Міністерство освіти і науки України

NURE

Харківський національний університет радіоелектроніки

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2025

(Випуск 2)

[електронне видання]

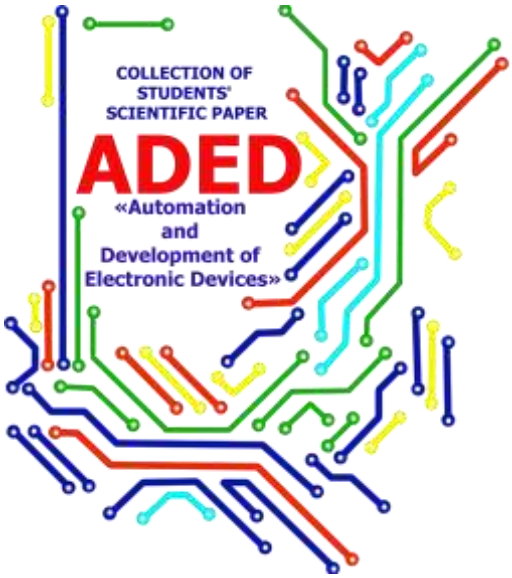
http://nure.ua/department/kafedra-komp-yuterno-integrovanih-tehnologiy-avtomatizatsiyi-ta-mehatroniki-kitam

http://itez.zntu.edu.ua/

http://kafea.kdu.edu.ua

Харків 2025

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(КІТАР)



ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2025

(Випуск 2)

[електронне видання]

Харків 2025

ЗМІСТ

УДК 004.934

АНАЛІЗ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА ПЕРСПЕКТИВИ ЇХ РОЗВИТКУ

Маруніч Р. В.
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
E-mail: rostyslav.marunich@nure.ua

***Аннотація*.** Сучасні системи контролю доступу (СКД) перетворюються з простих механічних рішень на складні інтелектуальні екосистеми. У статті проаналізовано еволюцію архітектури СКД – від автономних систем до мережевих та хмарних рішень, що забезпечують централізоване управління та масштабованість. Особливу увагу приділено аналізу сучасних методів ідентифікації: від традиційних карток RFID до безконтактної біометрії та мобільних технологій на основі NFC та BLE. На основі порівняльного аналізу різних методів аутентифікації складено детальну таблицю оцінки за критеріями надійності, зручності та вартості впровадження. Досліджено вплив штучного інтелекту на розвиток СКД, зокрема – можливості машинного навчання для виявлення аномальної поведінки та підвищення точності біометричного розпізнавання. Робота розкриває принципи конвергенції СКД з іншими системами безпеки через використання відкритих протоколів зв'язку, таких як OSDP. Встановлено перспективні напрями розвитку галузі, серед яких – інтеграція з IoT-технологіями, вдосконалення проактивних функцій безпеки та подальший перехід до безконтактних рішень. Результати дослідження пропонують практичний інструментарій для обґрунтованого вибору та впровадження СКД з урахуванням специфічних потреб сучасних підприємств.

***Ключові слова*:** система контролю доступу, СКД, біометрія, мобільний доступ, штучний інтелект, мережева архітектура, безпека.

ANALYSIS OF MODERN ACCESS CONTROL SYSTEMS AND PROSPECTS FOR THEIR DEVELOPMENT

Marunich R. V.
Kharkiv National University of Radioelectronics
Ukraine, 61166, Kharkiv, Nauky av.,14
E-mail: rostyslav.marunich@nure.ua

Abstract. Modern access control systems (ACS) are transforming from simple mechanical solutions into complex intelligent ecosystems. The article examines the evolution of ACS architecture, from standalone systems to networked and cloud-based solutions that offer centralized management and scalability. Particular attention is paid to the analysis of modern identification methods: from traditional RFID cards to contactless biometrics and mobile technologies based on NFC and BLE. Based on a comparative analysis of various authentication methods, a detailed evaluation table has been compiled, considering the criteria of reliability, convenience, and implementation cost. The impact of artificial intelligence on ACS development is explored, specifically the capabilities of machine learning for detecting anomalous behavior and improving the accuracy of biometric recognition. The work reveals the principles of ACS convergence with other security systems through the use of open communication protocols such as OSDP. Promising industry development directions have been established, including integration with IoT technologies, improvement of proactive security functions, and further transition to contactless solutions. The

research results offer a practical toolkit for informed selection and implementation of ACS, considering the specific needs of modern enterprises.

***Key words*:** Access control system, ACS, biometrics, mobile access, artificial intelligence, network architecture, security.

Стрімка цифровізація та автоматизація охоплюють усі сфери діяльності, що значно підвищує вимоги до систем безпеки, які мають бути не просто бар'єрами, а інтелектуальними компонентами інфраструктури [1-6]. Системи контролю та управління доступом (СКД або СКУД) є невід'ємною складовою комплексної системи безпеки будь-якого об'єкта, від офісних центрів до критичної інфраструктури [7]. СКД – це комплекс апаратних та програмних засобів, призначених для регулювання входу та виходу персоналу, транспорту та контролю доступу до певних зон. В умовах зростання вимог до безпеки та необхідності оптимізації бізнес-процесів, сучасні СКД еволюціонують від простих локальних рішень до інтелектуальних, мережевих екосистем.

Актуальність дослідження обумовлена стрімким розвитком технологій ідентифікації, зокрема, широким впровадженням біометрії та мобільного доступу, а також інтеграцією елементів штучного інтелекту (ШІ) для проактивного управління ризиками. Ключовою перевагою ШІ є здатність системи до постійного навчання та адаптації, що забезпечує динамічне оновлення рівнів безпеки відповідно до мінливої операційної обстановки [8-14].

Метою даної роботи є аналіз архітектурних рішень сучасних СКД, порівняння методів ідентифікації та визначення ключових трендів, що формують майбутнє галузі.

За принципом функціонування та масштабом СКД поділяються на автономні та мережеві.

Автономні СКД керують однією або кількома ізольованими точками доступу. Вони є простими, недорогими та не вимагають підключення до центрального сервера чи комп'ютера. Основним недоліком є обмежений функціонал, відсутність централізованого обліку подій та складнощі з оперативним управлінням великою кількістю користувачів.

Мережеві СКД є централізованими системами, де всі контролери підключені до єдиного сервера або хмарної платформи. Це дозволяє здійснювати централізоване управління правами доступу, моніторинг у реальному часі, збір статистики та інтеграцію з іншими системами безпеки. Узагальнена схема архітектури мережевої СКД представлена на рисунку 1.

Рисунок 1 – Узагальнена схема архітектури мережевої системи контролю доступу

Як видно з рисунка 1, ключовими компонентами мережевої СКД є: сервер СКД та база даних, які забезпечують логіку та зберігання даних; контролери, що приймають рішення про доступ на місці; зчитувачі, які ідентифікують користувача; та виконавчі пристрої (замки,

турнікети). Важливим елементом є модуль інтеграції, який забезпечує конвергенцію з системами відеоспостереження, пожежною сигналізацією та системами управління будівлею.

Сучасні СКД використовують різноманітні методи ідентифікації, які можна класифікувати за типом облікових даних:

– карткові системи, які використовують безконтактні карти (RFID, Mifare). Це найбільш поширений і економічно вигідний метод. Проте карти можуть бути втрачені, викрадені або передані стороннім особам;

– біометричні системи, що ґрунтуються на унікальних фізичних або поведінкових характеристиках людини (відбиток пальця, розпізнавання обличчя, райдужна оболонка ока). Біометрія забезпечує високий рівень надійності, оскільки облікові дані неможливо передати;

– мобільний доступ, який перетворює смартфон користувача на ідентифікатор за допомогою технологій NFC, Bluetooth Low Energy (BLE) або QR-кодів. Це забезпечує високу зручність, особливо у поєднанні з віддаленим управлінням.

Розвиток СКД визначається трьома основними напрямками: безконтактність, інтелект та конвергенція.

По-перше, використовується інтеграція штучного інтелекту (ШІ) для підвищення ефективності та безпеки СКД. Алгоритми машинного навчання можуть аналізувати шаблони доступу, виявляти аномальну поведінку (наприклад, спроби проходу «за хвостом») та проактивно попереджати про потенційні загрози. У біометрії ШІ значно покращує точність розпізнавання обличчя навіть за несприятливих умов (часткове приховування обличчя, зміна освітлення).

Також залучення безконтактної біометрії. Пандемія COVID-19 прискорила перехід до безконтактних рішень. Розпізнавання обличчя та райдужної оболонки ока стають пріоритетними методами, витісняючи контактні сканери відбитків пальців. Це підвищує гігієнічність, швидкість та зручність проходу.

Паралельно з біометрією активно розвиваються технології мобільної ідентифікації, що поєднують зручність безконтактного доступу з персоналізацією через особисті пристрої користувачів. Мобільні облікові дані та хмарні рішення. Смартфони стають основним засобом ідентифікації. Хмарні платформи (SaaS) дозволяють компаніям управляти доступом з будь-якої точки світу, знижуючи витрати на локальну інфраструктуру та забезпечуючи легке масштабування. Це особливо актуально для розподілених підприємств [1, 15].

Однак поява таких розрізнених хмарних та мобільних рішень гостро ставить питання про їхню ефективну інтеграцію з іншими компонентами безпеки [16]. Ця потреба знаходить свою реалізацію в глобальному тренді – конвергенції систем безпеки.

Конвергенція систем безпеки. Сучасні СКД інтегруються з іншими системами безпеки для створення єдиної платформи управління. Наприклад, при спробі несанкціонованого доступу СКД може автоматично активувати камери відеоспостереження для запису події, а також сповістити охоронну службу. Використання відкритих протоколів, таких як OSDP (Open Supervised Device Protocol), забезпечує безпечну та надійну комунікацію між компонентами різних виробників.

Для прийняття рішення про вибір СКД важливим є порівняння основних методів ідентифікації за ключовими критеріями (табл. 1).

Сучасні системи контролю доступу є динамічною галуззю, що активно впроваджує передові технології для забезпечення безпеки та ефективності. Перехід від автономних до мережевих та хмарних рішень забезпечує централізоване управління та масштабованість. Ключові тренди, такі як безконтактна біометрія (особливо розпізнавання обличчя), мобільний доступ та інтеграція ШІ, свідчать про рух у напрямку більш надійних, зручних та інтелектуальних систем [12, 17].

Таблиця 1 – Порівняльний аналіз сучасних методів ідентифікації

Метод	Надійність (Стійкість до підробки)	Швидкість і Зручність	Вартість Обладнання	Ключові Недоліки
Картки (RFID)	Середня (легко втратити/передати)	Висока (швидке зчитування)	Низька	Ризик передачі карти, необхідність постійного носіння
Код (PIN)	Низька (легко підглянути/забути)	Низька (повільне введення)	Дуже низька	Низька безпека, можливість підбору
Відбиток пальця	Висока (унікальність)	Середня (потребує контакту)	Середня	Чутливість до стану пальця, гігієнічні міркування
Розпізнавання обличчя	Дуже висока (завдяки ШІ)	Дуже висока (безконтактно)	Висока	Висока вартість, потенційні проблеми з приватністю
Мобільний доступ (BLE/NFC)	Висока (захист смартфона)	Висока (безконтактно)	Середня	Залежність від заряду батареї смартфона

Тож, перспективи розвитку СКД пов’язані з подальшою конвергенцією з іншими інженерними системами будівлі (IoT, BMS) та поглибленням аналітичних можливостей ШІ, що дозволить перейти від реактивного контролю до проактивного управління безпекою. Вибір конкретної СКД має ґрунтуватися на комплексному аналізі вимог до надійності, зручності та бюджету, з урахуванням довгострокової стратегії розвитку підприємства.

У ході проведеного дослідження було проаналізовано архітектуру систем контролю доступу та ключові тенденції їх розвитку. Дослідження підтвердили, що СКД еволюціонують від ізольованих фізичних рішень до інтегрованих інтелектуальних екосистем. Було встановлено, що перехід до мережевих та хмарних архітектур є фундаментальним, оскільки він забезпечує централізоване управління, масштабованість та віддалений контроль, що особливо критично для розподілених підприємств.

Порівняльний аналіз методів ідентифікації виявив чітку тенденцію до поєднання високої надійності та зручності. Біометричні технології, зокрема безконтактне розпізнавання обличчя, та мобільний доступ демонструють переваги перед традиційними картковими рішеннями, пропонуючи вищий рівень безпеки та гігієні. Доведено, що інтеграція штучного інтелекту є вирішальним фактором для підвищення ефективності СКД, оскільки надає системам здатність до проактивного аналізу ризиків, виявлення аномалій та адаптації до мінливої обстановки.

На основі порівняльного аналізу методів аутентифікації було розроблено детальну таблицю з оцінкою їх ефективності за критеріями надійності, зручності та вартості. Ця таблиця може слугувати практичним орієнтиром при виборі оптимального методу ідентифікації для конкретних умов експлуатації.

Було системно визначено та охарактеризовано три ключові напрями розвитку сучасних СКД: безконтактність, інтелектуалізація та конвергенція. Для кожного напряму встановлено конкретні технологічні рішення, такі як безконтактна біометрія, мобільний доступ на основі BLE/NFC, алгоритми ШІ для аналізу поведінки та протокол OSDP для інтеграції. Це дозволяє формувати обґрунтовані вимоги до сучасних та перспективних систем безпеки.

Дослідження також підтвердило ефективність архітектури мережевих та хмарних СКД для централізованого управління розподіленими об'єктами. Встановлено, що саме така архітектура, поєднана з модулем інтеграції, забезпечує основу для створення єдиної платформи безпеки, що є практичною відповіддю на сучасні виклики.

ЛІТЕРАТУРА:

1. Achkan, M. S., et al. Integration of cloud technologies into modern SCADA systems: prospects and challenges // «Computer-integrated technologies, automation and robotics» CITAR-2025. – 2025. – pp. 26-29

2. Сотник, С. Розробка автоматизованої інформаційно-пошукової системи вибору маніпулятора промислових роботів // Електромеханічні і енергозберігаючі системи. – 2025. – № 1 (68). – С. 52-58. https://doi.org/10.32782/2072-2052.2025.1.68.6

3. Sotnik, S., et al. Evaluating relational database scaling strategies in web engineering // International Conference on Advanced Trends In Radioelectronics and Infocommunications (ATRIC-2025) (May 21–22, 2025), Lviv Polytechnic Publishing House, Lviv, Ukraine. – 2025. – pp. 224-228

4. Shrubkovskyi, Y. V., et al. Development of a structural scheme for automatic dosing of liquid components // Період трансформаційних процесів в світовій науці: задачі та виклики: збірник наукових праць з матеріалами V Міжнародної наукової конференції, м. Кропивницький, 6 червня, 2025 р. / Міжнародний центр наукових досліджень. – Вінниця: ТОВ «УКРЛОГОС Груп. – 2025. – pp. 242-246

5. Cherednichenko, T., et al. Features of automatic working time control systems // Manufacturing & Mechatronic Systems 2025: Proceedings of IX st International Conference, Kharkiv, October 25-26, 2025: Thesises of Reports. – 2025. – pp. 54-57

6. Sotnik, S. Development of a range measurement module on an ultrasonic sensor with a GSM module // Radio Electronics, Computer Science, Control. – 2025. – 2. – pp. 32-44. https://doi.org/10.15588/1607-3274-2025-2-3

7. Vasylchenko, Y., et al. Development of Security and Fire Alarm Integrated Automation System at Enterprise // WSEAS Transactions on Systems. – 2025. – 24. – pp. 642-664. https://doi.org/10.37394/23202.2025.24.56

8. Marunich, R.V., et al. Modern IoT technologies for creating automated access systems // Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports. – 2025. – pp. 38-39

9. Marunich, R.V., et al. Features of IoT application in the security sector // «Computer-integrated technologies, automation and robotics» CITAR-2025. – 2025. – pp. 80-84

10. Polikanov, K. A., et al. Overview of modern technologies for residential automation // «Computer-integrated technologies, automation and robotics» CITAR-2025. – 2025. – pp. 85-89

11. Khalimonov, Y. I., et al. Overview of computer vision areas application for inspection and quality control // Комп'ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві : матеріали всеукр. наук.-практ. конф. здобувачів вищ. освіти і молодих учених, 20 листоп. 2024 р. / Харків. нац. автомоб.-дор. ун-т. – Харків. – 2024. – С. 117-121

12. Lykho, T.A., et al. Pattern recognition and computer vision technologies in decision support systems of robotic systems // Proceedings of the XVII International scientific and practical conference «Information technologies and automation – 2024», 2024. – pp. 645-648

13. Khalimonov, Y., et al. Approaches to ensuring proper working conditions using sensor technologies IoT // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024». – 2024. – pp. 24-25

14. Polikanov, K., et al. Smart home with house module: overview of automation technologies // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024». – 2024. – pp. 20-21

15. Nevludov, I. S., et al. Cloud giants: AWS, Azure and GCP // 2023 2nd International Conference on Innovative Solutions in Software Engineering Ivano-Frankivsk. – 2023. – pp. 18-24

16. Sotnik, S. Integration of IoT into security systems: opportunities and risks // International Journal of Academic Engineering Research (IJAER), 2024. – Vol. 8, Issue 11. – pp. 56-61

17. Abu-Jassar, A. T., et al. Some Features of Classifiers Implementation for Object Recognition in Specialized Computer systems // TEM Journal. – 2021. – 10(4). – pp. 1645-1654. https://doi.org/10.18421/TEM104-21