УДК 004.056.5

В. В. Кравчик

РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ З ВИКОРИСТАННЯМ GSM-МОДУЛЯ ТА RFID-МІТОК

Вінницький національний технічний університет

Анотація

У даній статті розглянуто методи та засоби контролю доступу. Було здійснено огляд існуючих аналогів, що представленні на ринку, а також постановка задачі. Було реалізовано на практиці охоронну систему з елементами контролю доступу.

Abstract

In this article it was consider t methods and means of access control. There will be a review of existing analogues available on the market, as well as setting goals. It was implemented in the practice of a security system with elements of access control.

Вступ

Останнім часом, проблеми безпеки все більше постають у різних сферах життя. Системи контролю і управління доступом (СКУД) міцно зайняли своє місце в переліку технічних систем безпеки.

СКУД, це сукупність програмно-технічних засобів і чітко сформованої системи управління всім пересуванням персоналу.

Захист будь-якого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим рубежем буде СКУД.

Результати дослідження

Система контролю і управління доступом призначена для автоматичного управління входом і виходом людей в будівлі і приміщення організації, в'їздом і виїздом транспорту на територію. Установка СКУД, дозволить забезпечити більш високий рівень безпеки на підприємстві. З'являється можливість отримання точної інформації про дотримання робочого графіка співробітниками, гнучкого завдання режимів доступу, обліку і контролю робочого часу, обмеження доступу та т.п.

СКУД забезпечує виконання таких основних функцій:

– відкривання дверей при зчитуванні ідентифікатора, доступ по якому дозволено в дану зону доступу (приміщення) в заданий часовий інтервал або по команді оператора СКУД;

– санкціоноване зміна (додавання, видалення) ідентифікаційних ознак і зв'язок їх з зонами доступу (приміщеннями) і часовими інтервалами доступу;

– захист від несанкціонованого доступу до програмних засобів для зміни (додавання, видалення) ідентифікаційних ознак;

– захист технічних і програмних засобів від несанкціонованого доступу до елементів управління, встановлення режимів і до інформації;

– збереження налаштувань і бази даних ідентифікаційних ознак при відключенні електроживлення;

– реєстрацію та протоколювання поточних і тривожних подій;

– автономну роботу зчитувача з УПУ в кожній точці доступу при відмові зв'язку з УУ.

Першою і основною частиною приладу є - це контроль доступу до приміщення. Це потрібно для того, щоб стороні люди не могли потрапи до приміщення без дозволу. Також зменшити ризик, того що хтось зможе заволодіти певною інформацією. Оскільки захищати конфіденційну

інформацію і не тільки можна великою кількістю різних засобів і способів, одним з яких є контроль доступу.

Другою частиною приладу виступає система сигналізації, яка може використовувати різноманітні сенсори і датчики для контролю периметру приміщення. Наприклад датчики руху, удару, диму, лазери, полум'я, відкриття та інші. Такий великий діапазон різноманітних датчиків потрібно, для того, щоб можна було покрити різні потреби споживача.

Можна сказати, що це гібридна система, оскільки вона включатиме в себе контроль доступа і систему сигналізації. Це потрібно, щоб покрити одразу два важливих моменти – це менеджети фізичний доступ, а також мати інформації, якщо хтось проникне в приміщення в час, коли нікого немає в приміщенні.

На ринку таких гібридних систем немає. Зазвичай вони розділені на два окремих прилади. Які не можуть мати інформації один від одного. Тому це комфортно, оскільки за потреби можна дізнатися чи зловмисник намагається потрапити до приміщення видаючи себе за авторизованого користувача. Існуючі системи не можуть дати одна одній такої інформації, оскільки вони абсолютно не зв'язані між собою ніякими способами.

Даний прилад буде мати ряд переваг, наприклад це те, що сигналізація може спілкуватися з блоком контролю доступу. Також до даної системи можна підключити велику кількість найрізноманітніших датчиків і сенсорів. Легкий контроль і налаштування доступу до приміщення. Простота використання приладу і його низький бюджет для створення. Одним словом, даний прилад універсальний, в рази дешевший за існуючі аналоги, також він набагато гнучкіший для використання і доопрацювання в подальшому.

Першими кроками є створення самої структурної моделі приладу. Тобто, з чого буде складатися прилад і як дані частини будуть зв'язані між собою. Далі потрібно обрати конкретні деталі, мається на увазі контролер, датчики які будуть використовуватися, пасивні радіодеталі і тому подібно. І з основних частин, а конкретніше останньої частини яка завершує даний етап проектування приладу перед написання самої логіки роботи приладу - є створення принципової схеми. Дана схема буде показувати як модулі і деталі будуть з'єднані між собою в подальшому[30].

Сигнальний пристрій або система сигналізації створюють звукову, візуальну або іншу форму сигналу тривоги про виникнення проблеми або певного стану.

Сигнальні пристрої – спеціальні пристрої в яких активізація відбувається при виникненні надзвичайної ситуації. Сигнальні пристрої бувають:

– звуковими (сирени);
– світловими (світлові сповіщувачі);
– голосовими (голосові додзвонювачі);
– цифровими (цифрові комунікатори);
– комбінованими (поєднують у собі ознаки звукових та світлових сповіщувачів тривоги).

Для початку потрібно зробити схему приладу сигналізації (рисунок 2.1). На даній структурній схемі показаний загальний принцип роботи приладу, а саме отримання і передача

сигналів між мікроконтролером, GSM модулем. RFID зчитувачем, датчиками та звуковим оповіщувачем.

Зі схеми видно, що GSM модуль та мікроконтролер спілкуються в дві сторони. Це слугує тому, що є можливість за допомогою дзвінка на GSM модуль керувати сигналізацією віддалено. Головною можливістю даної функції слугує перевірка стану сигналізації на даний момент часу.

Наступним кроком буде розроблення блок схеми роботи сигналізації, яка знаходиться в додатку Б. Із даної блок схеми можемо зробити такий висновок, що після запуску системи йде опитування заданих портів сигналізації для перевірки їх працездатності.

Наступним кроком йде введення коду активації сигналізації з клавіатури і перевірка його вірності. Після введення вірного коду, сигналізація стає в режим готовності і чекає поки не закриються двері. Після закриття дверей активується сигналізація.

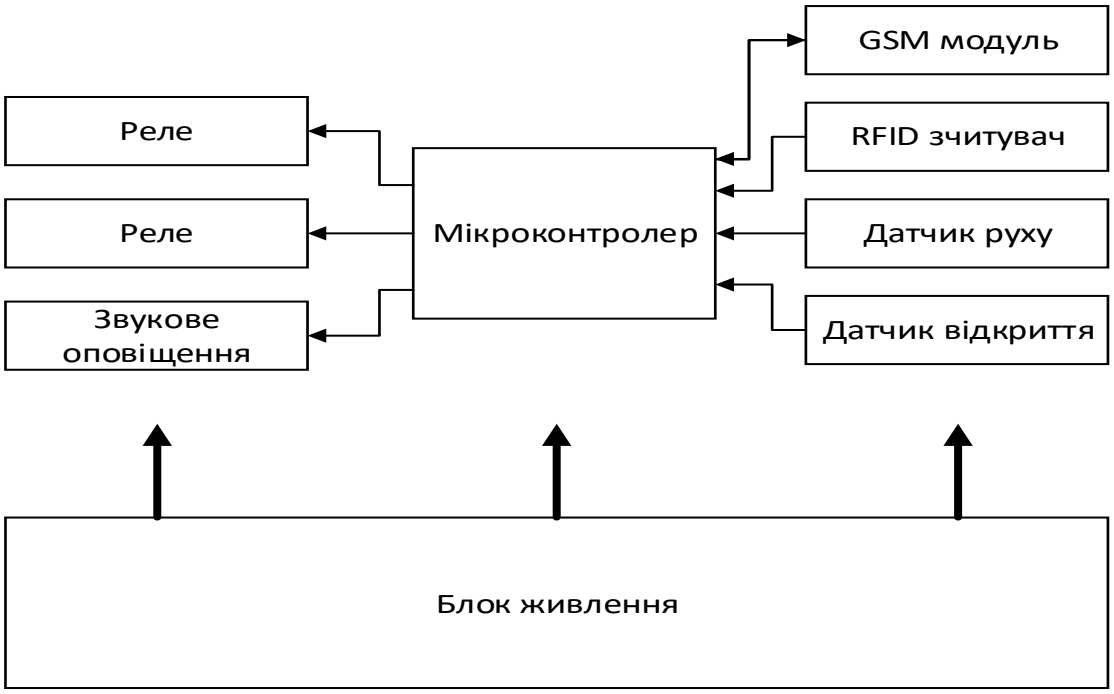

Рисунок 2.1 –Схема сигналізації

В режимі активної сигналізації, мікроконтролер постійно опитує всі датчики на їх спрацювання. Якщо один із датчиків спрацював, вмикається затримка часу після закінчення якої спрацює звуковий оповіщувач. Допоки не закінчиться затримка є можливість ввести код для деактивації сигналізації.

Якщо після спрацювання датчика не був введений в період затримки часу вірний код деактивації сигналізації, вмикається звуковий оповіщувач. Для вимкнення оповіщувача та деактивації сигналізації, потрібно ввести код з клавіатури.

Висновки

У ході виконання роботи було здійснено аналіз можливих варіантів несанкціонованого проникнення до приміщення, також було досліджено вразливі місця в охоронній системі, власне підміна RFID карток користувачів. Створено модель охоронної системи, наведено критерії її оцінки та методи перевірки. Запропоновано способи та методи захисту приміщення від витоку інформації по іншим каналам, яких не охоплює дана система, а також критерії оцінки об'єкту захисту.

Отже використання данної системи доцільне для установ та підприємств, де потрібно обмежити доступ та проводити аудит переміщення персоналу на об'єкті. Наступними кроками є: подальша модернізація системи для покращення її технічних характеристик, а також розширення функціональності продукту для різних потреб споживача.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Reynolds M. «Microwave RFID: Passive Scattering and Active Transponders», MIT, 2002.
2. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
3. RFID технология. [Електронний ресурс]. – Режим доступу: https://www.cleverence.ru/articles/rfid/rfid-tekhnologiya-chto-eto-takoe-kak-rabotaet-sistema-opisanie-i-primenenie/

Кравчик Володимир Володимирович — студент групи УБ-16б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: 27251607vova@gmail.com

Kravchyk Volodymyr V.— Management and information security Department student, Vinnytsia National Technical University, Vinnytsia, email : 27251607vova@gmail.com