УДК 004.42

АУДЕНТИФІКАЦІЯ КОРИСТУВАЧА В АВТОМАТИЗОВАНИХ МІКРОПРОЦЕСОРНИХ СИСТЕМАХ

Литвинов В. А., Ніколаєв В. В., Голубєв Л. П.

Київський національний університет технологій та дизайну

Мета. *Дослідження методів автентифікації користувача в системах контролю доступу та розробка нового методу автентифікації.*

Методика. *У роботі використана методика автентифікації на базі магнітних карт і парольного захисту.*

Результати. *Розроблено автоматизовану систему контролю доступу на базі магнітних карт та парольного захисту.*

Наукова новизна. *Розроблено новий механізм автентифікації користувача в системах контролю доступу, заснований на магнітних картах та парольного захисту.*

Практична значимість. *Розроблений алгоритм автентифікації користувача є універсальним і може бути застосований при автентифікації користувача в різних мікропроцесорних системах. Розроблена автоматизована система контролю доступу використовує запропонований метод автентифікації користувача.*

Ключові слова: *автентифікація, система, контроль, доступ, магнітна карта, RFID-карта, парольний захист*

Ідентифікація дозволяє суб'єкту (користувачеві, процесу, що діє від імені певного користувача, чи іншого апаратно-програмного компоненту) назвати себе (повідомити своє ім'я). За допомогою автентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова «автентифікація» іноді використовують словосполучення «перевірка справжності».

Існує досить велика кількість способів автентифікації користувача. Автентифікація користувача може бути заснована на наступних принципах [1, 3]:

• на пред'явленні користувачем пароля;

• на пред'явленні користувачем доказів, що він володіє секретною ключовою інформацією;

• на відповідях на деякі тестові питання;

• на пред'явленні користувачем деяких незмінних ознак, нерозривно пов'язаних з ним;

• на надання доказів того, що він знаходиться в певному місці в певний час;

• на встановлення автентичності користувача деякої довіреної стороною.

Постановка завдання

Автентифікація з використанням пароля простий і найпоширеніший спосіб в комп'ютерних системах, іноді він застосовується і в сучасних системах контролю

доступу – клавіатурне введення кодів доступу. Мабуть, паролі – найбільш вразлива частина будь-якої комп'ютерної системи. Як би не була захищена система від атак по мережі або по комутованих лініях, від «троянських коней» і аналогічних небезпек, вона може бути повністю скомпрометована зловмисником, якщо той отримає до неї доступ через невірно введений пароль. Важливо сформувати правила вибору паролів, і довести їх до кожного користувача [2, 4].

Тому виникає необхідність створити комбінований метод автентифікації користувача на основі парольного захисту і магнітних карт.

Результати досліджень

Алгоритм розробленого методу полягає в наступному.

Після включення система знаходиться в очікуванні введення кодів користувачів. На екрані дисплея горить напис WAIT CARD.

Суперкористувач (користувач, що володіє максимальними правами) є і власником супер-ключа. Піднісши супер-ключ (спеціальну унікальну магнітну карту) привілейований користувач переводить систему в режим введення кодів користувачів. Суперкористувач послідовно підносить до card reader магнітні картки користувачів для реєстрації їх в системі. У разі успішної реєстрації на екрані дисплея виводиться повідомлення про записи інформації в незалежну пам'ять Arduino і номер комірки в яку записаний код користувача. Можна вводити до 50 кодів користувачів. Вихід з цього режиму здійснюється після закінчення введення кодів всіх користувачів або після натискання кнопки RESET на платі Arduino.

Під час запису кодів в EEPROM система шифрує коди магнітних карт відповідно до розробленого спеціального криптографічного алгоритму. При чому ключем до шифрування служить код магнітної карти суперкористувача.

Для входу в систему користувач може скористатися своєю магнітною карткою або ввести пароль з мобільного терміналу по протоколу Bluetooth. Користувач системи має 3 спроби введення пароля з мобільного пристрою, якщо він введе неправильний пароль система заблокує зв'язок з даним мобільним пристроєм.

Блок-схема системи автентифікації користувача приведена на рис. 1.

Розглянемо основні технічні компоненти системи.

Магнітна картка MIFARE.

MIFARE – торгова марка сімейства безконтактних смарт-карт. Торгова марка об'єднує кілька типів мікросхем смарткарт, мікросхеми зчитувачів і продукти на їх

основі. Власником торгової марки є NXP Semiconductors,яка вважається найбільш поширеною торговою маркою безконтактних смарт-карт в світі: продано більше 10 млрд. смарт-карт і 150 млн. зчитувачів.

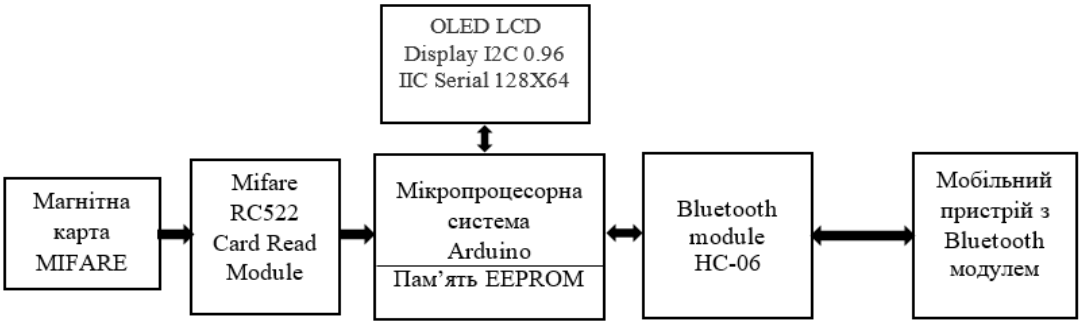

Рис. 1. **Блок-схема системи автентифікації користувача**

Система підтримує роботу з картами наступних форматів: MIFARE S50, MIFARE S70, MIFARE UltraLight, MIFARE Pro, MIFARE DESfire.

Технічні характеристики стандарту Mifare Classic.

• Об'єм пам'яті карти становить 1 або 4 КБ, стандарт EEPROM, батареї живлення не потрібно.

• Надійно розмежовані між собою 16 або 40 секторів, що підтримують багатофункціональне застосування. Кожен сектор має свій набір ключів доступу, що дозволяє розмежовувати доступ до різних програм.

• Кожен сектор складається з 4 блоків (3 інформаційних і 1 для зберігання ключів).

• Блок є найменшим компонентом, до якого адресується користувач, і складається з 16 байт.

• Термін зберігання даних в пам'яті до 10 років.

• До 100 000 циклів запису.

• Час, потрібний для отримання ідентифікаторів карти – 3 мс (старт, відповідь на запит, антіколлізія, вибір).

• Час зчитування 16-байтного блоку – 2,5 мс (без автентифікації), 4,5 мс (з автентифікацією).

• Повний зчитування карти + контрольне читання – хв. 8,5 мс (без автентифікації), хв. 10,5 мс (з автентифікацією).

• Типова операція з видачі квитка <100 мс, включаючи ідентифікацію карти, читання шести блоків (768 біт, 2 сектора автентифікації) і запис двома блоками (256 біт) з дублюванням.

Проведення операцій можливо, коли карта знаходиться в русі.

Модуль RC522 Card Read Module

HF RFID модуль RC522- цей пристрій для читання/запису міток і смарт-карт, яке використовує оригінальний чіп Philips MFRC522 і працює на частоті 13,56 МГц.

Модуль RC522 автоматично виявляє мітку, яка знаходиться в діапазоні зчитування і в режимі реального часу передає інформацію через один з логічних рівнів. Даний модуль містить всі необхідні для роботи компоненти, включаючи антену на друкованій платі.

RFID модулі RC522 можуть бути використані для інтеграції в платіжні і транспортні термінали, системи контролю доступу, вендингові апарати і ін. Крім цього є відмінною заміною настільних безконтактних зчитувачів для задач з інтеграцією в термінали [5].

Технічні характеристики RFID модуля RC522:

Робоча частота	13,56 МГц
Стандарт	ISO14443A
Підтримувані типи міток	Mifare: 1K, 4K, Ultralight, DESFire, Pro
Інтерфейс	SPI
Дальність зчитування	< 6 см
Максимальна швидкість передачі даних	10 Мбит/с
Робоча температура	от –20°C до +80°C
Розмір	40 × 60 мм

OLED LCD Display 0.96 IIC Serial 128X

OLED LCD Display I2C 0.96 IIC Serial 128X64 – це OLED монохромний 128 x 64dot матричний дисплей модуль з інтерфейсом I2C. в порівнянні з LCD, OLED-екрани є конкурентоспроможними із-за їх ряду переваг, таких як висока яскравість, почуття власного випромінювання, високий коефіцієнт контрастності, широкий кут огляду, широкий діапазон температур і низьке енергоспоживання. вони сумісні з Arduino / Arduino DUE / AVR / ARM.

Інтерфейс: I2C (3.3V / 5V логічний рівень)

Роздільна здатність: 128 * 64

Кут зору: > 160 градусів

Колір дисплею: білий

Джерело живлення: DC 3.3V ~ 5V

Робоча температура: –20 'C ~ 70'C

Застосування: пристрої автоматизації, смарт-годинник, MP3, термометр, інструменти, DIY проекти і т. д.

Bluetooth-модуль HC-06

Bluetooth модуль HC-06 для підключення Arduino до інших пристроїв по bluetooth. Модуль працює в пасивному режимі, тобто потрібно задати пошук на керуючому (Master) пристрої (ноутбук, телефон), знайти пристрій (за замовчуванням його ім'я linvor), після цього в Майстер-пристрої з'явиться послідовний порт, все що буде послано в нього з'явиться на вашому Arduino, і навпаки, все що Arduino надішле вам буде прийнято на вашому комп'ютері. Якщо необхідно можна змінити параметри модуля за допомогою AT команд.

Характеристики Bluetooth HC-06

Напруга живлення 3.3 - 6 В

Максимальна вхідна напруга логічної одиниці 5 В

Вихідна напруга логічної одиниці 3.3 В

Максимальний струм споживання 45 мА

Швидкість передачі даних 1200-1382400 бод

Дальність зв'язку при прямій видимості 30 м

При створенні автоматизованої системи автентифікації користувача був розроблений скетч для мікропроцесорної системи Arduino, який реалізує функції роботи з RFID-ключами [6, 7].

Нижче наведено фрагмент програми роботи з RFID-ключами.

```
void setup () {
  Serial.begin (9600); // Initialize serial communications with the PC.
  Serial.println ( "Prilozhite kartu / Waiting for card ...");
  SPI.begin (); // ініціалізація SPI / Init SPI bus.
  mfrc522.PCD_Init (); // ініціалізація MFRC522 / Init MFRC522 card.
}
void loop () {
  // Пошук нової картки / Look for new cards.
  if (! mfrc522.PICC_IsNewCardPresent ()) {
    return;
  }
  // Вибір картки / Select one of the cards.
  if (! mfrc522.PICC_ReadCardSerial ()) {
```

```
  return;
}
uidDec = 0;
// Видача серійного номера картки "UID".
for (byte i = 0; i <mfrc522.uid.size; i ++)
{
  uidDecTemp = mfrc522.uid.uidByte [i];
  uidDec = uidDec * 256 + uidDecTemp;
}
Serial.println ( "Serijnyj nomer karty / Card UID:");
Serial.println (uidDec);
// ------------------------
// починаємо порівнювати номер "UID", піднесеної до рідера карти,
// з записаним номером "UID" карти в sketch.
if (uidDec == XXXXXXXXXX) // якщо "UID" номер збігся.
{
  // включимо світлодіод.
  digitalWrite (ledPins [0], HIGH);
  // Друкуємо в Serial монітор.
  Serial.println ( "Hi Dmitry");
}
```

Зв'язок системи з мобільним пристроєм забезпечує Android-програма, розроблена з використанням технології MIT App Inventor.

Фрагмент програми, що реалізовує Bluetooth-з'єднання наведено нижче (рис. 2).

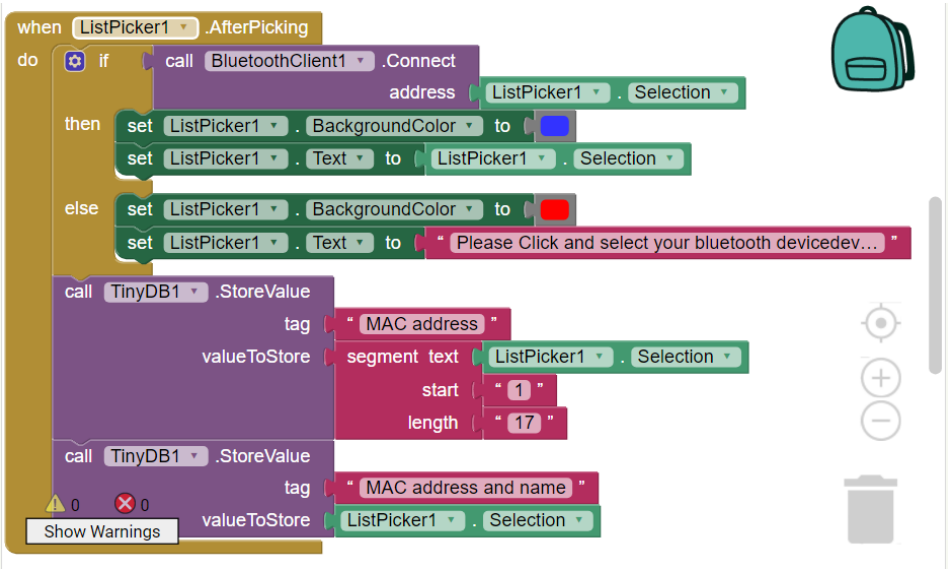

Рис. 2. **Фрагмент Android-програми, що реалізовує Bluetooth-з'єднання з мобільним пристроїм**

Процедура установки Bluetooth-з'єднання представлена на рис. 3.

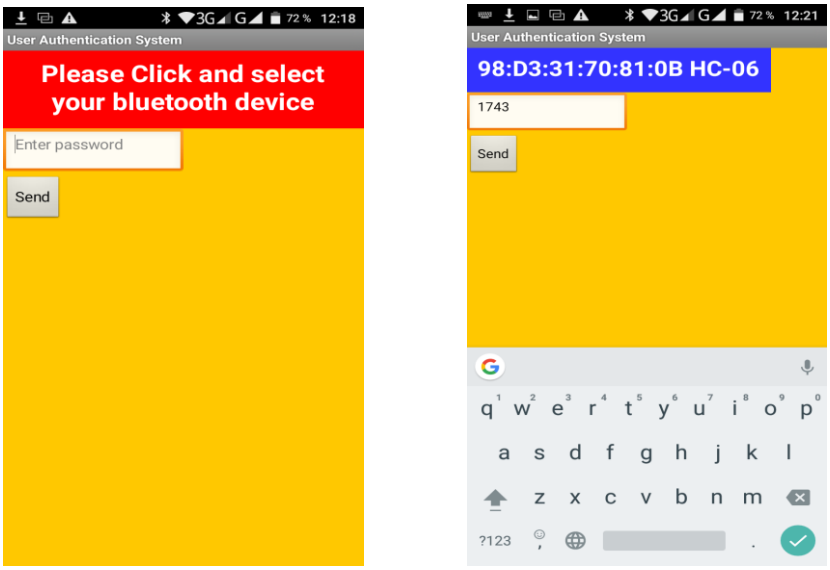

Рис. 3. **Установка Bluetooth-з'єднання на екрані мобільного терміналу**

Висновок

Таким чином розроблений новий комбінований механізм автентифікації користувача при роботі з мікропроцесорними системами. Застосовано унікальний алгоритм шифрування даних, заснований на операціях алгебри логіки і де в якості ключа використовується код RFID-ключа суперкористувача системи.

Розроблена система дозволяє здійснювати автентифікацію користувача мікропроцесорної системи як за допомогою RFID-карт, так і за допомогою пароля, використовуючи мобільний термінал.

Розроблений механізм автентифікації користувача є універсальним і може бути застосований в будь-яких автоматизованих мікропроцесорних системах - в виробничих системах, системах контролю управління доступом, системах відеоспостереження, системах управління складськими запасами і т. д.

Список використаних джерел

1. Петин В. Arduino и Raspberry Pi в проектах Internet of Things. / В. Петин – СПб. : БХВ-Петербург, 2016. – 320 с.
2. Соммер У. Программирование микроконтроллерных плат Arduino/Freeduino / У. Соммер – СПб. : БХВ-Петербург, 2015. –

References

1. Petin, V. (2016). *Arduino i Raspberry PI v proektah Internet of Things* [Arduino and Raspberry PI in Internet of Things projects] St. Petersburg: BHV-Peterburg [in Russian].
2. Sommer, U. (2015). *Programmirovanie mikrokontrollernyh plat Arduino / Freeduino* [Programming of microcontroller cards Arduino / Freeduino]. St. Petersburg: BHV-

256 с.
3. Можчиль Б. В. Использование микропроцессоров при создании автоматизированных систем управления / Б. В. Можчиль, Є. Ю. Фетисенко, Л. П. Голубев. // Технології та дизайн. – 2016. – № 3. – Режим доступу: http://nbuv.gov.ua/UJRN/td_2016_3_6
4. Голубєв Л. П. Розробка автоматизованої системи визначення спеціальності навчання за результатами ЗНО / Л. П. Голубєв, Д. А. Макатьора // Вісник КНУТД. – К. : КНУТД, 2016. – № 2. – С. 106-113.
5. Столяров В. Г. Автоматизированное удаленное управление устройствами при помощи Ардуино / В. Г. Столяров, Л. П. Голубев. // Технології та дизайн – 2016. – № 4. – Режим доступу: http://nbuv.gov.ua/UJRN/td_2016_4_12
6. Офіційна документація проекту Arduino [Електронний ресурс]. Режим доступу: http://www.arduino.ru
7. Авторські матеріали з сайту «Паяльник» [Електронний ресурс]. Режим доступу: http://geektimes.ru/

Peterburg [in Russian].
3. Mozhchil', B.V., Fetisenko, E.U., Golubev, L.P. (2016). *Ispol'zovanie mikroprocessorov pri sozdanii avtomatizirovannyh sistem upravleniya* [The use of microprocessors in the creation of automated control systems]. *Tekhnologiï ta dizajn – Technology and design 3(20).* Retrieved from: http://nbuv.gov.ua/UJRN/td_2016_3_6 [in Ukraine].
4. Golubev, L.P., Makat'ora, D.A. (2016). *Rozrobka avtomatizovanoï sistemi viznachennya special'nosti navchannya za rezul'tatami ZNO* [Development of an automated system for determining the specialty of training on the results of external testing] Visnik KNUTD – Bulletin of the KNUTD. Kyiv: KNUTD, 2(95), pp. 106-113. [in Ukraine].
5. Stolyarov, V. G., Golubev, L.P. (2016). *Avtomatizirovannoe udalennoe upravlenie ustrojstvami pri pomoshchi Arduino* [Automated remote device management with Arduino]. *Tekhnologiï ta dizajn - Technology and design 4(21).* Retrieved from: http://nbuv.gov.ua/UJRN/td_2016_4_12 [in Ukraine].
6. *Oficijna dokumentaciya proektu Arduino* [Arduino Project Official Documentation]. Retrieved from: http://www.arduino.ru [in Russian]
7. *Avtors'ki materiali z sajtu «Payal'nik»* [Author's materials from «Solderer» site]. Retrieved from: http://geektimes.ru/ [in Russian]

Аутентификация пользователя в автоматизированных микропроцессорных системах

Литвинов В. А., Николаев В. В., Голубев Л. П.
Киевский национальный университет технологий и дизайна

Цель. *Исследование методов аутентификации пользователя в системах контроля доступом и разработка нового метода аутентификации.*

Методика. *В работе использована методика аутентификации на базе магнитных карт и парольной защиты.*

Результаты. *Разработана автоматизированная система контроля доступа к ресурсам микропроцессорных систем на базе магнитных карт и парольной защиты.*

Научная новизна. *Разработан новый механизм аутентификации пользователя в системах контроля доступа, основанный на магнитных картах и парольной защите.*

Практическая значимость. *Разработанный алгоритм аутентификации пользователя является универсальным и может быть применен при аутентификации пользователя в различных микропроцессорных системах. Разработанная автоматизированная система контроля доступа использует предложенный метод аутентификации пользователя.*

Ключевые слова: *аутентификации, система, контроль, доступ, магнитная карта, парольная защита*

Authentication of the user in automated microprocessor systems

Litvinov V. A, Nikolaev V. V., Golubev L. P.
Kyiv National University of Technology and Design

Objective. *Investigation of user authentication methods in access control systems and development of a new authentication method.*

Methodology*. The method of authentication based on magnetic cards and password protection was used in the work.*

Findings. *An automated system for controlling access to resources of microprocessor systems based on magnetic cards and password protection has been developed.*

Originality. *A new mechanism for user authentication in access control systems based on magnetic cards and password protection has been developed.*

Practical value. *The developed user authentication algorithm is universal and can be used for user authentication in various microprocessor systems. The developed automated access control system uses the proposed method of user authentication.*

Keywords: *authentication, system, control, access, magnetic card, password protection*