УДК 681.12

М.В. Коломієць

РОЗРОБКА ПРОГРАМИ АВТЕНТИФІКАЦІЇ ЗА ГОЛОСОМ ДЛЯ СИСТЕМ БЕЗПЕКИ

Вінницький національний технічний університет;

Анотація

В даній роботі розглянуто та досліджено системи безпеки обмеження доступу за допомогою біометричної ідентифікації, а саме автентифікації в системах безпеки за допомогою голосу. Досліджено процес автентифікації за голосом і на основі розроблено метод реалізації програмного продукту. При розробці програми, було використано математичні алгоритми побудови системи, процес порівняння зразків голосу, який включає в себе багатоетапний процес, та обрано оптимальну мову програмування і середовище де безпосередньо здійснювалася розробка програмного продукту для систем безпеки. Також було розглянуто практичне застосування розробки, а програмний продукт був перевірений шляхом тестування

Ключові слова: захист інформації; біометричні системи; аутентифікація за голосом.

Abstract

In this work is investigate security restrict access using biometric identification, such as authentication in security systems by voice. The process of authentication and voice based on the method of implementation of the software. In developing the program, used mathematical algorithms system of comparing samples to vote, which includes a multi-layered process, and selected the optimal programming language and environment which was carried directly Development of software for security systems. It was also considered practical application development and software product was tested by the test.

Keywords: information security; Biometric systems; voice authentication.

Вступ

У міру розвитку комп'ютерних мереж і розширення сфер автоматизації цінність інформації неухильно зростає. Державні секрети, наукові праці, комерційні, юридичні та лікарські таємниці все частіше довіряються комп'ютерним базам, які, як правило, підключені до локальних і корпоративних мереж. Популярність глобальної мережі Інтернет, з одного боку, відкриває величезні можливості для електронної комерції, але, з іншого боку, створює потребу в більш надійних засобах безпеки для захисту корпоративних даних від доступу ззовні.

Для доступу до системи потрібно застосовувати такі методи ідентифікації, які не працюють у відриві від їх носія. Цій вимозі відповідають біометричні характеристики людського організму. Сучасні біометричні технології дозволяють ідентифікувати особу за фізіологічними та психологічними ознаками.

Результати дослідження

Вхідними параметрами для програми ідентифікації користувача є його ідентифікатор, наприклад ім'я та прізвище або яке-небудь слово, і якийсь фрагмент безперервної мови. На основі цих даних може бути прийнято тільки два рішення:

- позитивне - користувач зареєстрований в системі і намагається увійти під своїм власним ім'ям;
- негативне - користувач не зареєстрований або ж він намагається отримати доступ по чужому ідентифікатору.

Розробляється система ідентифікації заснована на використанні ключового слова або фрази. Це дозволяє спростити алгоритм верифікації і, в той же час, зменшити число хибнопозитивних спрацьовувань, тому що кожен користувач може мати свою індивідуальну (секретну) фразу.

Завдання ідентифікації входять в одну з областей штучного інтелекту - розпізнавання образів. При цьому в якості способу розуміється сукупність деяких параметрів, що характеризують об'єкт. У даній роботі кожен фрагмент визначається тільки одним параметром - мірою його схожості з відповідним еталоном. При цьому міра подібності може змінюватися в інтервалі від 0 до 1. Чим ближче міра подібності до 1, тим більше спільного між досліджуваним фрагментом і відповідним йому еталоном.

Ознака утворює одномірний простір, який ділитися на дві частини. При попаданні параметра в них приймається відповідне рішення - позитивне або негативне. Хоча можливий поділ і на три області - позитивну, негативну і невизначеність , коли системі складно точно визначити приналежність користувача. В обох випадках значення кордонів розраховуються для кожного користувача окремо на етапі реєстрації.

У загальному вигляді система ідентифікації користувача складається з двох частин: етап реєстрації, що здійснюється лише один раз, і етап власної ідентифікації, який проводитися кожного разу, коли необхідно дати допуск.

На етапі реєстрації новий користувач вводить свій ідентифікатор, наприклад ім'я та прізвище, а потім вимовляє кілька разів ключове слово або фразу (створюються еталони). Число повторів ключової фрази може варіюватися для кожного користувача, а може бути постійним для всіх. Наприклад, в системі, що розробляється, число повторів було прийнято рівним трьом. Після попередньої обробки фрагменти попарно порівнюються, і на основі їх заходів подібності обчислюється значення кордону для поділу простору ознак. Найпростішою функцією для обчислення кордону можна прийняти пошук мінімуму або середнього арифметичного для результатів попарного порівняння еталонів.

На етапі ідентифікації користувач вводить або вибирає зі списку свій ідентифікатор і вимовляє ключову фразу. Після її попередньої обробки вона порівнюється з усіма фрагментами і обчислюється середня міра подібності. Якщо її значення менше значення кордону поділу для даного користувача, то приймається негативне рішення, в іншому випадку приймається позитивне рішення.

Для цього було розроблено програмне забезпечення для реєстрації користувачів і для входу в систему.

При тестуванні використовувалися 6 чоловічих голосів і 2 жіночих. Схожість голосів визначається у відсотках, тому потрібно з'ясувати максимально можливий поріг збігу. Еталонний голос використовувався чоловічий, тому для тестування використовувалася велика кількість саме чоловічих голосів.

Тестування проводилося на дуже слабкій звуковій карті інтегрованій в материнську плату. Картка з високим рівнем шуму і ігноруванням високих і низьких частот, а також зі слабким мікрофоном, який не забезпечує необхідний рівень запису. З хорошою звуковою підсистемою, можна домогтися значно кращих результатів.

Помилок в програмі в ході тестування виявлено не було.

Висновки

Розроблений програмний продукт дозволяє визначити легальність використання інформації, яка зберігається на комп'ютері, та надійність захисту від несанкціонованого використання. Також метод ідентифікації за голосом є простим для користувача та не вимагає додаткових маніпуляцій для встановлення та використання програмного забезпечення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. - Феникс, 2012 г. – 387 с.
2. Ю.Н. Хитрова, Применение речевой биометрии в системах ограничения доступа. [Электронный ресурс]: Режим доступа: http://www.e—expo.ru/docs/sp/cat/data/media/18_ru.pdf

Коломієць Марія Володимирівна — *студентка групи УБ-16м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: maria181mvk@gmail.com*

Науковий керівник: Яремчук Юрій Євгенович *— доктор технічних наук, професор кафедри менеджменту та безпеки інформаційних систем , Вінницький націо-нальний технічний університет, м. Вінниця*

Kolomiets Maria V.— *Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email : maria181mvk@gmail.com*

Supervisor: Yaremchuk Yuriy Y.— *DrSci, Professor of Management and Security of Information systems, Vinnytsia National Technical University, Vinnytsia*