

УДК 004.056.5

Здолбіцька Н.В., к.т.н., доц., Здолбіцький А.П., Семенко О.О.
Луцький національний технічний університет

СИСТЕМИ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ І УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ

Здолбіцька Н.В., Здолбіцький А.П., Семенко О.О. Системи електронної ідентифікації і управління доступом користувачів. У статті розглянуто сучасні засоби системи електронної ідентифікації і управління доступом користувачів. Проведено порівняльний аналіз засобів безпеки. Проаналізовано особливості функціонування, основні характеристики та параметри, які необхідно враховувати при проектуванні систем доступу, виборі режиму роботи і конкретної апаратури для реалізації. Розроблено програмно-апаратний комплекс для тестування роботи найпоширеніших сьогодні на ринку засобів автентифікації. Комплекс використовує платформу Arduino, як найбільш недороге та водночас гнучке рішення із великою кількістю модульних давачів та засобів фізичної ідентифікації та контролю.

Ключові слова: системи електронної ідентифікації, системи контролю та управління доступом, електронні замки, електронні ключі.

Здолбицкая Н.В., Здолбицкий А.П., Семенко О.О. Системы электронной идентификации и управления доступом пользователей. В статье рассмотрены современные средства системы электронной идентификации и управления доступом пользователей. Проведен сравнительный анализ средств безопасности. Проанализированы особенности функционирования, основные характеристики и параметры, которые необходимо учитывать при проектировании систем доступа, выборе режима работы и конкретной аппаратуры для реализации. Разработан программно-аппаратный комплекс для тестирования работы самых распространенных сегодня на рынке средств аутентификации. Комплекс использует платформу Arduino, как наиболее недорогое и одновременно гибкое решение с большим количеством модульных датчиков и средств физической идентификации и контроля.

Ключевые слова: системы электронной идентификации, системы контроля и управления доступом, электронные замки, электронные ключи.

Zdolbitska N.V., Zdolbitskyu A.P., Semenکو O.O. Electronic identification and access control systems for users. The article deals with modern means of electronic identification and access control system. A comparative analysis of security measures has been carried out. Functional features, main characteristics and parameters to be considered in the design of access systems, the choice of operating mode and specific equipment for implementation are analyzed. A hardware and software complex has been developed to test the most common authentication tools on the market today. The complex uses the Arduino platform as the most inexpensive yet flexible solution with many modular sensors and physical identification and control tools.

Keywords: electronic identification systems, access control and management systems, electronic locks, electronic keys.

Постановка проблеми.

Одна з основних проблем, яка актуальна сьогодні для підприємств – це забезпечення безпеки громадян та збереження їх матеріальних та особистих цінностей. Системи контролю й керування доступом створюються, як правило, на промислових підприємствах, складських комплексах, в офісах і гаражах з метою обмеження доступу в різні зони з підвищеними вимогами до безпеки, тарифікації послуг, контролю робочого часу.

Впровадження систем контролю і управління доступом, безумовно, створює для компанії додатковий технологічний і сучасний імідж. Тому такі системи встановлюються як у банківській сфері, на об'єктах середнього і малого бізнесу (супермаркети, торговельні комплекси, готелі, приватний сектор), так і на об'єктах державного та загальносуспільного призначення (аеропорти, вокзали, прикордонні території). Незаперечною перевагою даних систем є зручність для користувача – можливість отримати доступ до різних приміщень (об'єктів), використовуючи один носій кодової інформації (у більшості випадків – картка). Різні системи електронної ідентифікації дозволяють чітко розмежувати доступ і проконтролювати дії персоналу та інших відвідувачів. Основні пристрої доступу: турнікети, електромеханічні та електромагнітні замки, засувки, шлагбауми, паркомати, веб-камери. Сучасний ринок пропонує комплекс різноманітних рішень від різних компаній-виробників, тому у покупця є широкий вибір апаратних засобів безпеки і програмне забезпечення для управління ними [1].

Питанням системи електронної ідентифікації і управління доступом користувачів присвячено багато досліджень [3-9,13]. Зокрема використання методу біометричних технологій ідентифікації спрощує процедуру аутентифікації особи та піднімає надійність системи [2,11,12]. Підсилити системи контролю можна з допомогою веб-камер, вивівши зображення в режимі реального часу [7], online пристроїв доступу або мобільних ідентифікаторів [10].

Система контролю і управління доступом – це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу / виходу та переміщень людей чи транспортних засобів на

територіях, які знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення.

За допомогою системи контролю доступу досягається:

- електронна ідентифікація осіб, що мають право доступу;
- забезпечення можливості дистанційної візуальної ідентифікації власників перепусток;
- аудит робочого часу;
- розмежування доступу до різних приміщень;
- керування автоматичними режимами;
- реєстрація часу перебування особи на об'єкті;
- обробка інформації та ведення статистики.

Основні функції системи можна назвати такі:

- організація пропуску на об'єкті;
- введення електронного обліку відвідувачів і їх реєстрація в базі;
- контроль периметра;
- формування протоколу подій;
- забезпечення дисципліни на об'єкті;
- контроль приходу / відходу співробітників підприємства, дотримання ними трудового порядку;
- контроль дій співробітників охорони, операторів;
- запобігання проникнення осіб, допуск яких до будівлі заборонений;
- запобігання проникнення на склад, у виробничий відділ або офіс осіб, доступ яким туди заборонений,
- системи відеоспостереження.

Системи електронної ідентифікації і управління доступом користувачів дають можливість забезпечити безпеку підприємства шляхом обмеження доступу в різні зони об'єкта або на весь об'єкт в цілому.

На об'єктах системи електронної ідентифікації і управління доступом користувачів здійснюються незалежно з іншими інформаційними мережами, а також може інтегруватися в чинні системи.

Викладення основного матеріалу і обґрунтування отриманих результатів.

Розрізняють централізовані та автономні системи електронної ідентифікації і управління доступом користувачів.

Централізовані системи, в яких контролери об'єднано в єдину мережу та підключено до комп'ютера, що здійснює загальне керування, що входять до складу вже наявних систем: відеоспостереження, пожежної та охоронної сигналізації. Їх встановлюють на великих офісних та промислових об'єктах з великою кількістю співробітників та відвідувачів. Система дозволяє одночасно керувати значним числом пунктів пропуску, оперативно вводити зміни до програми та додавати нові функції.

Автономні – самостійно керують роботою периферійних елементів та контролюють точки доступу. Використовуються в адміністративних, суспільних та освітніх закладах, приватних будівлях тощо. Безпосередньою перевагою автономних систем є помірна вартість та простота установлення, легке керування та надійність в експлуатації.

Автономна система – управління розрахована на незначну кількість дверей (до 20 шт.) та користувачів (не більше 50 осіб). Це ідеальне рішення для таких об'єктів, як невеличкі магазини, офісні та житлові приміщення. Програмування системи відбувається за допомогою карток.

Бездротова система – найскладніша та найуніверсальніша серед усіх. Вона передбачає і віддалене управління доступом у режимі реального часу, коли кількість користувачів у системі велика і права доступу постійно змінюються. Широко застосовується в офісах, агенціях, школах, університетах, культурних і спортивних центрах, виробничих приміщеннях тощо.

Принцип роботи

Ідентифікатор – ключовий елемент, що встановлює право доступу особи на контрольну територію. Цю функцію можуть виконувати:

- картка з магнітною смужкою;
- безконтактна картка;
- спеціальний брелок;
- цифровий код, що безпосередньо вводиться на клавіатурі;

- біометричні системи аутентифікації.

Інформація зчитується спеціальним пристроєм та передається на контролер для подальшої обробки. Зазвичай, зчитувальні пристрої виконують з урахуванням вимог підвищеного опору механічним впливам.

Контролер. На основі отриманих даних саме він приймає рішення щодо надання чи заборони доступу. Залежно від типу системи, контролер може працювати автономно чи в об'єднанні з іншими під керуванням головного комп'ютера. Для гарантованої безперервної роботи контролер забезпечено блоком резервного живлення або власним акумулятором.

Отримана інформація зберігається в пам'яті системи для подальшого використання: складання звітів, статистики, обліку робочого часу.

Додаткове обладнання: конвертори, давачі, кнопки виходу, турнікети, електронні замки, механізми доведення дверей, аларми тощо.

За потреби, до системи контролю і управління доступом може бути встановлене програмне забезпечення. Програмне забезпечення дає змогу формувати різноманітні звіти щодо користувачів, ключів, подій тощо. Поряд з цим існують і слабкі сторони таких систем, а саме – залежність від енергоживлення і необхідність проводити постійне сервісне обслуговування як апаратних, так і програмних компонентів даних систем.

Вартість обладнання та монтажу систем контролю і управління доступом залежить від конфігурації системи, кількості точок доступу, а також типів і марок використовуваного обладнання. У наведеній таблиці вказані ціни на різні системи контролю і управління доступом при реалізації їх через інтернет-компанії. Як видно з таблиці 1, в якій наведена лише мала частина комплектів систем контролю і управління доступом, використовуваних для невеликих об'єктів захисту, на ринку подібного обладнання можна вибрати модель, необхідну по функціональності, надійності і відповідно до фінансових можливостей покупця.

Таблиця 1. Тип системи контролю і управління доступом

Тип системи контролю і управління доступом	Середня вартість, грн
З доступом по електронному ТМ (TouchMemory) ключу з електромеханічним накладним замком для установки в приміщенні	1798
З доступом по телефону через інтернет з електромагнітним замком для установки на вуличні вхідні двері	3265
З відеодомофоном і викличною панеллю з доступом по електронному ТМ (TouchMemory) ключу з електромагнітним замком	5787
З доступом за відбитком пальця і карти з вологостійким електромагнітним замком для установки на ворота	10459
З онлайн-урахуванням робочого часу та доступом за відбитком пальця і карти з електромагнітним замком для установки в приміщенні	13146

Переваги використання:

- зручність і простота використання;
- забезпечення можливості дистанційної візуальної ідентифікації власників перепусток;
- доступна ціна;






Загрози і ризики:

- матеріальні втрати;
- зміна профілю доступу;
- клонування – створення нових пропусків;
- саботаж або відмова в доступі;
- правка співробітниками логів свого робочого часу;

Дослідження показали, що найбільш використовуваним з усіх біометричних методів для ідентифікації особистості (голосова ідентифікація, сітківка ока, геометрія обличчя і т.ін.) є використання відбитка пальця, оскільки ймовірність помилки при ідентифікації користувача набагато менша у порівнянні з іншими біометричними методами та сам пристрій потребує небагато місця. Використання цього методу спрощує процедуру аутентифікації особи та піднімає надійність системи в цілому.

Пропуск до приміщення працівників, допуск яких не передбачає надання чи використання тимчасової перепустки, здійснюється виключно за допомогою пластикової перепустки, що є одночасно службовим посвідченням

Таблиця 2. Порівняльна характеристика використання ідентифікаторів

Ідентифікатор	Переваги використання:	Недоліки
Мобільний ідентифікатор U-Prox BLE ID 	Зручність (смартфон завжди з Вами); Доступ в приміщення без карт; Відкривання дверей і шлагбаумів зі смартфона; Регульована дальність читання; Безпечна ідентифікація. Ціна: 0.8 \$.	Періодичне оновлення ПЗ.
Ключ-брелок з вбудованим чіпом 	Тонкий корпус, вибір кольорів; Привабливий зовнішній вигляд, Друк ID: так Можливість нанесення логотипу; Робоча температура: -30 ° C ... + 50 ° C; Температура зберігання: -40°C ... + 75°C; Розміри (мм): 37x30x3. Ціна: 0.5 \$. Носії даних (брелоки) також можна прикріпити до механічних ключів.	Проблема втрати безпеки виникає при втраті ключ-брелока.
Карта доступу IL-06M 1K 	Друк ID: немає; Кольоровий друк: так; Робоча температура: -30 ° C ... + 75 ° C; Температура зберігання: -40°C...+ 85°C; Обсяг пам'яті: 1024 байт, EEPROM; Розміри (мм): 86 x 54 x 0.76. Габаритні розміри (мм) 86 x 54 x 0.76 Вага (г) 6 Ціна: 0.5 \$.	Малий термін служби, необхідність чіткого позиціонування. Проблема втрати безпеки виникає при втраті самої картки. Тобто, залишається проблема ідентифікації самого власника картки.
Браслет для доступу IL-11ER 	Розбірний корпус; Дозволяє нанести логотип; Можливість наносити персоналізацію; Вологозахищений; Еластичний і міцний; Розмір (мм): діаметр 60; Колір: червоний, синій; Матеріал: пластик, силікон. Ціна: 2 \$.	Робітникам, які працюють на підприємстві біля станків, забороняється працювати зручним годинником або браслетом.
Сканер відбитків пальців 	Температура: -20 ° - +50 ° Розміри: 56 x 20 x 21,5 мм Ціна: 5 \$. Його зручно використовувати і не можна забути.	При механічному пошкодженні – доступ неможливий.

Авторами розроблено програмно-апаратний комплекс для тестування роботи найпоширеніших сьогодні на ринку засобів автентифікації. Комплекс використовує платформу Arduino, як найбільш недороге та водночас гнучке рішення із великою кількістю модульних датчиків та засобів фізичної ідентифікації та контролю.

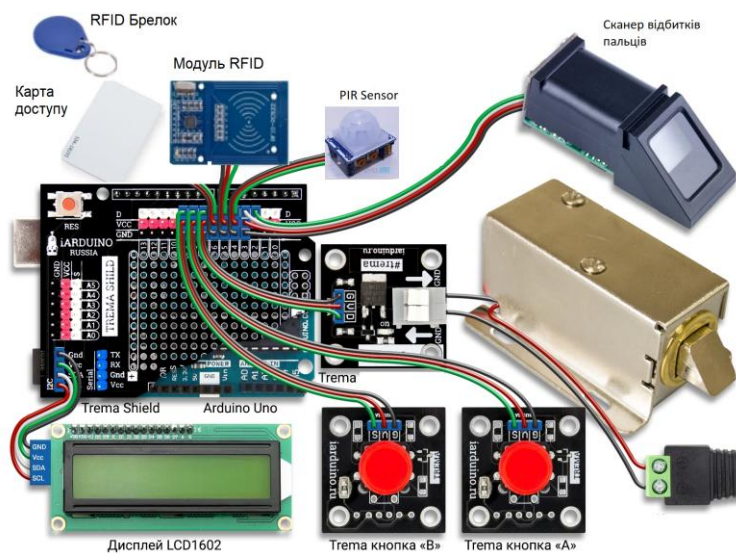


Рисунок 1. – Система контролю доступу на базі Arduino

У даному випадку розглянуто проект, що стосується системи автоматичного відкривання та закривання дверей. Система керується мікроконтролером ATmega328P та включає електромагнітний замок, який відкриває двері, ідентифікатори, РК-дисплей для відображення інформації про стан дверей, аудіо-зумер для подачі звуку протягом тривалості відкритих дверей і контролер для контролю відкривання і закривання дверей, якщо людина або предмет, виявлені датчиком. Розглянуто випадок, коли унікальний ідентифікатор ключа попередньо задається в код програми. Можна доопрацювати і розширити функціонал контролера. Наприклад, додати функцію додавання нових ключів і видалення їх з пам'яті.

Висновки

Система електронної ідентифікації і управління доступом користувачів – це один з важливих факторів питання комплексного забезпечення безпеки підприємства. Вона призначена для санкціонованого доступу співробітників і транспорту в дозволена зону об'єкта, ведення обліку робочого часу. Система контролю доступу фіксує і обробляє інформацію про кожне проходження користувача через елемент обмеження доступу, а також захищає приміщення від несанкціонованого проникнення.

Основний спосіб покращення захищеності: поєднання декількох методів ідентифікації.

Усі фактори аутентифікації мають свої недоліки і кожен окремо взятий фактор не завжди може забезпечити належний рівень захисту. Якщо виникає необхідність організувати сильний захист, стає очевидно, що потрібно комбінувати кілька факторів і використовувати їх разом.

Список бібліографічних посилань

1. Безопасность средств безопасности: СКУД [Електронний ресурс]. – Режим доступу: <https://habr.com/ru/post/277279/>. – Назва з екрану.
2. Беседіна С.В., Литвин Ю.В. Особенности разработки информационной системы идентификации особи за отпечатками пальцев // Информационная безопасность та комп'ютерні технології: Збірник тез доповідей II Міжнародної науково-практичної конференції, 20-22 квітня 2017 року, м. Кропивницький: ЦНТУ, 2017. – С. 23-24.
3. Волхонский В.В. Системы контроля и управления доступом - Санкт-Петербург: СПб: Университет ИТМО. 2015. – 105 с.
4. Гадецька З.М. Створення системи безпеки в готелях України та Черкаського регіону. – Молодий вчений – № 2 (05) – лютий, 2014 р. – С. 8-11.
5. Здолбіцька Н.В., Здолбіцький А.П., Брей В.Ю. Електронний замок на базі AT89C2051 з ідентифікатором I-Button // Тези Всеукраїнської науково-практичної інтернет-конференції Сучасні методи, інформаційне та програмне забезпечення систем управління організаційно-технологічними комплексами, 28 квітня 2015 р. – Луцьк, 2015. – С. 48-49.
6. Литвинов В. А., Николаев В. В., Голубев Л. П. Аудентифікація користувача в автоматизованих мікропроцесорних системах // Технології та дизайн. Мехатроніка, комп'ютерна інженерія та метрологія 2304-2605 № 1 (26) 2018 р. – с. 1 - 9.
7. Монашко С.Ю., Здолбіцька Н.В., Здолбіцький А.П. Arduino – проект рухомої веб-камери // Міжвузівський збірник Комп'ютерно-інтегровані технології: освіта, наука, виробництво – Луцьк: Видавництво ЛНТУ. – Вип. 15. – 2014. – С. 32–36.

8. Невлюдов И.Ш., Пономарева А.В, Бортникова В.О., Мордик А.А. Интеллектуальная система контроля и управления доступом на основе интегральных параметров. *Технология приборостроения* 3' 2016. - С. 3-6.
9. Резанов Б.М., Бульба С.С., Шокотько Д.В. Фактори аутентифікації системи контролю та управління доступом // *Кібернетична безпека. Системи управління, навігації та зв'язку*, 2017, випуск 3(43) – 63-65 с.
10. Современные Системы контроля доступа [Электронный ресурс]. – Режим доступа: http://iseoua.com/kupit/sca?gclid=CjwKCAjwsIbpBRBNEiwAZF8-z466c51YuyKs6uj_fQyGQN2G_I3JB2JdGZXB84i3PsmynC3vMPmWDBoC2PIQAvD_BwE. – Назва з екрану.
11. Столяров В.Г., Голубев Л.П. Автоматизированное удаленное управление устройствами при помощи Ардуино // *Технології та дизайн. Мехатронні системи та комп'ютерні технології*. – № 4 (21). – 2016 год. – 1-12 с.
12. Фам Зуй Тхай Некоторые вопросы применения методов сравнения отпечатков пальцев для биометрических систем идентификации личности / Зуй Тхай Фам // *Международный научно-исследовательский журнал*, №7 (38). Часть 1. – 2015. – С.127-130 [Электронный ресурс]. – Режим доступа: <http://research-journal.org/technical/nekotorye-voprosy-primeneniya-metodovsravneniya-otpechatkov-palcev-dlya-biometricheskix-sistem-identifikaciiilichnosti>.
13. Marco Schwartz. *Arduino Home Automation Projects*. – 2014. – 120 p.
14. https://uk.wikipedia.org/wiki/Система_контролю_i_управління_доступом