

УДК 378+ 681.324

Н.А. Кошева

Національна юридична академія України ім. Я. Мудрого, Харків

БЕЗПЕКА СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ

Кожна людина, що бажає здобути освіти дистанційно через Інтернет, повинна ідентифікувати себе яким-небудь чином або гарантовано забезпечити оплату рахунків за курси, що вивчаються. Також

вона повинна нести відповідальність за збереження отримуваних матеріалів, не порушувати авторські та інші права по наданих матеріалах. Необхідно запобігати можливості підміни користувача, саме для

цього слід володіти певними відомостями про особу слухача.

Методи реєстрації і аутентифікації залежать від систем аутентифікації / ідентифікації, вживаних в конкретній СДО.

На даний момент широкий розвиток в світі отримали наступні системи реєстрації/ аутентифікації користувачів (Декларація ЄС 1999г., NIST 800-63, APEC Framework 2007 і так далі):

- програмні (паролі, компоненти ПО та ін.);
- технічні (смарт-карти, електронні ключі типа eToken і т.п.);
- біометричні (сканери сітківки ока, відбитку пальця, долоні, голосу, клавіатурного почерку і ін.).

Перераховані системи розрізняються своєю вартістю, складністю реалізації, часом реєстрації нового користувача і аутентифікації або ідентифікації, вірогідністю помилкового приймання законного користувача за порушника, і навпаки, а також наявністю або відсутністю деяких специфічних функцій, безпосередньо не пов'язаних з операцією розпізнавання користувача. Також їх застосовність залежить від необхідності особистої реєстрації користувача в інституті. Наприклад, пароль можна передати по електронній пошті, а смарт-карту передати по віртуальному простору неможливо, то ж стосується біометричних параметрів людини.

Застосування смарт-карт, електронних ключів, біометричних засобів вимагає наявності спеціального зчитуючого обладнання. Останнім часом пристрої зчитування відбитку пальця вбудовують в маніпулятор-мишу, а сітківка ока може розпізнаватися за допомогою web-камери. Паролі при нинішньому розвитку обчислювальної техніки стали ненадійними, вони часто розкриваються. Натомість використання таких біометричних параметрів людини, як

голос або клавіатурний почерк, є надійним і недорогим способом ідентифікації користувачів.

Для ідентифікації по голосу необхідна наявність звукової плати, і, принаймні, мікрофону, тобто робоча станція має бути забезпечена мультимедіа-системою, вартість якої теж може бути невеликою.

При розпізнаванні по клавіатурному почерку жодного додаткового обладнання не потрібно, достатньо стандартної клавіатури.

У всіх випадках має бути реалізоване або куплене у сторонніх виробників ПО, що виконує функції реєстрації, аутентифікації користувачів, а також зберігання і обробки даних про користувачів системи, функціонує в глобальній мережі, подібній до Інтернету (найчастіше воно будується на клієнт-серверній архітектурі).

Оскільки більшість існуючих систем побудована на математичній моделі нейронних мереж, процес реєстрації займає значно більший період часу, чим розпізнавання користувачів. Оскільки активація нейронів у складі мережі здійснюється по деякій імовірнісній функції, існує певний відсоток можливої помилки як в ту, так і в іншу сторону.

Список літератури

1. Теренин А.А. Проблемы обеспечения безопасности систем дистанционного обучения / А.А. Теренин // Защита информации. Инсайд. – 2008. – № 4 (22). – С. 80-82.
2. Теренин А.А. Безопасность систем дистанционного обучения / А.А. Теренин // Защита информации. Инсайд. – 2008. – № 5 (23). – С. 86-89.
3. Теренин А.А. Создание защищенного канала передачи данных между распределенными ресурсами предприятия / А.А. Теренин // Защита информации. Инсайд. – 2005. – № 3. – С. 71-77.

УДК 004.853 (043.2)

С.В. Кунцев

Українська академія банківської справи Національного банку України, Суми

ТЕХНОЛОГІЯ РОЗРОБКИ ПРОГРАМ АНАЛІЗУ ДАНИХ ЗА ДОПОМОГОЮ АЛГОРИТМІВ DATA MINING БІБЛІОТЕКИ XELOPES

Сучасні інформаційні системи оснащуються аналітичними підсистемами – системами підтримки прийняття рішень (СППР). Згідно класифікації [1] розрізняють системи, засновані на телекомунікаціях і документах, на моделях, на даних і знаннях. Для аналізу даних і отримання нових знань в СППР використовують методи Data Mining. Найширше аналітичні технології Data Mining використовуються у галузі створення CRM-систем (11%), банківській справі (8%) і в маркетингу (5%) [2].

Основою для побудови СППР може служити програмний продукт компанії ZSoft [3] – бібліотека

Xelopes, яка є відкритим, незалежним середовищем з гнучкою архітектурою, яка призначена для вбудування в будь-яку інформаційну систему з метою забезпечення функціональності Data Mining. До складу бібліотеки Xelopes входять алгоритми "описові", які виконують пошук асоціативних правил і кластеризацію, і алгоритми "прогнозні", які виконують класифікацію і будують функцію регресії.

Проте, процес виявлення знань в даних є складним навіть за наявності відповідного програмного забезпечення. Очевидно, що для вирішення проблем потрібна ретельна підготовка фахівця-аналітика.