УДК 004.56.53

Г.М. Кожушко, д.т.н.,професор,
Ю.Р. Зоураб, аспірант,
Р.О. Єрмілов, аспірант
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ВЕРИФІКАЦІЯ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ СУЧАСНИХ АПАРАТНИХ ПРИСТРОЇВ

В наш час, коли в системі вищої освіти часто застосовується дистанційне навчання, дуже важливим стає питання якості отриманих знань. Якщо при традиційній аудиторній системі освіти облік присутності студентів вести доволі просто, то при переході на дистанційну систему визначати дійсну присутність студентів стає доволі проблематичним. Особливо гостро це питання постає при проміжному та підсумковому тестуванні по дисциплінах. Завжди існує ймовірність, що при тестуванні за комп'ютером може знаходитися інша людина, яка більш свідома в даному предметі та має пароль для входження в систему. Тому важливим є спроможність системи дистанційної освіти (СДО) перевіряти, чи дійсно знаходиться за віддаленим комп'ютером той студент, що проходить тестування, тобто проводити верифікацію користувача.

Розглянемо найбільш відомі методи та засоби апаратного забезпечення, що дають можливість встановлення достовірності особи за біометричними характеристиками людини [1,2]. Треба враховувати, що для роботи системи потрібні деякі вкладення на придбання апаратури, тому важливо визначити надійний і прийнятний за ціною спосіб розпізнавання користувача в системі дистанційної освіти.

Сканування сітківки ока – відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Перевагою є надзвичайна складність підробки та відсутність безпосереднього контакту з обладнанням. Сканери для сітківки ока набули великого поширення в надсекретних системах контролю доступу, оскільки вони мають один із найнижчих відсотків відмови доступу зареєстрованих користувачів і майже 0 % помилкового доступу[3]. Пристрої цього класу є одними з найдорожчих – від 500 до 1000 $ і тому відносяться до найменш популярних. Очікувати на падіння вартості систем цього класу не доводиться, тому що в них використовуються відеокамери високої роздільної здатності. У СДО застосування цих методик малоймовірне.

Сканування відбитку пальця – перевагою розпізнавання є простота використання, зручність та надійність. Весь процес займає мало часу і не вимагає зусиль від тих, хто використовує систему доступу. Такий пристрій ідентифікації не потребує багато місця на клавіатурі чи механізмі, до того

ж багато сучасних смартфонів обладнані функцією зчитування відбитку пальця. Вартість окремого пристрою складає 80-100 $. До недоліків можна віднести безпосередній контакт з обладнанням.

Сканування долоні – переваги ідентифікації по геометрії долоні можна порівняти з плюсами ідентифікації за відбитком пальця у питанні надійності, хоча пристрій для зчитування відбитків долонь займає більше місця. Слід відмітити, що системи цього класу не висувають особливих вимог до чистоти, вологості та температури рук. Вартість пристроїв для ідентифікації користувачів з геометрії долоні більш висока у порівнянні з попереднім, і становить від 250 до 3000 $. Імовірність того, що цей спосіб колись використовуватиметься в СДО, дуже низька.

Голосова ідентифікація – привабливістю даного методу є зручність у застосуванні. Основним занепокоєнням, пов'язаним із цим біометричним підходом є точність ідентифікації. Однак це не є серйозною проблемою, тому що пристрої ідентифікації особистості по голосу розрізняють різні характеристики людської мови. В даний час голосова ідентифікація використовується для управління доступом до приміщення середнього ступеня безпеки, наприклад, лабораторії або комп'ютерного класу. Розпізнавання людини по голосу зручний, але в той же час не такий надійний, як інші біометричні методи, наприклад, людина з застудою або ларингітом може відчувати труднощі при використанні даних систем. Ідентифікація по голосу є традиційною для людей і не викликає психологічного неприйняття, іншими перевагами є невисока вартість обладнання (близько 50 $) та відсутність безпосереднього контакту.

Геометрія обличчя – один з найбільш швидко зростаючих напрямків у біометричній індустрії. Розвиток цього напряму пов'язаний із швидким зростанням мультимедійних відеотехнологій, завдяки яким можна побачити все більше відеокамер, встановлених вдома та на робочих місцях, або інтегрованих в комп’ютер чи смартфон.

Принцип роботи пристроїв цього класу дуже простий: мініатюрна відеокамера вводить зображення обличчя людини, що знаходиться перед комп'ютером. Програмне забезпечення порівнює введений портрет з еталоном, що зберігається в пам'яті[3]. Дуже важливим є те, що цей клас біометричних систем потенційно здатний здійснювати безперервну ідентифікацію користувача комп'ютера протягом усього сеансу його роботи, до того ж відеосистеми використовують для впізнання ті ж категорії, що й людина. Нарешті, результати останніх досліджень показують, що системи персональної ідентифікації, які ґрунтуються на аналізі відеоінформації, здатні забезпечити високий ступінь розпізнавання без розміщення користувача в строго контрольованій обстановці. Вартість пристроїв становить від 100 $ та вище.

Проаналізувавши переваги та недоліки вищеописаних методів, можна зробити висновок, що використання відбитка пальця для ідентифікації

особи в системі дистанційної освіти на даному етапі є найбільш надійним і прийнятним за вартістю з усіх біометричних методів.

Література

1. Kim H., Lee E.A. Authentication and Authorization for the Internet of Things //IT Professional. – 2018. – Т. 19. – №. 5. – С. 27-33.

2. Ali M. L. et al. Keystroke biometric systems for user authentication //Journal of Signal Processing Systems. – 2017. – Т. 86. – №. 2-3. – С. 175-190.

3. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. Випуск 6 (113). – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. – 320 с. С 215-223.

УДК 621.39

Н.М. Слепченко, аспірант,
О.В. Шефер, д.т.н., професор,
С.Г. Кислиця, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ПРОБЛЕМАТИКА ІНВАРІАНТНОСТІ СИСТЕМ ЗВ'ЯЗКУ СТОСОВНО ЗАВАД

Позначимо через $n = n(t)$ і $\xi = \xi(t)$ випадкові реалізації, що належать двом множинам завад N і Ξ відповідно. Довільну кількісну характеристику завадостійкості позначимо P, а ймовірність помилки $-p$. У загальному випадку характеристика завадостійкості є функцією обох завад:

$$P = P(N, \xi). \quad (1)$$

Цей запис означає, що розглянута характеристика завадостійкості являє собою результат усереднення по реалізаціях nзавади N, і є функцією параметрів множини N і реалізації ξ з множини Ξ.

Будемо називати *систему зв'язку абсолютно інваріантною стосовно завади* Ξ, якщо для усіх $\xi \in \Xi$ виконується рівність:

$$P(N, \xi) = P(N, 0) = P(N). \quad (2)$$

Еквівалентним цьому визначенню будемо вважати також запис:

$$P = in\,\mathrm{var}\,\Xi. \quad (3)$$

За відсутності завади N з умови інваріантості (2) випливає, що $P(N, \xi) = P(0, 0) = P(0)$. Якщо, наприклад, характеристикою завадостійкості є ймовірність помилки p, то $p = 0$. При цьому, звичайно, не має змісту розглядати такі тривіальні випадки, як, наприклад, обрив у прийомній антені, при якому ймовірність помилки дорівнює $1/2$ при будь-якій заваді (у тому числі і за її відсутності), і коли формально слід вважати