписом, який створює своїм особистим криптографічним ключем. В блок банку даних інформації 1 записують інформацію, що надійшла від робочої станції користувача 2, протоколюють всі операції користувача, із зазначеної інформації виділяють ототожнюючу частину, яку використовують в блоці виробництва 5 ІВС «ОСВІТА» для виготовлення та ідентифікації стандартизованих обов'язкових для галузі освіти документів про освіту державного зразка та студентських квитків державного зразка. З ототожнюючої частини інформації виділяють інформаційну частину (Прізвище, Ім'я, По-батькові, назва факультету, назва спеціальності, дата, тощо), яку наносять на картку документа про освіту чи студентського квитка при її виготовленні методом фотокомп'ютерних технологій. Ідентифікацію документа проводять шляхом зчитування його інформаційної частини та порівняння її з інформаційною частиною даних, що міститься у відповідній ототожнюючій частині даних даного документа. В державному реєстрі навчальних закладів ІВС «ОСВІТА» проводять вхідний та вихідний аналіз інформації на наявність суперечливої інформації про назву навчального закладу, прізвище керівника навчального закладу, назву спеціальності, ліцензований обсяг на певну спеціальність. При виявленні суперечливої інформації, суперечливість якої визначають, порівнюючи її з інформацією того ж користувача, що міститься у блоці банку даних інформації 1, роботу користувача з системою припиняють до усунення суперечливості. Виявлену суперечливу інформацію, відокремлюють. В ІВС «ОСВІТА» можлива додаткова перевірка достовірності інформації банку даних інформації при виготовленні документів про освіту. Для цього використовують зв'язок між логічно пов'язаними документами. При цьому перед виробленням картки документа про освіту для певної особи перевіряють наявність в блоці банку даних інформації 1 історії відповідних цьому документу про освіту та логічно пов'язаних з ним студентських квитків для цієї ж особи. При кожному сеансі обміну інформацією достовірність інформації підтверджується електронним цифровим підписом користувача ІВС «ОСВІТА», який реалізують за допомогою пари асиметричних ключів - відкритого

та особистого. ІВС «ОСВІТА» забезпечує високий рівень захисту, достовірності та цілісності інформації.

СПОСІБ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ВИРОБНИЧОЇ СИСТЕМИ

