С.В. Устенко, *д.е.н., професор*
А.В. Солодкий, *магістр*

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ БЕЗПЕКОЮ ОФІСУ

Сучасний офіс являє собою приміщення, яке призначене для роботи певної кількості людей з урахуванням складного технологічного середовища, паркувальної та приофісної зони. Ніхто в офісі не застрахований від випадків затоплення, вимкнення світла, займання, проникнення сторонніх осіб тощо. Відбуваються багато процесів, які можуть залишитися непоміченими й завдати великої шкоди працівникам, офісному приміщенню та орендарю загалом. Все це вимагає застосування ефективних та інноваційних підходів для забезпечення та контролю безпеки як офісного персоналу, так і офісу загалом, для чого і призначені системи контролю та управління безпекою офісу.

Мета роботи – розкрити призначення системи контролю та управління безпекою офісу, проаналізувати існуючі системи та комплекси, розглянути та проаналізувати новітні розробки у цьому напрямку, представити архітектурні рішення таких систем з використанням новітніх технологій.

Огляд систем контролю та управління безпекою офісу. Система контролю та управління безпекою офісу є програмно-апаратним комплексом, в якому об'єднуються різні види підсистем, технології, заходи для забезпечення безпеки персоналу, обладнання та інформації в офісному приміщенні. Модульна структура систем такого типу дає змогу інтегрувати її в офіси різних розмірів, використовуючи різні підсистеми, що визначають ключові аспекти безпеки офісу. Серед них є:

- система контролю і управління доступом (СКУД);
- системи охоронної сигналізації;
- система відеоспостереження;
- системи пожежної безпеки та пожежогасіння;
- системи моніторингу водопостачання;

- системи моніторингу якості повітря;
- системи безперебійного живлення тощо

Вони об'єднуються в одну керовану екосистему за допомогою багатьох компонентів, таких як сервер, ПЗ, центрів керування підсистемами, що покращує контроль та прискорює швидкість реагування на небезпеку чи непередбачені ситуації. Також для об'єднання використовують інтерфейс RS-485, Wi-Fi, Ethernet та GSM. Програмне забезпечення таких систем дозволяє зручно налаштовувати та підключати модулі, датчики та інші компоненти. Також дає змогу зручно відстежувати та керувати безпекою офісу з різних пристроїв на кшталт смартфону, комп’ютеру, планшету, налаштовувати систему, створювати різні сценарії для передбачення та запобіганню небезпекам. Подібні системи широко використовуються в офісних, промислових приміщеннях, домівках й називаються інтегрованими системами безпеки, які передбачають спільне використання ресурсів підсистем (пожежної та охоронної сигналізації, відеоспостереження, систем контролю управління доступом), в результаті чого система як ціле набуває нових якісних властивостей, на відміну від автономної роботи підсистем[1]. В публікації [2] дослідженні особливості використання охоронних СКУД”, а система визначається як «сукупність сумісних між собою апаратних і програмних засобів, спрямованих на обмеження і реєстрацію доступу людей, транспорту і інших об'єктів в, або з приміщення, будівлі, зони і території тощо».

Незважаючи на всі переваги, інтеграція, проектування та впровадження таких систем безпеки може потребувати чималих коштів, що може стати обмежуючим фактором для деяких компаній з обмеженим бюджетом. Також потрібно залучати висококваліфікованих спеціалістів для підтримки та обслуговування.

Масштаби охоронюваного об’єкту, кількість співробітників на пряму визначають архітектуру необхідної СКУД, яка буває автономною та мережевою.

Архітектурні рішення. ***Автономна СКУД*** (рис. 1) характеризується використанням одного або декількох незалежних контролерів і відсутністю головного контролера – серверу системи. Кожен з них знаходиться на своєму пропускному пункті та виконує функцію контролю та управління доступом для певного об’єкту. Обмін даними між контролером, зчитувачем та виконавчим пристроєм відбувається через інтерфейси RS-485 та RS-232. При цьому налаштування кожного контролера здійснюється окремо. Зважаючи на те, що контролери зазвичай встановлюються в важкодоступних місцях і враховуючи можливу кількість дверей та співробітників на підприємстві, стає зрозумілим, що такий підхід підходить лише для невеликих об'єктів.

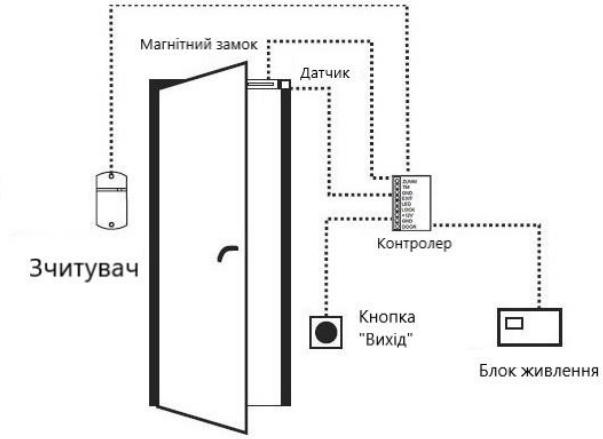

Рисунок 1 - Загальна схема автономної СКУД

Джерело: розроблено авторами

Запропонована також ***мережева архітектура СКУД***, яка має у своєму складі центральний контролер – сервер управління, з яким з’єднані всі локальні контролери, з якими відбувається обмін інформацією. Для побудови мережевої СКУД потрібно прокласти кабельні траси для забезпечення інформаційного зв'язку контролерів. Однак, при використанні мережевого інтерфейсу Ethernet для забезпечення інформаційного зв’язку, з’являється можливість використання існуючої на об'єкті комп'ютерної мережі. В систему входить мікроконтролер, двері з електромеханічним замком, зчитувач, карта доступу та сервер управління з програмним забезпеченням СКУД. Мережеві системи контролю доступу можуть бути інтегровані з системами

відеоспостереження, що дозволяє прив'язувати записи подій до відеозаписів відповідних камер, а також із системами охоронно-пожежної сигналізації.

Список використаних джерел

1. Litvinchuk I. Спосіб оцінювання інтегрованих систем безпеки на об’єкті інформаційної діяльності [Електронний ресурс] / I. Litvinchuk, N. Korshun, M. Vorokhob // Електронне наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 135–143. – 2020. – Режим доступу до ресурсу: https://doi.org/10.28925/2663-4023.2020.10.135143.

2. Роговий М. І. Дослідження особливостей використання охоронних СКУД [Електронний ресурс] / Роговий М. І. – 2019. – Режим доступу до ресурсу: http://openarchive.nure.ua/handle/document/10963.