СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

УДК 519.711:343.98

Білогуров В.А.,
старший науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0003-1896-0782
Назарок Д.С.,
старший науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0002-3000-4534

КЛЮЧІ ТА ІДЕНТИФІКАТОРИ В СИСТЕМАХ УПРАВЛІННЯ ДОСТУПОМ

У статті розглянуті ідентифікатори доступу як засоби захисту інформації і матеріальних цінностей. Розглянуті у розвитку контактні засоби контролю доступу, безконтактні та комбіновані смарт-карти. Описана будова найпоширеніших смарт-карт, досвід їхнього практичного використання. Описані ідентифікатори стандартів MIFARE, EM MARINE, TEMIC. Вивчена можливість перепрограмування таких карт з метою розширення додаткових функцій. Розглянуто основні підходи виробників смарт-карт для забезпечення захисту даних від дій зловмисників.

Розглянуті типові зчитувачі (рідери), наведені їхні основні характеристики.

Ключові слова: *ідентифікатори доступу, смарт-карти, зчитувач.*

В статье рассмотрены идентификаторы доступа как средства защиты информации и материальных ценностей. Рассмотрены в развитии контактные средства контроля доступа, бесконтактные и комбинированные смарт-карты. Рассмотрено строение распространенных смарт-карт, опыт их практического использования. Рассмотрены идентификаторы стандартов MIFARE, EM MARINE, TEMIC. Изучена возможность перепрограммирования таких карт с целью расширения дополнительных функций. Рассмотрены основные подходы производителей смарт-карт для обеспечения защиты данных от действий злоумышленников.

Рассмотрены типичные считыватели (ридеры), приведены их основные характеристики.

Ключевые слова: *идентификаторы доступа, смарт-карты, считыватель.*

Вступ

Сьогодні проблеми забезпечення безпеки громадян і держави, персональних і громадських секретів не втратили свою актуальність: чим більше таємниць, тим більше бажання і можливостей їх розкрити. Підтвердженням тому є як різноманітні системи кодування і передачі даних, так і пристрої, що перехоплюють і дистанційно декодують цю інформацію. Найпростіший приклад – підробки безконтактних карт, в тому числі з банківськими додатками.

У статті розглянуті будова смарт-карт, їх можливості, технічні характеристики і варіанти практичного застосування різних систем безпеки на основі “міток” (ключів) і зчитувальних пристроїв (рідерів).

Контактні, безконтактні і комбіновані смарт-карти

Смарт-карта (smart-card, proximity, ProxCard, мітки, транспондери) – це, перш за все, носій інформації. Електронні технології, вбудовані в смарт-карти (далі СК) і пов’язане з ними обладнання, прискорили процедури аутентифікації і, як наслідок, такі дії: проведення платежу, відмова від обслуговування, пропуск на об’єкт або обмеження доступу та інше.

Системи кодового доступу почали широко використовуватися не так давно. Кодові замки (механічні та з застосуванням електроніки), “навантажені” на електромагнітні замки (соленоїди, з’єднані з дверною засувкою) були дуже популярні в 1970–1990-х роках. Щоб відкрити такий замок, потрібно ввести послідовність цифр. Очевидно, такі замки не були панацеєю від несанкціонованого проникнення. Крім того, за тодішньою технологією мікросхем електронні пристрої не можна було оперативно перепрограмувати.

З розвитком мікроелектроніки, мікропроцесорів і персональних комп’ютерів (ПК) з’явилися нові пристрої кодового доступу. Вони були дуже різні – від набору кодової комбінації (логіна і пароля) за допомогою клавіатури, до брелока – ключа з USB-роз’ємом, який був ідентифікатором користувача ПК або програмного забезпечення. Різновидом такого кодового пристрою був зчитувач (сканер) папілярних ліній з пальців.

Рис. 1. Ідентифікатор-таблетка iButton

Деякі з описаних вище систем застосовуються до цього часу. Але поряд з ними з’явилися пристрої набагато ефективніші і захищені, а також прилади, які можуть копіювати мітки/ключі (що робить захист дуже вразливим).

Контактні кодові пристрої типу iButton (див. рис. 1) широко застосовуються в побутових додатках, домофонах та інших простих системах доступу. "Таблетки" iButton мають вбудовану незалежну пам'ять об'ємом від 256 байт до 8 кбайт (див. табл. 1). Зчитувачі карт iButton оснащені двома контактами з нержавіючої сталі. Виробництво таких зчитувачів може бути організовано практично скрізь. Мітки iButton не бояться прямого попадання вологи. Окремі моделі мають додаткові властивості. Наприклад, прилад DS1991 (обсяг пам'яті 1 кбіт) має захист пам'яті за допомогою пароля, DS1963S (4 кбіт) дозволяє реалізувати додаткові методи активної аутентифікації. Інтерфейс карт iButton описаний в літературі і дозволяє з'єднувати кілька зчитувачів в єдину двопровідну мережу.

Таблиця 1

Характеристики кодових пристроїв iButton

Код приладу	Обсяг пам'яті, біт	Додаткові можливості
DS1971	256+64, ЕППЗП (електронний перепрограмований запам'ятовуючий пристрій)	
DS1973	4К, ЕППЗП	
DS1991	1344, енергонезалежний ОЗП (оперативно запам'ятовуючий пристрій)	Захист пам'яті паролем
DS1992	1К, енергонезалежний ОЗП	
DS1993	4К, енергонезалежний ОЗП	
DS1994	4К, енергонезалежний ОЗП	Годинник
DS1995	16К, енергонезалежний ОЗП	
DS1996	64К, енергонезалежний ОЗП	
DS1963S	4К, енергонезалежний ОЗП	Посилена аутентифікація, лічильник циклів запису
DS1963L	4К, енергонезалежний ОЗП	Лічильник циклів запису

Приблизно у цей же час з'явилися нові носії інформації в різному виконанні: на основі картону, пластика, пластикових брелоків, напівпровідникових кристалів, що імплантуються в органічну тканину. На відміну від iButton, карти-мітки (СК) на пластиковій і особливо паперовій основі бояться вологи. Карта з вбудованим мікроконтролером, що містить процесор, пам'ять і інтерфейс введення-виведення, працює під управлінням вбудованої операційної системи (ОС). Форма карти, контактів, їх розташування, призначення регламентовані стандартами ISO/IEC 7816 та ISO/IEC 7810.

Безконтактні СК (БСК) зручніші, вони можуть спрацьовувати на відстані до 10 см від рідера (для надійної взаємодії між міткою і рідером досить повітряного зазору в 3–5 см). БСК містять мікроконтролер і антену, передача даних здійснюється (залежно від стандарту) на частоті 125 кГц або 13,56 МГц (в комунікаційних системах на основі технологій ближнього поля). Стандарти описані в специфікаціях ISO 18902, ISO 7816, ISO 14443 варіанти A і B (рідше ISO/IEC 15693), EMV (Europay, MasterCard, Visa), IPS/JEDEC J-STD-020C, ECMA 340, ETSI TS 102 190 і інші.

Варто уважно ознайомиться з описом стандарту ISO 7816, в якому прописані вимоги до конструкції і технології обміну цифровими даними для контактних СК (на основі контактних кристалів) і ISO 14443A і 14443B – для безконтактних

карт. Додаткова інформація викладена на інтернет-сторінці http://www.smart-park.ru/index.php/products/smartcards.htm. Там же наведені технічні характеристики найбільш популярних мікроконтролерів, які можуть стати в нагоді розробникам і користувачам систем безпеки і кодового доступу. Системи, що працюють на основі технології Java, регламентовані стандартами Java Card 2.1.1 і вище.

Якщо СК оснащені одночасно контактним (кристал) і безконтактним інтерфейсом, їх називають дуальними. Комбіновані СК (комбі-карти) мають два або кілька мікроконтролерів – вбудованих мікросхем. У безконтактних смарт-картах застосовується технологія RFID (Radio Frequency Identification, радіочастотна ідентифікація) – спосіб автоматичної ідентифікації об'єктів, при якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в мітках. Основними напрямами розвитку технологій RFID з використанням безконтактних пластикових карт є:

- контроль доступу та облік робочого часу на підприємствах;
- платний доступ на автомобільні паркінг, підйомники, атракціони та ін.;
- платежі за користування громадським транспортом;
- заміна або доповнення банківських і дисконтних карт із магнітною полосою;
- безключовий доступ до автотранспорту.

Ініціалізація СК відбувається за допомогою системи контролю управлінням доступу (СКУД).

Карти на основі пластика і картону

Існують три основні стандарти карт: Mifare, EM Marine і HID. Перший добре захищений, але головна його відмінність від EM Marine, який розроблений раніше, полягає в можливості запису на мітку (носій, карту, ідентифікатор, ключ) додаткової інформації. Карта EM Marine не має пам'яті для зберігання інформації, тому в ній не можливий перезапис. Стандарт носія визначається мікросхемою (мікроконтролером). На рис. 2 представлений вид розібраної карти стандарту EM Marine.

Сьогодні поширені СК всіх трьох стандартів у різних виконаннях (пластикова карта, в тому числі з прорізом для кріплення, брелок, таблетка, в тому числі прогумований "наручний" браслет з міткою – для експлуатації в умовах водного середовища і великій вологості). Карти всіх стандартів можна візуально відрізнити одну від одної за деякими ознаками. Наприклад, карта EM Marine має на поверхні набір цифр – унікальний номер, тоді як більш захищена карта (з тими ж типорозмірами) Mifare не має ніяких написів (див. рис. 3).

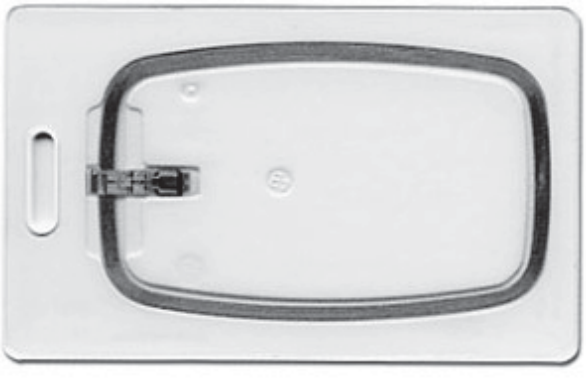

Рис. 2. Розібрана карта стандарту EM Marine

Рис. 3. Зовнішній вигляд ідентифікаторів у різному виконанні

При тривалій експлуатації цифри на пластику поступово стираються. Карта стандарту HID (або ProxCard II) теж може мати на пластиковому носії набір цифр, але відрізняється наклейкою на лицьовій стороні “HID”; зі зворотного боку пластику та ж абревіатура нанесена методом тиснення. Це – головна відмінність однакових за зовнішнім виглядом карт з габаритними розмірами стандарту Clamshell. Типорозмір СК і БСК визначається стандартом ISO/IES 7816-2.

З ключами в іншому виконанні (браслети, брелоки та інше) менше можливостей помістити і прочитати написи. Карти (мітки в інших виконаннях) відрізняються одна від одної також радіочастотою, на якій відбувається взаємодія з рідером. Розглянемо деякі приклади.

Мітки стандарту Mifare

Брелок стандарту Mifare використовується в дисконтних, платіжних і транспортних системах. Корпус обшитий натуральною шкірою, на брелок можна нанести логотип (див. рис. 3 зліва знизу). Мітка допускає шифрування даних і забезпечує до 100 000 циклів перезапису. Вона відрізняється від міток свого класу підвищеною швидкістю транзакції з швидкодією, яка вимірюється в мілісекундах. Об’єм внутрішньої пам’яті становить 1 024 байт. З цієї мітки неможливо зробити копію простим перезаписом інформації (приклавши до зчитувача із запам’ятовуванням коду). Збереження даних пам’яті до 10 років – загальна характеристика міток цього класу. Технічні характеристики ключа мітки моделі IL-07MK фірми IronLogic стандарту Mifare:

- мікросхема Mifare S50;
- робоча частота 13,56 МГц;
- тип карти – читання/запис;
- час транзакції 164 мс;
- обсяг пам’яті 1024 байт;
- матеріал корпусу – натуральна шкіра;
- колір чорний;

• габаритні розміри 40,0х40,0х5,5 мм;
• діапазон робочих температур -30 ... + 50 ° С.

Мітки стандарту EM Marine

Карта IL-05ELR стандарту EM Marine (виробник IronLogic) з прорізом для кріплення має підвищену дальність зчитування даних (на 50–70 % відносно звичайної карти цього стандарту). Ці відомості надані розробниками і підлягають перевірці. На БСК нанесено її унікальний номер, що може спростити пошук у базі даних при відсутності пристрою, що зчитує. Для персоналізації карти можна використовувати наклейку (див. рис. 3). Технічні характеристики ідентифікатора IL-05ELR IronLogic стандарту EM Marine:

• мікросхема EM Marine;
• робоча частота 125 кГц;
• тип карти – тільки читання;
• формат друку ID – ххх, ххххх;
• матеріал корпусу – пластик ABS;
• колір корпусу – білий, сірий, зелений, синій;
• габарити (ДхШхТ) 86,0х54,0х1,6 мм;
• діапазон робочих температур -30 ... + 55 ° С.

Карта ідентифікується за системою Wiegand 26 з робочою частотою 125 кГц відповідно до протоколу DS1990A. Зрозуміло, існують карти аналогічного типорозміру у стандарті Mifare, оснащені функціоналом читання/запис, наприклад, IL-05M фірми IronLogic, яка має функції шифрування і антиколізії, можливість перезапису до 100000 циклів і довговічність 10 років.

Мітки стандарту Temic як аналог EM Marine

Як різновид БСК стандарту EM Marine існують мітки стандарту Temic – RFID карти для запису і копіювання унікального номера. Вони імітують карти стандарту HID Proxll, EM Marine та інших, але працюють у діапазоні частот 100–150 кГц.

Карта IL-05T тієї ж фірми IronLogic оснащена кристалом T5557 і працює на частоті 125 кГц. Реалізуючи стандарт EM Marine, мітка Temic, однак, забезпечена, функціоналом читання/запис і не має надрукованого на пластику набору символів. За зовнішнім виглядом відрізнити таку карту від Mifare практично неможливо. Саме тому нанесення ідентифікаційного символьного коду на сам пластик є важливою відмінною ознакою. Наприклад, карту IL-06E IronLogic з мікросхемою EM Marine, що функціонує на частоті 125 кГц, також не можна відрізнити від IL-05ELR за зовнішніми ознаками, хоча вона містить інший мікроконтролер.

Всі карти всередині одного стандарту взаємозамінні: карту EM Marine ISO-IL-06E можна замінити картою IL-05ELR, а карту IL-06M IronLogic Mifare ISO-IL-05M Mifare.

Комбіновані мітки

Особливий (комбінований) тип – це БСК того ж типорозміру IL-06E & M IronLogic ISO з 2 кристалами EM Marine + Mifare 1K. Карта може працювати з системами відразу двох стандартів, причому заготовка такої карти коштує всього на 10 % дорожче. Комбінована карта корисна в тих випадках, коли на одному

об'єкті встановлено зчитувачі різних стандартів. Технічні характеристики двокристалевої карти IL-06E & M IronLogic ISO:

- мікросхема EM Marine + Mifare 1K;
- робоча частота 125 кГц + 13,56 МГц;
- тип карти – тільки читання + читання/запис;
- матеріал корпусу – ПВХ.

Існують різні за типом мітки з "відкритим" корпусом (для наповнення). Це означає, що в захищений від вологи прогумований корпус можна встановити будь-який з кристалів серій EM4100, EM4102, MF1S50, MF1S70, MF Ultralight, T5557, I-Code I, I-Code II, щоб використовувати в пристроях відповідного стандарту. Безконтактна СК представленого форм-фактора підтримує кілька функцій (карта доступу, банківська карта, ідентифікаційна мітка та ін.).

Конструкція та елементна база карт

Антена, як правило, виконана металізованими доріжками у вигляді декількох спіральних кіл по периметру основи карти (іноді в центрі) – пластика або картону.

На рис. 2 можна побачити внутрішню будову БСК. Карти, в яких кристал виведений на поверхню і призначений для електричного контакту з пристроєм зчитування даних, мають свої відмінності. Кристал – це мікропроцесор із вбудованою операційною системою і пам'яттю невеликого обсягу (до сотень кілобайт). У різний час випускалися 8-, 16- і 32-розрядні мікропроцесори, що визначають і обсяг внутрішньої пам'яті БСК. Найпопулярніший свого часу кристал AE55C1 виробництва компанії Renesas Technology був 32-розрядний. Пам'ять такого кристала складала десятки кілобайт.

Інший популярний мікропроцесор – ST19WR66 виробництва компанії ST Microelectronics містить ПЗП обсягом 224 кбайт, що забезпечує зберігання операційної системи разом із програмою шифрування даних за стандартом ISO 14443B. Такий кристал має незалежну пам'ять, яка використовується ОС для зберігання персональної інформації власника, включаючи біометричну. Саме на основі подібних мікросхем (з великим об'ємом пам'яті) реалізовані "електронні" паспорти, термін дії яких обмежений 10 роками.

Більш досконалий пристрій, реалізований на основі мікроконтролера AE55C1 з масковим ПЗП, має корисний об'єм пам'яті 240 кбайт і дозволяє підвищити щільність зберігання кодів і даних у порівнянні зі "старими" мікросхемами Renesas Technology, орієнтованими на БСК без банківського додатка.

Обсяг пам'яті, нові технології

Відносно нова версія ОС для сімейства мікропроцесорів JCOP3131 компанії IBM підтримує стандарти шифрування даних AES і EES (останній забезпечує підвищений рівень захисту з ключем малої довжини). Збільшити обсяг пам'яті до 1 Мбайта вдалося за допомогою розробки кристалів для БСК з флеш-пам'яттю. Практично, можна зробити одну карту (один пластик) багатофункціональним інструментом: електронним пропуском, корпоративним посвідченням і картою з банківським додатком. Можливості конфігурації різних додатків у карті з таким обсягом пам'яті дуже великі. Зручно і додавати нові функції в уже випущену карту. У такі карти можна записувати і біометричні дані, якщо дозволяють можливості кристала.

Захист даних

Традиційні технології шифрування даних не обмежуються AES (Advaced Encryption Standard), SHA (Secure Hash Algorithm) і американським FIPS (Federal Informaion Processing Standards), які в межах цієї статті не розглядаються. Однак слід згадати технологію NFC – зв'язок у ближньому полі (Near Field Communiacation), яка досить перспективна в цей час для експериментів "просунутих" користувачів і радіолюбителів, оскільки забезпечує оперативну і захищену передачу даних між пристроєм зчитувача і міткою на відстані до 10 см (заявлена виробником відстань). Така система практично не схильна до перешкод через малу відстань між БСК і рідером.

Важливою особливістю СК з можливістю перезапису даних є їх надійність при збоях будь-якої природи. Дані в пам'яті зберігаються в тому ж вигляді, якими вони були до початку незавершеної операції зміни і процесу запису. Ця властивість називається "атомарністю" змін даних у пам'яті.

У банківському секторі використовуються СК на основі операційних систем, запрограмованих за допомогою мови Java. Ця технологія регламентована галузевим стандартом VGP (Visa Global Platform), який сьогодні дуже популярний у фінансовій сфері. Транспондери (proximity-карти, СК, мітки) реалізовані відповідно до стандарту ISO 14443A/B. Вони працюють (резонують) на неліцензійованих частотах 125 кГц і 13.56 МГц і нікому не заважають, тому що не викликають конфліктів з іншим електронним обладнанням. Інтегрування в ту ж карту (підкладку) інших електронних компонентів (відповідно до цього стандарту) не збільшує товщину носія (картону).

Мікросхеми для таких СК виготовляються відомими компаніями (Atmel, On Track, Inside Contactless і іншими). Вони працюють на зумовленій стандартом частоті (див. вище) і разом з антенами, вбудованими у пластик або картон, перетворилися в напівфабрикат RFID-системи доступу, що функціонує відповідно до стандарту ISO 15693-2.

Існують відмінності між частотами і конструктивним виконанням мітки (карти). Кожна мітка-пристрій RFID містить кристал і антену, зокрема штамповану "котушку". Цікаво, що на відносно низьких частотах до 145 кГц котушка намотана на конденсатор, який налаштовує частоту, а на більш високих (13,56 МГц) становить кілька струмопровідних доріжок спіралі по периметру пластикової карти.

Існують багаторазові СК, на які оператор (зазвичай в касі метрополітену) за допомогою спеціального пристрою – програматора – записує інформацію про кількість поїздок і терміні дії СК. Обсяг перезаписуваної інформації залежно від технічних параметрів мітки може становити від декількох десятків кілобайт до декількох Мбайт. Таким чином, на тій же площі карти розробники розміщують різну кількість композитних блоків.

Розширилися і функціональні можливості смарт-карт. Зчитування і запис даних у мітку називають емуляцією. Щоб передати дані між NFC-пристроями (смарт-картою і системою зчитування/запису даних), їх треба зблизити на відстань 4–5 см і менше або, якщо мова йде про системи контактного доступу (таблетки для зчитувачів у старих системах домофонів), привести до контакту. Цей контакт ініціює роботу інтерфейсу і конфігурацію мережі рівноправних вузлів.

Важливою особливістю протоколу NFC є підтримання режиму пасивного з'єднання (passive mode of communication), який дозволяє забезпечити сеанс зв'язку

енергією, використовуючи ресурси тільки одного з пристроїв (зчитувача, на який подано електроживлення). Така технологія активно використовується для передачі невеликих обсягів даних, доступу на об'єкти, контролю відвідуваності об'єктів з фіксацією часу проходу, контролю переміщень по великій території співробітників або вантажів, проведення платежів, конфігурації доступу до дротових і бездротових мереж Wi-Fi і в багатьох інших випадках.

У системах безпеки використовуються нові рішення, що автоматизують контрольні процедури і підвищують ступінь їх надійності. Аутентифікація за допомогою мітки і системи кодового доступу – це надання, з одного боку, і перевірка, з іншого, доказів того, що пред'явник мітки є саме тим, кому вона належить. Під час вдосконалення систем безпомилкової аутентифікації стає актуальним комплекс методів, наприклад, поєднання кодового доступу з посвідченням особи, що містить біометрію, дактилоскопію, особливості особи, голосу та інших індивідуальних рис. Такі комплексні методи аутентифікації, захисту інформації та обмеження доступу забезпечать більш надійну взаємодію людей і комп'ютерів.

Прогресивна біометрія

Сьогодні біометричний паспорт на основі однойменних модулів – абсолютно реальна річ. Системи обмеження доступу, торгові точки, корпоративні перепустки (і облік відвідуваності співробітників), електронні документи (закордонні біометричні паспорти) з появою біометричного модуля AT77SM0101BCBO2VKE виробництва Atmel (і аналогів) були вдосконалені. Такі модулі є закінченою підсистемою і поставляються разом із програмним забезпеченням для аутентифікації, що полегшує роботу користувача. Модуль реалізований на основі мікроконтролера тієї ж фірми AT91RM9200 з архітектурою ARM9 і оснащений декількома інтерфейсами, в тому числі Ethernet, SPI і RS-232.

У конфігурацію біометричного модуля входить кристал – датчик FingerChip (Atmel) з розмірами 0,4 мм (товщина) і 14 мм (сторона). Він стійкий до ударних навантажень, забруднень і вологості, саме тому в ньому зручно зберігати дактилоскопійовані дані в цифровому вигляді. Існують й інші датчики різних компаній-виробників. Загальною тенденцією є мініатюризація датчиків. Наприклад, ще 3–4 роки тому інтегральна схема скануючого датчика фірми Fingerprint Cards мала здатність 363 dpi і розміри 2,24 x 10,64 мм.

Вставка мікросхеми з мініатюрною антеною в документ на паперовому носії може здійснюватися кількома методами. Найбільш популярною та надійною є вставка/вклейка в надрукований документ і подальше ламінування.

Зчитувальні пристрої

Системи на основі СКУД дозволяють легко і швидко збирати з декількох модулів функціональні системи охорони і безпеки з кодовим доступом, що вимагають мінімальної кількості зовнішніх елементів. Кодовий доступ реалізується через дистанційне (до 10 см) зчитування коду на мітці, його ініціалізацію, декодування і формування сигналу управління для виконавчого пристрою (наприклад, електромагнітного замка дверей або блокувача на "вертушці").

Як "замикаючий" пристрій можна використовувати не лише сам замок (наприклад, ЕМЗ-4 або ML-100), а й будь-яке активне навантаження, розраховане на відповідну напругу живлення. Так, система кодового доступу, реалізована на

модулі Matrix II EH IronLoic (див. рис 4), розрахована на підключення навантаження з напругою 12 В ± 20% і струмом до 5 А. Якщо необхідний більший струм, то комутацію виконують через додаткове реле.

Пасивні системи RFID складаються з трьох частин: рідера, пасивної мітки і ведучого комп'ютера. Рідер є шлюзом, за допомогою якого цифрові дані вводяться в контролери на базі ПК і в інтегровані системи. Пристрій, що зчитує містить мікроконтролер, передавальну антену, блок визначення рівня сигналу радіохвилі (peak detector), блок для передачі енергії мітці і блок читання інформації з допомогою детектування зміни поля (backscatter modulation – відбита модуляція). Рідери випускаються декількох видів: вбудовані, з клемником для підключення (див. рис. 4), клавіатурні рідери (з роз'ємами USB/microUSB), рідери в модулях PCMCIA ПК і КПК та інші.

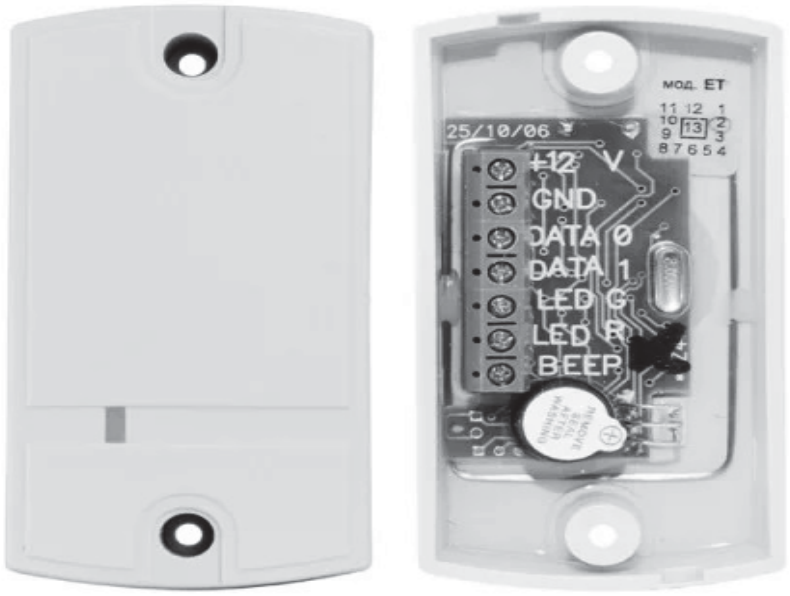

Рис. 4. Зовнішній вигляд зчитувача Matrix II EH IronLogic

Радіочастотний синусоїдальний сигнал генерується рідером для передачі енергії мітці і отримання від неї даних. Найбільш поширеними частотами є 125 кГц і 13,56 МГц. На більш високих частотах функціонують інші системи RFID, і для них розроблені інші методи зв'язку. Наприклад, на частоті 2,45 ГГц між рідером і міткою використовується радіозв'язок, на частотах 125 кГц, 145 кГц і 13,56 МГц використовується електромагнітний зв'язок.

Періодичні коливання напруженості електромагнітного поля є основою для передачі даних від мітки до рідера і назад. У системі існує лише один передавач у повному сенсі цього слова – рідер. Електромагнітне поле, створюване рідером, використовується для:

• живлення – мітки не мають внутрішньої батареї живлення або іншого джерела енергії. Вони живляться від електромагнітного поля, яке створене рідером;

• синхронізації – більшість міток ділять частоту зв'язку для внутрішнього тактування різних модулів і лічильників, хоча деякі мають вбудований генератор;

• передачі даних від мітки – рідер стежить за рівнем випромінюваного поля, модуляцією якого передаються дані (форматом вихідних даних може бути I2C, SPI, RS2400, LEVEL + STROBE або PWN).

Популярний зчитувач Matrix II EH 125 кГц (див. рис. 4) використовується в системах контролю доступу. За допомогою перемичок можна встановити тип вихідного інтерфейсу – Touch Memory або Wiegand. Зчитувач з картами Proximity працює у стандарті HID і Em Marin.

Технічні характеристики рідера Matrix II EH IronLogic:

• частота – 125 кГц;

• читання карт доступу Em Marin і HID ProxCard II;

• дальність впевненого виявлення мітки – від 6 до 14 см;

• живлення зчитувача 8–18 В постійного струму, споживання струм на рівні 50 мА;

• індикація: звуковий сигнал, світлодіод (2 кольори, зелений і червоний, припускають зовнішню індикацію світлодіодом і звуком);

• температура експлуатації -40 ... + 50 ° С;

• матеріал – пластик ABS;

• колір: від чорного до світло-сірого або навіть “металік”;

• вхідний інтерфейс: Dallas Touch Memory (емуляція DS1990A), Wiegand 26;

• максимальна відстань від зчитувача до контролера (система з ПК) – до 15 м (інтерфейс DS1990A) і до 100 м (інтерфейс Wiegand);

• габарити 85 х 44 х 18 мм.

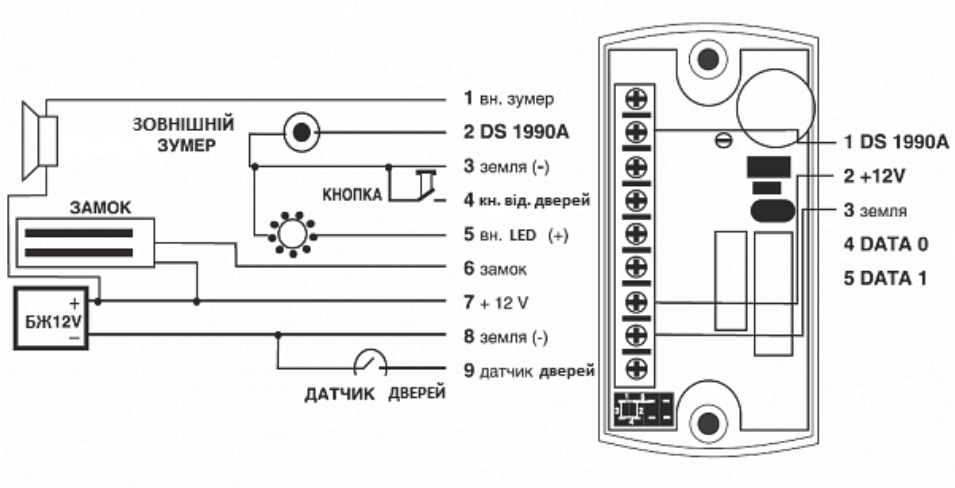

Рис. 5. Схема підключення ланцюгів живлення і комутації зчитувача Matrix II EH IronLogic

Підключення рідера до контролера і навантаженнz ілюструє рис. 5. Більшість рідерів описаних форм-факторів випускаються в аналогічному виконанні, що полегшує їх монтаж. Вони встановлюються у відкритих для доступу місцях, тому необхідно пред’являти підвищені вимоги до “вандалозахищеності”.

Зчитувачі мають і деякі функціональні відмінності. Наприклад, існують рідери (різних стандартів), які вже містять джерело живлення і готові до роботи від мережі 220 В, мають на виході транзистор з відкритим колектором, до якого підключають навантаження (реле), або слабкострумове електромагнітне реле з можливістю комутації навантаження до 6 А .

Головна відмінність систем дистанційного кодового доступу приблизно одного енергетичного діапазону полягає в тому, що одні системи можуть тільки зчитувати з мітки код, без можливості зворотного запису інформації на мітку, а інші дозволяють обмінюватися інформацією і записувати в пам'ять тієї ж мітки (в т. ч. БСК) нові дані.

Сьогодні СК (вона ж транспондер, мітка або ключ) може виглядати як брелок, браслет і таблетка (див. рис. 3) і може функціонувати у складі комп'ютерних систем, мобільних телефонів, автомобілів і будь-якого іншого обладнання (сфера їх застосування практично не обмежена). Можна припустити, що мініатюрнішу мітку, але з тим же принципом роботи і функціоналом, можна імплантувати під шкіру людини і/або тварини за допомогою медичних технологій, що дозволяє не тільки її ідентифікувати, а й контролювати переміщення. Такі технології давно апробовані і сьогодні вже нікого не дивують, хоча ще десятиліття тому описувалися письменниками-фантастами.

За тим же принципом (специфікації для банківських карт Master Card Pay Pass на основі технології RFID) працюють "електронні" шафки в басейнах, фітнес-клубах і аквапарках, де міткою є браслет, що видається клієнту.

Висновки

Усі описані технології, як вчора, так і сьогодні, застосовуються в широкому спектрі завдань. У магазинах, у комплексі протикрадіжних систем (пристроїв), мітки використовуються вже понад двадцять років. Широко поширені мітки для протиугінних систем автомобілів (двигун затихне через 10 ... 60 с, якщо власник не прикладе мітку до певного місця). Ключі дорогих і престижних автомобілів також забезпечені вбудованою "міткою", яка зчитується рідером, встановленим у голівці замку запалювання. Схожа система застосовується у складі пристроїв типу Аркан Сателіт, які відстежують автомобілі, забезпечені визначником місцезнаходження по GPS.

Мітки застосовуються досить широко в оборонній промисловості: для контролю доступу – смарт-карти, для ідентифікації людини при доступі до секретних відомостей – спеціальні кристали, що імплантуються під шкіру. І якщо раніше відстежити переміщення об'єкта можна було тільки за допомогою ізотопів, то сьогодні електроніка справляється з цим без особливих труднощів.

Весь спектр використання безконтактних пристроїв нового покоління практично неможливо описати. Безконтактні пристрої контролю будуть вдосконалюватися, а мікроконтролери в системах ідентифікації – розвиватися, поповнюючись новими функціями для комплексного захисту об'єктів і секретної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Форма контактів, їх розташування. Wikipedia, the free encyclopedia. ISO/IEC 7816. URL: https://en.wikipedia.org/wiki/ISO/IEC_7816 (дата звернення: 01.02.2019).

2. Форма карти. Wikipedia, the free encyclopedia. ISO/IEC 7810. URL: https://en.wikipedia.org/wiki/ISO/IEC_7810 (дата звернення: 01.02.2019).

3. Стійкість матеріалу картки. Wikipedia, the free encyclopedia. ISO 18902. URL: https://en.wikipedia.org/wiki/ISO/IEC_18902 (дата звернення: 01.02.2019).

4. Частотні характеристики картки RFID. Wikipedia, the free encyclopedia. ISO/IEC 14443. URL: https://en.wikipedia.org/wiki/ISO/IEC_14443 (дата звернення: 01.02.2019).

5. Частотні характеристики картки. Wikipedia, the free encyclopedia. ISO/IEC 15693. URL: https://en.wikipedia.org/wiki/ISO/IEC_15693 (дата звернення: 01.02.2019).

REFERENCES

1. Forma kontaktiv, yikh roztashuvannia. “The form of contacts, their location”. Wikipedia, the free encyclopedia. ISO/IEC 7816.URL: https://en.wikipedia.org/wiki/ISO/IEC_7816 (date of application: 01.02.2019) [in Ukrainian].

2. Forma karty. “Card form”. Wikipedia, the free encyclopedia. ISO/IEC 7810. URL: https://en.wikipedia.org/wiki/ISO/IEC_7810 (date of application: 01.02.2019) [in Ukrainian].

3. Stiikist materialu kartky. “Material card stability”. Wikipedia, the free encyclopedia. ISO 18902. URL: https://en.wikipedia.org/wiki/ISO/IEC_18902 (date of application: 01.02.2019) [in Ukrainian].

4. Chastotni kharakterystyky kartky RFID. “Frequency characteristics of the RFID card”. Wikipedia, the free encyclopedia. ISO/IEC 14443. URL: https://en.wikipedia.org/wiki/ISO/IEC_14443 (date of application: 01.02.2019) [in Ukrainian].

5. Chastotni kharakterystyky kartky. “Frequency characteristics of the card”. Wikipedia, the free encyclopedia. ISO/IEC 15693. URL: https://en.wikipedia.org/wiki/ISO/IEC_15693 (date of application: 01.02.2019) [in Ukrainian].

UDC 519.711:343.98

V.A. Bilohurov,
Senior Researcher, State Research Institute
MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-1896-0782,
D.S. Nazarok,
Senior Researcher,
State Research Institute MIA Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0002-3000-4534

KEY AND IDENTIFIERS IN ACCESS CONTROL SYSTEMS

The subject of this article was the main and auxiliary means and devices, which allowed first to differentiate access to information and objects, and subsequently to automate such access. Contact, non-contact and combined smart cards that operate at 125 kHz or 13.56 MHz (in near-field communication systems) are considered. Standards are described in specifications ISO 18902, ISO 7816, ISO 14443 variants A and B (less frequently ISO/IEC 15693), EMV (Europay, MasterCard, Visa), IPS/JEDEC J-STD-020C, ECMA.

Typical use of smart cards (tags) is discussed:

– access control and time management at enterprises;
– paid access to car parks, lifts, attractions, etc;
– payments for the use of public transport;
– replacement or addition of bank and discount cards with magnetic stripe;
– keyless access to vehicles.

There are three main card standards: Mifare, EM Marine and HID. The media standard is defined by the chip. The tag allows data encryption and provides up to 100,000 overwrite cycles.

Design and element base of maps are considered. Attention paid to the volume of tags memory and the use of new technologies. Ways of protection against unauthorized

interference such as traditional technologies of data encryption AES (Advaced Encryption Standard), SHA (Secure Hash Algorithm), and American FIPS (Federal Informaion Processing Standards) are considered.

The article focuses on the use of biometric module AT77SM0101BCBO2VKE manufacturing Atmel in particular for foreign passports. Design and peculiarities of operation of readers, as well as the use of common tags for anti-theft systems of cars are considered.

Possessing the basic functionality of systems and components of remote access control can be useful to practitioners in implementing law enforcement practices.

Keywords: access identifiers, smart cards, reader.

Отримано 19.03.2019
Рецензент Марченко О.С., к.т.н.