

О. В. Айко^{1,a}, О. Д. Василенко¹, В. М. Степаненко¹

Анотація

Ключові слова: системи контролю доступу, безпека підприємства

Системи контролю доступу (СКД) (рис. 1)[1] стали необхідним елементом безпеки для різних типів підприємств у сучасному світі. Забезпечення доступу до об'єктів та інформації має критичне значення для збереження конфіденційності та запобігання недозволеному втручанню. Великі, середні, малі та мікропідприємства потребують індивідуального підходу до впровадження систем контролю доступу, враховуючи їхні особливості та потреби.



Рис. 1. Схема СКД

^aaiko.alexenader@gmail.com

Рис. 2. Засоби ідентифікації

Отримані результати можуть бути корисними для організацій, які планують впровадження систем контролю доступу, дозволяючи їм обрати оптимальний варіант відповідно до своїх потреб та можливостей.

З метою забезпечення ефективності та безпеки роботи підприємства, використання систем контролю доступу стає надзвичайно важливим аспектом. Кожен тип підприємства має свої особливості та вимоги до забезпечення безпеки. Наприклад, для великих корпорацій можуть бути важливі масштабованість та централізоване керування доступом, тоді як для малих та середніх підприємств можливо більше підійде більш проста та економічна система контролю доступу. Отже, вибір системи контролю доступу (рис. 3) повинен відповідати конкретним потребам та можливостям кожного підприємства.

Крім того, у світі зростаючої кількості кіберзагроз та вимог до збереження конфіденційності, важливою стає інтеграція сучасних технологій, таких як біометрична автентифікація, у системи контро-



Рис. 3. СКД



Рис. 5. Картка із штрих-кодом

лю доступу. Це дозволяє підвищити рівень безпеки та запобігти недозволеному доступу до об'єктів та інформації.

Таким чином, дослідження особливостей та можливостей систем контролю доступу для різних типів підприємств є актуальним та важливим завданням. Розуміння принципів роботи та вибір оптимальної системи контролю доступу допоможе підприємствам забезпечити ефективну та безпечну роботу своїх працівників та зберегти конфіденційність важливої інформації

1. Огляд систем контролю доступу (СКД)

Системи контролю доступу (СКД) [2] [3] - це комплексні технологічні рішення, спрямовані на забезпечення безпеки об'єктів та контролю доступу до них. Основним принципом роботи СКД є обмін інформацією між електронними пристроями (рис.4) [4], які автоматично перевіряють право доступу особи до об'єкта.

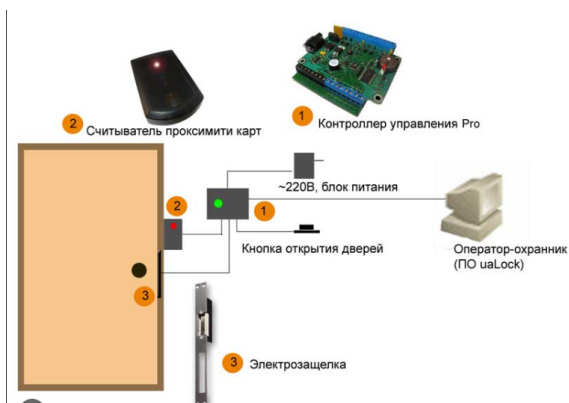


Рис. 4. Схема СКД

Основні типи СКД включають в себе карткові системи (рис. 5) [5], біометричні системи, та системи ідентифікації за допомогою PIN-кодів або паролів [6].

Засоби ідентифікації та компоненти СКД є важливими для забезпечення безпеки підприємств [7], оскільки вони дозволяють відокремити доступ (рис. 6) до об'єктів лише для авторизованих осіб, що зменшує ризик несанкціонованого доступу та випадків порушень безпеки.



Рис. 6. Турнікет-трипод

2. Класифікація підприємств

1. Великі підприємства:

- Характеризуються великим обсягом працівників та територією.
- Вимагають складних інтегрованих систем контролю доступу з високим рівнем безпеки.
- Вимоги до СКД: висока швидкість реакції системи, можливість інтеграції з іншими системами безпеки.

2. Середні підприємства:

- Мають помірний обсяг працівників та території.
- Зазвичай використовують стандартні СКД з можливістю розширення.
- Вимоги до СКД: надійність, простота в установці та обслуговуванні.

3. Малі підприємства:

- Мають обмежений обсяг працівників та території.
- Використовують прості та витратні ефективні СКД.
- Вимоги до СКД: вартість, простота в установці та використанні.

4. Мікропідприємства:

- Мають невеликий обсяг працівників та території.
- Використовують прості СКД, які можуть бути легко розгорнуті та керовані.
- Вимоги до СКД: низька вартість, простота в установці та ефективне використання.

3. Оцінка ефективності СКД для різних типів підприємств

1. Аналіз загальної структури СКД:

Дослідження показало, що ефективність СКД в значній мірі залежить від правильної організації їх структури. Основними компонентами є контролер доступу, читачі карток або біометричних даних, програмне забезпечення для управління та база даних для зберігання інформації про доступ. Інтеграція цих компонентів у єдину систему дозволяє ефективно контролювати доступ до об'єктів підприємства.

2. Порівняння структур СКД для різних типів підприємств та їх вартості:

Виявлено, що великі підприємства зазвичай потребують більш складних та коштовних систем контролю доступу через великий обсяг приміщень та персоналу. Важливо підкреслити, що вартість системи повинна відповідати потребам та можливостям підприємства.

3. Експертний аналіз систем біометричної автентифікації:

Було проведено експертний аналіз систем біометричної автентифікації, який показав їх високу ефективність у визначенні особи за унікальними фізичними характеристиками. Такі системи є надійними та складають основу для безпечного контролю доступу на підприємствах різних типів. Ці аспекти дослідження демонструють значення правильного підбору та налагодження систем контролю доступу для різних типів підприємств, що сприяє підвищенню їх ефективності та безпеки.

Висновки

Дослідження особливостей застосування систем контролю доступу (СКД) для різних типів підприємств виявило ряд ключових висновків. Перш за все, ефективне використання СКД може значно підвищити рівень безпеки та контролю над доступом до об'єктів та інформації на підприємствах. Виявлено, що великі, середні, малі та мікропідприємства мають свої унікальні вимоги до СКД, врахування яких дозволяє максимально використовувати переваги цих систем.

Однак, разом з перевагами використання СКД та-

кож виникають потенційні проблеми. Зокрема, важливо враховувати витрати на впровадження та підтримку систем, а також забезпечити сумісність із вже існуючими інформаційними та технічними системами підприємства.

Практична цінність результатів дослідження полягає в можливості визначення оптимальних стратегій впровадження та підтримки СКД для підприємств різних типів. Рекомендації щодо впровадження СКД мають спрямовуватися на максимальне врахування потреб і можливостей конкретного підприємства, а також забезпечення найвищого рівня безпеки при оптимізації витрат.

У майбутньому, дослідження в цій області може включати розробку більш деталізованих методик оцінки ефективності та вибору СКД для різних типів підприємств, а також дослідження нових технологій та методів автентифікації для поліпшення безпеки та зручності використання систем контролю доступу.

Перелік використаних джерел

1. *Ohvana.ua*. Що таке СКУД? — URL: <https://ohvana.ua/uk/stati-i-obzory/chto-takoe-skud.html> ; (дата звернення: 05.06.2023).
2. Юдін О. К., Весельська О. М. Аналіз та класифікація систем контролю та управління доступом на підприємстві // Наукові технології. — 2018. — С. 220—221.
3. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. — Москва : Горячая линия - Телеком, 2010. — С. 272.
4. Проксimiti карта Satel KT-STD-2. — URL: <https://smartel.ua/ua/product/proksimitikarta-satel-kt-std-2/>. Електронний ресурс.
5. Пластикові картки зі штрих-кодом та номером. — URL: <https://www.50kopeek.kiev.ua/ua/uslugi/kartochki-numeraciya-shtrih-kodom/>. Електронний ресурс.
6. Роговий М. Дослідження особливостей використання охоронних СКУД // Харківський національний університет радіоелектроніки. — 2019. — С. 23—40.
7. Whitman M. E. Principles of information security. — Cengage Learning, 2012.