УДК 681.52

Андреєв П.І., магістрант, гр.АТ-23м
Державний університет «Житомирська політехніка»,
Степаняк М.В., канд .техн. наук, доцент кафедри КСА ІКТА
НУ «Львівська політехніка»

ПРИСТРІЙ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ДО ОБ'ЄКТА

Сьогодні збільшився об'єм крадіжок особистого і державного майна в багатьох організацій та приватних осіб. Це актуальна проблема, особливо для великих компаній, де провал засобів захисту може завдати істотної матеріальної шкоди підприємствам та їх клієнтурі. Через те цим організаціям слід надавати виняткову увагу заходам безпеки. В результаті виникає проблема захисту й контролю доступу в приміщення. І тепер ця проблема є поєднанням тісно пов'язаних допоміжних видів діяльності в галузі права, організації, управління, технології, програмування і математики. Однією з ключових задач при розробці системи безпеки є надійне й ефективне управління доступом до об'єкта захисту.

Мета роботи - розробка системи контролю й управління доступом (СКУД) до об'єкта. Для досягнення даної мети було сформульовано наступні завдання: зробити аналітичний огляд аналогічних технічних рішень; провести вибірку і обґрунтування технічних норм системи; розробити архітектуру системи; розробити принципову схему; алгоритм програми, що керує; розробити структуру друкованої плати.

Структурна схема даної СКУД представлена на рис 1. Безпека ідентифікації користувача полягає в наступному. Користувач доторкається особистим ідентифікатором до адаптера. Мікроконтролер перериває робочу програму, та починає зчитувати 64-бітний код з ідентифікатора. Потім код переправляється на панель управління (ПУ), де він порівнюється з кодами, які знаходяться в таблиці авторизації. У випадку відповідності цей сигнал надходить в мікроконтролер, щоб відкрити перші двері шлюзу.

Встановлення автентичності користувача відбувається в шлюзі, тобто його автентифікація.

При проходженні користувача через шлюз, на панелі управління записуються наступні елементи: час, дата і напрямок проходження користувача. Вся отримана інформація відмічається та записується в базі даних ПК. СКУД має режим аварійної роботи. У випадку пожежі

вмикається пожежний сповіщувач, з якого відправляється сигнал в МК.

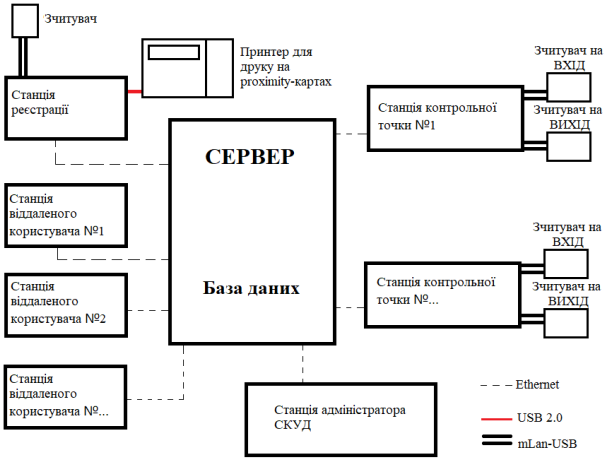

Рис. 1. Структурна схема СКУД

Мікроконтролер посилає сигнал до двох пристроїв управління, які вмикають електродвигуни і двері шлюзу відчиняються. У цей час на панель управління також подається сигнал тривоги. При виникненні будь-якої екстремальній ситуації в СКУД диспетчер спроможний за власною ініціативою відкрити шлюз. Окрім того, він забезпечує автономну роботу контролерів в наступних ситуаціях: мережевий кабель відключений або комп'ютер не відповідає; струм відсутній. У всіх випадках двері шлюзу заблоковані, і мікроконтролер переходить в сплячий режим, поки не отримано відповіді від комп'ютера або не відновлене живлення.

СКУД діє так, що процедури виявлення вмикаються в разі порушення графіка роботи. Іншими словами, коли ви намагаєтесь вручну відчинити двері або саботувати датчики мікроконтролера, запускаються процедури виявлення, щоб визначити клас порушення та повідомити про це панелі управління. Усі спроби вторгнення контролюються МК. Однак, за умови входження зловмисника до шлюзу, всі системи будуть заблоковані до прибуття адміністратора або служби безпеки.

Усяка спроба несанкціонованого доступу до об'єкта захисту через СКУД реєструється на панелі управління. Зберігається та вноситься до архіву бази даних пам'яті комп'ютера: час, номер і тип порушення правил роботи системи. Якщо порушення сталося по вині авторизова-

ного користувача, інформація про порушення записується на ім’я користувача.