



УКРАЇНА

(19) **UA** (11) **25459** (13) **U**
(51) **МПК (2006)**
G06F 11/30
G09B 7/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СИСТЕМА КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ НАВЧАЛЬНОГО ЗАКЛАДУ

1

2

(21) u200703422

(22) 29.03.2007

(24) 10.08.2007

(46) 10.08.2007, Бюл. № 12, 2007 р.

(72) Спірягін Максим Ігорович, Спірягін Валентин Ігорович, Белозьоров Євген Володимирович, Поляченко Олена Юріївна, Крамар Микола Максимович, Петров Олександр Степанович, Поляков Олександр Сергійович, Ключев Сергій Олександрович, Спірягін Костянтин Ігорович, Шохін Денис Віталійович

(73) СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

(57) Система керування доступом до інформаційних ресурсів навчального закладу, яка містить робочу станцію, сегмент локальної мережі або мережі Internet, сервер інформаційної бази даних, яка **відрізняється** тим, що як додатковий рівень захисту застосовано Smartcard та Card Reader для її технічного застосування, в системі встановлено сервер підтримки web- та ftp-технологій.

Корисна модель відноситься до обчислювальних та моделюючих пристроїв і може бути використана для рішення існуючих проблем захисту інформаційних ресурсів навчального закладу і організації доступу до них студентів та співробітників.

Відомо систему керування доступом до інформаційних даних мережі [див. United States Patent № US 6,988,138 B1, Int. Cl. G06F11/30, Appl. №09/608,208 date of Patent Jan. 17, 2006], яка містить робочу станцію, сегмент локальної мережі, сервер інформаційної бази даних. Цю систему обрано за прототип.

Недоліком відомої системи є низький рівень авторизації та аутентифікації користувача, а також неможливість роботи з інформаційними ресурсами через мережу Internet.

В основу корисної моделі поставлено задачу удосконалення системи керування доступом до інформаційних ресурсів мережі шляхом того, що пристрій забезпечено Smartcard та Card Reader для її технічного застосування, в наслідок чого поліпшиться процес авторизації та аутентифікації користувачів інформаційних ресурсів локальної мережі навчального закладу.

Поставлена задача досягається тим, що у системі керування доступом до інформаційних ресурсів навчального закладу, що містить робочу станцію, сегмент локальної мережі та сервер інформаційної бази даних, згідно корисної моделі, як додатковий рівень захисту систему споряджено

Smartcard та Card Reader для її технічного застосування, у системі також застосовано сервер підтримки web- та ftp-технологій.

Smartcard захищена від підробки, її неможливо скопіювати, тому що після персоналізації карти, ключі доступу ніколи і ніде не з'являються у відкритому виді, користувачі унікально ідентифікують і аутентифікують себе з використанням унікального імені користувача і пароля.

Суть корисної моделі пояснюється кресленням, де зображено структурну схему системи керування доступом до інформаційних ресурсів навчального закладу (Fig.), яка містить сервер інформаційної бази даних 1, сервер підтримки web- та ftp-технологій 2, сегмент локальної мережі навчального закладу 3 або мережі Internet 4, робочу станцію 5, Card Reader 6 для технічного застосування Smartcard 7.

Система керування доступом до інформаційних ресурсів навчального закладу функціонує наступним чином.

Кожен студент або співробітник навчального закладу одержує на руки персональну Smartcard 7, а також логін, пароль(пін-код). Перед початком роботи з інформаційними ресурсами навчального закладу користувач уставляє свою Smartcard 7 у Card Reader 6 будь-якої робочої станції 5, яка має підключення до сегменту локальної мережі навчального закладу 3 або мережі Internet 4. Клієнтська частина додатка програмного забезпечення визначає наявність Smartcard 7 в Card Reader 6 і

(13) **U**

(11) **25459**

(19) **UA**

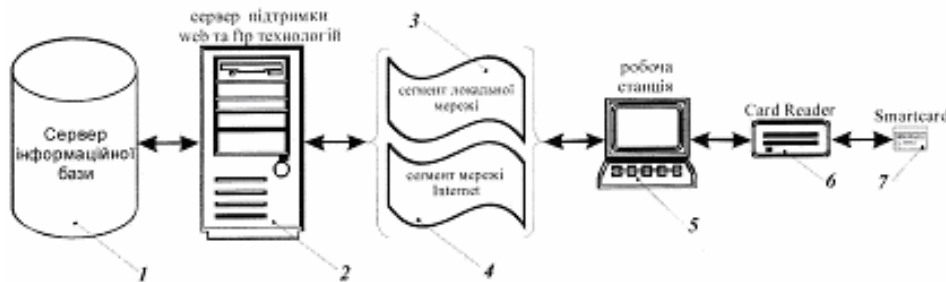
зчитує відтіля реєстраційні дані. Виконується базова перевірка цих даних (цілісність і т.п.), після чого додаток установлює захищене з'єднання за допомогою сервера 2 із сервером інформаційної бази 1. Введені з клавіатури дані авторизують Smartcard 7, після цього відправляється ключ користувача до серверу 1. У свою чергу, сервер 1 перевіряє наявність у базі даних користувачів подібного запису. Для підвищення захищеності системи паролі зберігаються у інформаційній базі даних у вигляді зашифрованих відбитків. Якщо подібний запис у базі знайдено, сервер 1 виконує також ряд додаткових перевірок (термін дії картки, рівень доступу та ін.). При проведенні сеансу доступу, сервер 1 перевіряє наявність дозволу на використання інформаційних ресурсів. Якщо користувача авторизовано успішно, сервер 1 передає клієнту необхідний дозвіл. Використання захищеного з'єднання зводить нанівель перехоплення даних. Клієнтська частина програмного забезпечення стежить за наявністю Smartcard 7 в Card Reader 6. У випадку витягу Smartcard 7 з Card Reader 6 з'єднання клієнта із сервером 1 розрива-

ється. У свою чергу, при проведенні сеансу з мережі Internet, сервер 1 стежить за тим, який термін дії картки надано користувачу. По закінченні цього терміну сервер 1 також розриває з'єднання.

У випадку витягу Smartcard 7 з Card Reader 6 з'єднання клієнта із сервером 1 розривається.

Система керування доступу до інформаційних ресурсів навчального закладу дозволяє:

- автоматизовано управляти і контролювати локальну мережу навчального закладу;
- надавати послуги Internet студентам і співробітникам;
- з'єднувати кілька комп'ютерних мереж кампусів у єдину керовану структуру з одним центральним сервером;
- розмежувати доступ до мережних ресурсів для операторів, адміністраторів та інших користувачів;
- організувати одночасну роботу безлічі користувачів у системі за допомогою сервера підтримки web- та ftp-технологій;
- використовувати мікропроцесорні Smartcard як студентські та читачькі квитки.



Фіг.