

УДОСКОНАЛЕННЯ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

Вінницький національний технічний університет;

Анотація

Проаналізовано засіб контролю доступу до приміщень на основі фізичних карток з можливістю обмеження часу доступу. Такий підхід дозволяє враховувати фактор часу, що мінімізує ризики несанкціонованого проникнення та підвищує ефективність системи безпеки. Особливу увагу приділено функціоналу тимчасового доступу, який дозволяє гнучко налаштовувати права доступу для окремих категорій персоналу

Ключові слова: контроль доступу, фізична картка, часові обмеження, безпека приміщень, ідентифікація персоналу, тимчасовий доступ.

Abstract

The access control method based on physical cards with the ability to limit access time has been analyzed. This approach takes into account the time factor, minimizing the risk of unauthorized entry and increasing the efficiency of the security system. Special attention is paid to the temporary access functionality, which allows flexible adjustment of access rights for specific categories of personnel.

Keywords: access control, physical card, time restrictions, premises security, personnel identification, temporary access.

Вступ

В умовах високих вимог до безпеки на підприємствах та в організаціях контроль доступу до приміщень набуває особливої актуальності. Збільшення кількості персоналу, різноманітність функціональних зон та необхідність обмеження доступу до окремих приміщень потребують впровадження ефективних та гнучких рішень. Особливо важливо мати можливість регулювати доступ окремих працівників не лише за їх посадою, але й за конкретним часовим проміжком, що дозволяє запобігти несанкціонованому перебуванню у приміщеннях..

Метою цієї роботи є покращення захисту носіїв інформації шляхом контролю доступу до приміщень на основі фізичних карток, що дозволяє забезпечити індивідуальний підхід для окремих працівників на визначений період часу, з урахуванням підвищених вимог до безпеки та ефективності функціонування підприємства.

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати існуючі системи контролю доступу;
- розробити методику контролю доступу з урахуванням часових обмежень;
- зробити висновки щодо доцільності застосування фізичних карток з обмеженим часом доступу.

Аналіз відомих систем контролю доступу

Системи контролю доступу на основі фізичних карток широко застосовуються в різних сферах для забезпечення безпеки та зручності доступу до об'єктів. Фізично ці картки виглядають як посвідчення особи або кредитні картки, але при взаємодії з пристроєм читання карток - працюють як електронний ключ [1]. Вони використовуються для обмеження доступу до приміщень на підприємствах, в офісах, готелях, паркінгах та інших місцях, де важливо контролювати переміщення осіб. Такі картки є прос-

тими у використанні, надійними та економічно вигідними рішеннями для контролю доступу.

Основною перевагою фізичних карток є їх доступність і простота в інтеграції до використовуваних систем безпеки. Зазвичай такі системи працюють на основі технології RFID або магнітних карток, що дозволяє здійснювати швидкий і зручний доступ без необхідності використання паролів або додаткових пристроїв. Вони також забезпечують можливість масштабування системи, оскільки легко додавати нових користувачів або змінювати рівні доступу без значних затрат.

Системи контролю доступу на основі карток працює на основі взаємодії кількох компонентів, що дозволяють забезпечити контроль доступу до визначених зон [2]. Вони набули широкого поширення завдяки своїй ефективності та зручності. Серед таких рішень особливу увагу привертають картки HID iCLASS SE та Ajax Pass, які пропонують різні рівні безпеки та функціональності. HID iCLASS SE вирізняється високим рівнем захисту, завдяки використанню шифрування даних, в той час як Ajax Pass є більш доступним варіантом, що використовує технологію RFID для зручного доступу [3, 4]. Обидві картки знаходять своє застосування в різних типах організацій, від великих підприємств до малих офісів, і можуть бути адаптовані під різні вимоги безпеки.

Таблиця 1 – Порівняння ефективності карток

Характеристика	Базові картки (без обмежень)	Картки з часовими обмеженнями
Тип пристрою	Безконтактна карта	Безконтактна карта
Технологія зв'язку	NFC	iCLASS (RFID, NFC)
Шифрування	AES-128 (DESFire EV1)	AES-128, AES-256 (Seos)
Інтеграція з мобільними пристроями	Немає	HID Mobile Access
Робоча температура	-25°C до +50°C	-25°C до +70°C

Як видно з таблиці 1 картки з часовими обмеженнями мають більше можливостей щодо налаштування безпеки. Проте обидва види карток не передбачають гнучкості щодо створення тимчасових правил контролю доступу до приміщень.

Удосконалення методики контролю доступу

Удосконалення методики контролю доступу передбачає впровадження системи, яка не лише обмежує доступ до приміщень за допомогою фізичних карток, але й враховує час доступу кожної особи. Такий підхід дозволяє значно підвищити рівень безпеки, оскільки забезпечує персоніфікацію доступу, де кожен працівник отримує картку з чітко визначеними часовими обмеженнями на доступ. Це особливо корисно для організацій, де існує потреба в детальній контролі за переміщенням персоналу в межах підприємства, наприклад, у випадках, коли доступ до певних приміщень повинен бути дозволений тільки на обмежений період часу, або коли потрібно уникнути несанкціонованого перебування людей у чутливих зонах.

Принцип роботи такої системи полягає в тому, що кожному співробітнику надається персональна картка з вбудованими даними, що включають, зокрема, час, в який працівник може здійснити доступ до певного приміщення. Це може бути реалізовано через спеціальні електронні картки з вбудованим чипом або RFID-технологією. Після того як працівник прикладає свою картку до зчитувача, система перевіряє, чи знаходиться поточний час у межах дозволеного періоду доступу. Якщо доступ дозволений, система відкриває замок, і працівник може потрапити в приміщення. Якщо час обмежений або не збігається із дозволеним періодом, доступ буде заблоковано, навіть якщо картка є актуальною.

Висновки

Удосконалення методики контролю доступу через використання карток з обмеженням часу доступу значно підвищує ефективність системи безпеки на підприємствах. Така система дозволяє забезпечити точний контроль за переміщенням персоналу в межах організації, мінімізуючи ризик несанкціонованого доступу та перебування у чутливих зонах. Врахування часових обмежень не тільки покращує захист, але й дає змогу гнучко налаштовувати рівень доступу для різних категорій працівників, а

також зменшувати ризики, пов'язані із втратою працівниками карток доступу.

Завдяки інтеграції з додатковими системами безпеки, такими як відеоспостереження, можна досягти ще більшого контролю та оперативної реакції на потенційні порушення. Таким чином, впровадження технологій контролю доступу з часовими обмеженнями є важливим кроком до підвищення рівня безпеки та ефективності роботи організацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Dnepr Security: Картки доступу – важливий елемент в системі контролю доступу. URL: <https://dneprsecurity.com/sovety/karti-dostupa-%E2%80%93vazhnij-aksessuar-v-sisteme-kontrolja-dostupa.html> (дата звернення: 19.03.2025).

2. Національний оператор безпеки Імперія: Система контролю доступу (СКУД). Принцип дії, склад, особливості застосування. URL: <https://imperija.org.ua/article/sistema-kontrolyu-dostupu-skud-princip-dii-sklad-osoblivosti-zastosuvannya> (дата звернення: 19.03.2025).

3. Ajax: Pass безконтактна картка керування охороною. URL: <https://ajax.systems/ua/products/specs/pass/> (дата звернення: 19.03.2025).

4. HID iCLASS SE system Express R10. URL: <https://www.hidglobal.com/products/iclass-se-express-r10> (accessed: 19.03.2025).

Кошевець Ілля Анатолійович — студент групи БКС-216, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: ilianam-ber200003@gmail.com

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Ilya Koshevets — student of the BKS-21b group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ilianam-ber200003@gmail.com

Yurii Baryshev — PhD(eng), Associate Professor of the Information Protection Department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua.