4. Риндак В. Г. Проектна діяльність школяра в середовищі програмування Scratch / В. Г. Риндак. // навчально-методичний посібник. – 2009. – С. 116.
5. Таболкін Д. Інформатика: дитяча енциклопедія / Д. Таболкін. // Харків. – 2005. – С. 319.
6. Чепіль М. М. Педагогічні технології / М. М. Чепіль. // навчальний посібник. Київ. – 2012. – С. 224.

Адамішин Оксана
Науковий керівник – доц. Франко Юрій

ФОРМУВАННЯ ПРАКТИЧНИХ ВМІНЬ СТУДЕНТІВ МЕТОДАМИ ТА ЗАСОБАМИ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Аналіз останніх досліджень показав, що питання розвитку методів ідентифікації користувачів у системах дистанційного навчання розглянуті в багатьох роботах різних вчених. Наприклад, роботи Іванова А. І., Сорокіна І. А., Рибчинко Д. Є. присвячені дослідженню динамічних методів біометричної ідентифікації, зокрема, динаміці рукописного почерку та клавіатурного почерку [1, 3, 9]. У роботах Юркова П. Ю., Бабенко Л. К., Федорова В. М., Каткова О. Н., Дворянкина С. В. розглянуті методи динамічної біометричної ідентифікації за голосовим сигналом [1, 3, 5]. Роботи Диденко С. М., Шапцева В. А. присвячені дослідженню динамічних методів ідентифікації користувачів за почерком миші, зокрема за допомогою математичного апарату нейронних мереж [1, 2, 3]. Аналіз результатів дослідження свідчить про недостатню вивченість проблеми використання методів ідентифікації користувачів у системах дистанційного навчання в закладах освіти.

Мета статті – формування практичних вмінь студентів для дослідження залежностей між індивідуальними біометричними параметрами людини для її унікальної ідентифікації в системах дистанційного навчання.

Сьогодні однією з найактуальніших проблем вищої школи є психологічне обгрунтування організації індивідуального навчання в телекомунікаційному комп'ютерному освітньому середовищі. Тобто проблема верифікації за допомогою психофізичних параметрів має багато спільних точок дотику з проблемою індивідуальних технологій навчання.

Сучасні біометричні інформаційні системи та технології розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, образу обличчя, малюнка ліній долоні, райдужної оболонки, голосу) або поведінкових рис (підпису, ходи) [6-8].

Дистанційна освіта висуває певні вимоги до психологічних особливостей студента: по-перше, у нього повинна бути висока стійка мотивація до отримання освіти; по-друге, студент досить чітко повинен представляти бажаний результат навчання, по-третє, він повинен розуміти, що несе відповідальність за знання, отримані за допомогою системи дистанційного навчання (СДН).

Дистанційна освіта забезпечує людині вільний графік навчання, асоціюється з вільним відвідуванням сервера СДН. У зв’язку з цим, існує ймовірність того, що при тестуванні студент може посадити за комп’ютер замість себе більш обізнану в предметі людину. Навігаційна система дистанційної освіти повинна перевіряти, чи знаходиться за віддаленим комп’ютером саме той, якого навчають, за якого він себе видає, тобто, зробити розпізнавання користувача.

Яким чином сьогодні вирішується ця проблема, то це вимагає додаткових досліджень. Кожен вступник на навчання в системі дистанційної освіти людина отримує своє вхідне ім’я і пароль для входу на сервер з навчальними матеріалами. При зверненні студента до сервера про нього можна збирати інформацію, корисну для викладача: перелік сторінок, відвіданих користувачем за сеанс роботи; час, проведений на кожній сторінці; активовані гіперпосилання на даній сторінці; перелік файлів, які були скопійовані користувачем з навчального сервера; час тестування; та ін.

При необхідності адміністратор сервера системи дистанційного навчання може за допомогою інформації, що збирається відновити будь-який сценарій сеансу роботи будь-якого студента.

Але вся зібрана таким чином інформація є непрямою. Тобто, якщо в систему увійшов чоловік по вхідному імені та паролю свого колеги з метою відзначитися і взяти участь в

тестуванні, то його неможливо викрити. Іншими словами, потрібні прямі докази того, що даний сеанс навчання провів дійсно той користувач, з чиїм ім'ям зіставлене вхідне ім'я і пароль.

Вирішити цю проблему можна двома способами. Перший спосіб заснований на використанні додаткового апаратного забезпечення, він найбільш надійний, але пов'язаний з додатковими витратами, на які сьогодні, швидше за все, не піде жодна система дистанційної освіти, хоча все залежить від того, наскільки "відповідальні" знання отримує студент.

Додаткове апаратне забезпечення дозволяє здійснювати верифікацію по біометричних характеристиках людини: відбиток пальця; геометрія руки; райдужна оболонка ока; сітківка ока; голос людини; геометрія особи.

При всьому різноманітті біометричних методів в системах дистанційного навчання в основному використовуються три: розпізнавання за відбитком пальця, за зображенням особи (двохвимірному або тривимірному – 2D або 3D-фото) та за райдужною оболонкою ока. Однак будь-який з них заснований на зіставленні даних ідентифікованої об'єкта і біометричного еталона. Таке зіставлення неможливо без запису і збереження біометричної інформації, тобто без її документування [2,4].

Аналізуючи основні способи розпізнавання, які існують, на сьогоднішній день, можна зробити прогноз, що в системах дистанційного навчання вже в найближчому майбутньому почнуть застосовуватися програмні методи. Ці методики не змушують до додаткових витрат на придбання спеціального обладнання, вони цікаві педагогіці в тому плані, що аналізують психофізичний стан студента в поточний момент часу.

На основі аналізу сучасних біометричних систем розпізнавання людини у пропонується використати мультимодальну (бімодальну) систему ідентифікації, яка складається з двох характеристик: обличчя та голос.

Мультимодальна біометрична система ідентифікації, являє собою багатофакторну ідентифікацію персоналу, яка складається з двох основних статичних компонентів: ідентифікація за зображенням людини; ідентифікація за парольною фразою.

Ідентифікація за обличчям здійснюється в режимі реального часу в момент піднесення або підходу до пристрою з камерою. Для реєстрації та ідентифікації достатньо трьох зображень.

Ідентифікація за голосом проводиться на основі використання статичної парольної фрази. На етапі реєстрації фразу необхідно повторити декілька разів так досягається максимальна надійність і оцінюється варіативність виголошення.

Мультимодальне рішення являє собою узагальнення результатів, отриманих у ході голосової і лицьової ідентифікації. Результатом обробки цих модулів є математичні ймовірності подібності Голосу (Voice) та Обличчя (Face) еталонного зразка користувача, які надійшли на вхід аудіо/відео потоком. На основі цих величин розраховується мультимодальна ймовірність ідентифікації [5].

Мультимодальна система для ідентифікації, розпізнавання і авторизації об'єктів, об'єднала дві біометричні характеристики: голос і обличчя.

Спочатку було розроблено алгоритм роботи модуля зі звуком (голосом): включення пристрою, вибір режиму (запис еталона або ідентифікація), при виборі першого – відбувається прийом звукового стерео-сигналу, шумозаглушення і запис еталонної спектрограми; при виборі другого – пристрій приймає звуковий стерео сигнал у режимі реального часу, здійснює шумозаглушення і порівнює його з еталоном. У разі якщо запис не відповідає еталону, значить ідентифікований об'єкт не отримає доступ (рис. 1 а).

Потім було розроблено алгоритм роботи модуля з зображенням: включення пристрою, вибір режиму (збереження еталона або ідентифікація), при виборі першого – відбувається прийом 3D відеосигналу, накладення знімків і збереження еталонного зображення; при виборі другого – пристрій приймає 3D відеосигнал у режимі реального часу, здійснює накладення знімків і порівнює їх з еталоном. У разі якщо зображення особи не відповідає еталону, значить ідентифікований об'єкт не отримає доступ (рис. 1 б).

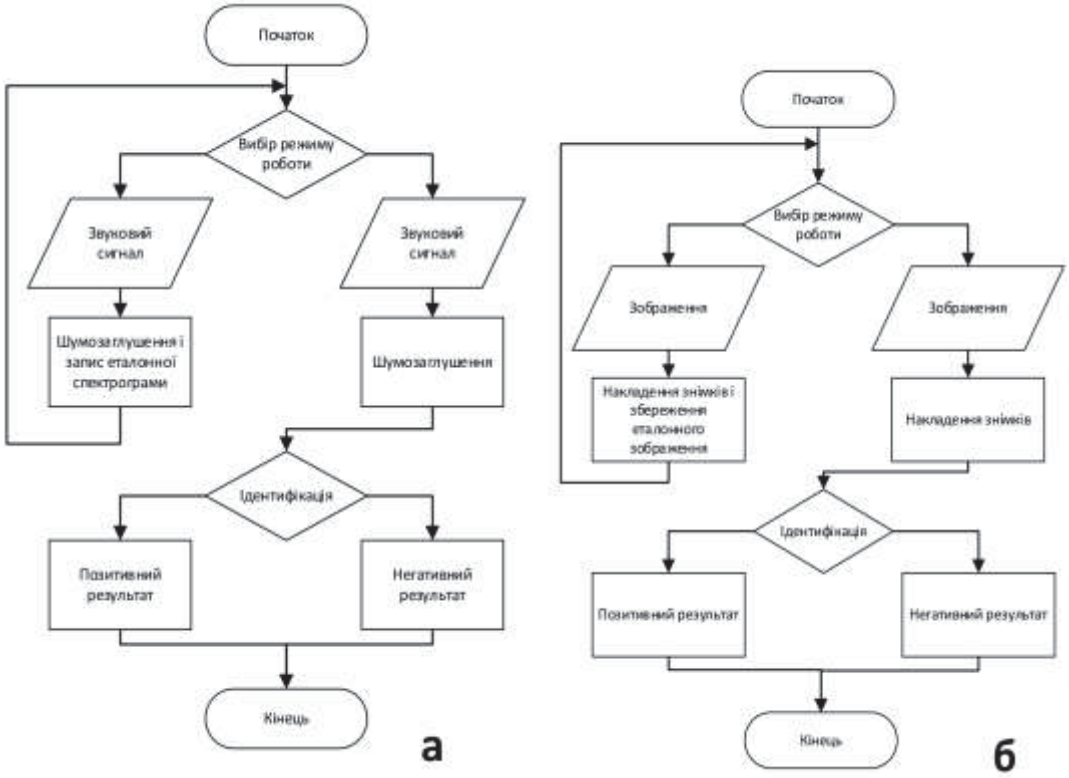


Рис. 1. Алгоритми роботи модулів звуку та зображення

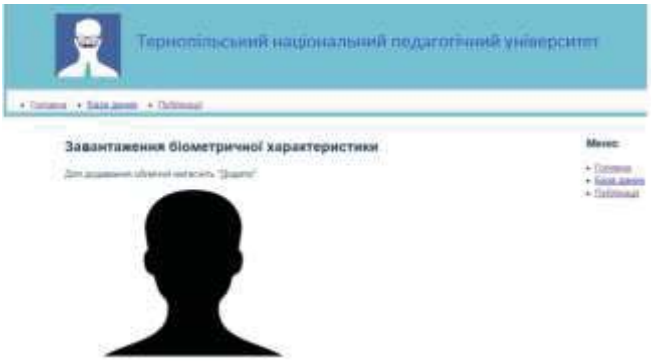
Для реалізації розробленого алгоритму створення еталону зображення та подальшого шифрування біометричних зразків використано сучасні мови Webпрограмування: HTML5 та JavaScript, а також спеціальну мову CSS (каскадні таблиці стилів), щоб візуально представити сторінки, написаних мовами розмітки даних. На рис. 2 представлено головну сторінку створеного сайту, який має наступну структуру сторінок: головна, БД, публікації та шифрування.

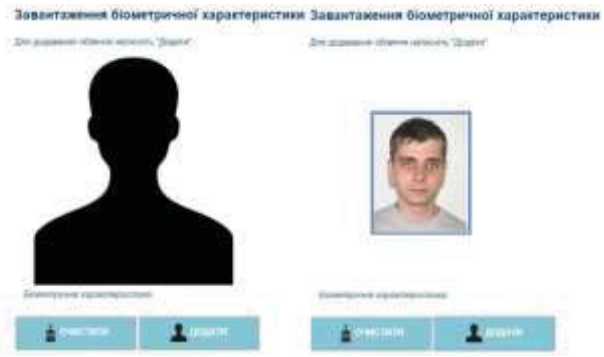
Рис. 2 Головна сторінка системи Рис. 3. Додавання характеристик

Першим кроком при роботі з сайтом є додавання біометричної характеристики для цієї дії необхідно натиснути кнопку «Додати», а для завантаження нової – «Очистити» (рис. 3). Після того, як біохарактеристика відобразиться у браузері, можна переходити до наступних кроків.

Другий та третій кроки – це знебарвлення та виділення області ідентифікації (рис. 4).

Четвертий крок – це виділення кордонів та додавання еталону до БД (рис. 5).





П’ятий, останній крок, реалізує шифрування еталона засобами CryptoJS (рис. 6).

Рис. 4. Попередня обробка

Рис. 5. Додавання еталону в базу даних

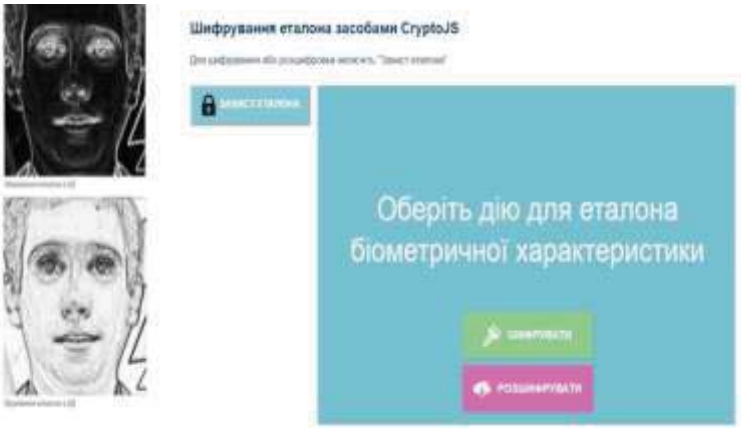


Рис. 6. Захист еталону

Проведено аналіз основних способів розпізнавання в системах дистанційного навчання.. Реалізовано розроблений алгоритм створення еталону біометричної характеристики, подальше її шифрування та зберігання шляхом використання сучасних мов Web-програмування: HTML5 та JavaScript, а також спеціальну мову CSS (каскадні таблиці стилів), щоб візуально представити сторінки, написаних мовами розмітки даних. Запропоновані методики не змушують до додаткових витрат на придбання спеціального обладнання, вони цікаві педагогіці в тому плані, що аналізують психофізичний стан студента в поточний момент часу.

ЛІТЕРАТУРА:

1. Газин А. И. Особенности голосовой аутентификации личности [Електронний ресурс] – 2010. – Режим доступу до ресурсу: cyberleninka.ru/article/n/osobennosti-golosovoy-autentifikatsii-lichnosti.pdf.
2. Прудник А. М., Власова Г. А., Я. В. Рощупкин. – Биометрические методы защиты информации /. – Минк: БГУИР, 2014. – 123 с.
3. Системи контролю доступу [Електронний ресурс]. – Режим доступу до ресурсу: http://www.npblog.com.ua/
4. Моржаков В., Мальцев А. Современные биометрические методы идентификации / БДИ. – 2009. – №2. 2012. – 123 с.
5. Мальцев А. Современные биометрические методы идентификации [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: https://habrahabr.ru/post/126144/
6. Медведев С. Ю. Преобразование Фурье и классический цифровой спектральный анализ [Електронний ресурс] / Вибродиагностика для начинающих и специалистов – Режим доступу до ресурсу: http://www.vibration.ru/preobraz_fur.shtml.
7. K.-R. Muller. S. Mika, G. Ratsch, K. Tsuda. and B. Scholkopf. An introduction to kernel-based learning algorithms, IEEE Transactions on Neural Networks, 12(2). pp. 181–201, 2001.
8. Nilsson M., Nordberg J., Claesson I. Face Detection Using Local SMQT Features and Split Up SNoW Classifier // Proceedings of IEEE Int. Conf. ICASSP, V. 2, P. 589–592, 2007
9. CryptoJS. JavaScript бібліотека криптографічних стандартів [Електронний ресурс] – Режим доступу до ресурсу: https://code.google.com/archive/p/crypto-js