УДК 004.056
DOI: 10.31673/2409-7292.2020.044650

Омельченко М.О.

ХАРАКТЕРИСТИКА ТА ЗАГАЛЬНІ ВИМОГИ ДО СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

У статті досліджуються вимоги щодо функціонального призначення систем контролю та управління доступом (СКУД), функціональний склад СКУД і загальні вимоги до неї, інтеграційна та мережева побудова СКУД, системи охоронної сигналізації, системи пожежної сигналізації, системи контролю і управління доступом, можливості СКУД, систем контролю управління доступом, системи відеоспостереження.

Ключові слова: СКУД, інтегрована система безпеки, інформаційна безпека, відеоспостереження, система тривожної сигналізації, об'єкт інформаційної діяльності.

Вступ.

Системи контролю та у управління доступом (СКУД) є необхідним атрибутом будь-якої організації. Існує необхідність обмежити доступ до важливих процесів та захистити ресурси і активи в різних місцях виробництва, включаючи цехи, конвеєри, склади та лабораторії. В сучасному виробництві часто трапляються такі прикрі випадки, як крадіжки, вандалізм власності підприємства, пошкодження майна і навіть напади на співробітників [1]. На теперішній час тенденція розробників зводиться до створення багатофункціональних централізованих систем контролю та управління доступом із використанням радіочастотних технологій (RF) та технологій безконтактних смарт-карт.

Сучасна централізована СКУД може принести користь підприємствам, які не мають контролю доступу або застосовують автономну систему на важливих об'єктах. Автономні системи володіють певними обмеженнями у своїх характеристиках і однією з їх слабких сторін є неефективна здатність відстежувати людей, які отримали доступ до приміщень, що ускладнює розслідування подій. Було проведено попереднє дослідження для вивчення різних технологій, таких як штрих-коди, QR-коди, Bluetooth, біометрія, RFID, безконтактні смарт-карти та NFC, шляхом огляду відповідних академічних журналів, статей та статей про технології в Інтернеті. Дослідження показали, що найкращою технологією для впровадження є безконтактна смарт-карта. Основна увага в цій роботі полягає у висвітленні проектування та розробки системи централізованого контролю доступу для середньостатистичного підприємства, яка також здатна повною мірою використовувати зібрані дані для інших корисних завдань, таких як автоматизація обліку робочого часу, планування роботи та перевірка зайнятості в режимі реального часу.

Основна частина. Ключові технології СКУД.

З тих пір, як вперше з'явилася концепція електронної системи контролю доступу, вона була протестована та впроваджена з використанням різних технологій. Різні підходи мають свої власні переваги та недоліки. Далі розглядаються основні технології, які можуть бути використані при проектуванні СКУД:

Штрих-коди та коди швидкого реагування (QR). Обидві технології вимагають прямої видимості, що може спричинити деякі затримки, особливо коли користувачеві важко розташувати коди належним чином для сканування. Хоча вони є недорогим рішенням контролю доступу, вони є технологіями з низьким рівнем безпеки, оскільки коди можна дублювати дуже легко.

Bluetooth. На ринку вже є декілька комерційних продуктів, зокрема Kevo Smart Lock та EC Key, які перетворюють пристрої з підтримкою Bluetooth на ключ. Головною проблемою цього підходу є споживання батареї пристрою (смартфона) користувача. Для того, щоб користувачі могли швидко та зручно подорожувати через точки входу, їх Bluetooth рекомендується вмикати та постійно залишати у видимому режимі. Це розряджає заряд акумулятора мобільних пристроїв, і в разі несправності мобільних пристроїв або розрядження пристроїв слід розглянути плани резервного копіювання.

Біометрія. Біометрія забезпечує найвищу форму захисту, оскільки усуває певні пристрої облікових даних, забезпечуючи таким чином контроль доступу, який неможливо передавати на відміну від ключів або карток. Однак, завдяки високому рівню безпеки, він також має високі витрати на впровадження. Розгортання біометричних даних для безпеки підприємства на об’єктах з великою кількістю користувачів та великим трафіком може бути нерозумним, оскільки його характер автентифікації може спричинити збої доступу у точках входу.

Радіочастотна ідентифікація (RFID). Все більш поширена технологія з 1970-х років, оскільки ця технологія стає більш доступною. Однією з її головних переваг є той факт, що вона не вимагає прямої видимості і може мати велику дальність читання, що робить її одним з найкращих кандидатів для ідентифікації та відстеження об'єкта. Однак використання пристроїв RFID, які працюють на високій частоті і, отже, мають високий діапазон зчитування, не може обмежувати пропускну здатність системи. Тож в ідеалі пристрої, що працюють на низькій частоті (НЧ), були б кращим вибором для систем контролю доступу.

Безконтактна смарт-карта. Безконтактна смарт-карта використовує радіочастоту між картою та зчитувачем, що не вимагає фізичного вставлення картки, оскільки зчитування здійснюється шляхом її проходження вздовж зовнішньої частини зчитувача. Ці картки відповідають стандарту ISO-14443, із варіаціями типів A, B та C. Оснащені пам'яттю та можливістю шифрування роблять ці карти ідеальним варіантом для програм, які вимагають певного рівня безпеки. Смарт-карта Сантандера є прикладом використання безконтактних смарт-карт для безпечного застосування в навчальних закладах у великих масштабах [2].

Системи ближнього поля (NFC) NFC. Нова технологія, яка дозволила використовувати смартфони як облікові дані користувача. Перевагою такої технології є можливість використання єдиного (комунікаційного) пристрою доступу. Але відсутність стандартизації серед операторів стільникових телефонів, виробників телефонів та виробників безпеки є найбільшою перешкодою на шляху адаптації технології [3].

Перспективна структура централізованої СКУД.

На сьогоднішній день існує дуже багато різновидів СКУД різних виробників, а також її компонентів. Незважаючи на унікальність кожної конкретної системи контролю доступу, вона повинна містити наступні основні елементи (рис. 1):

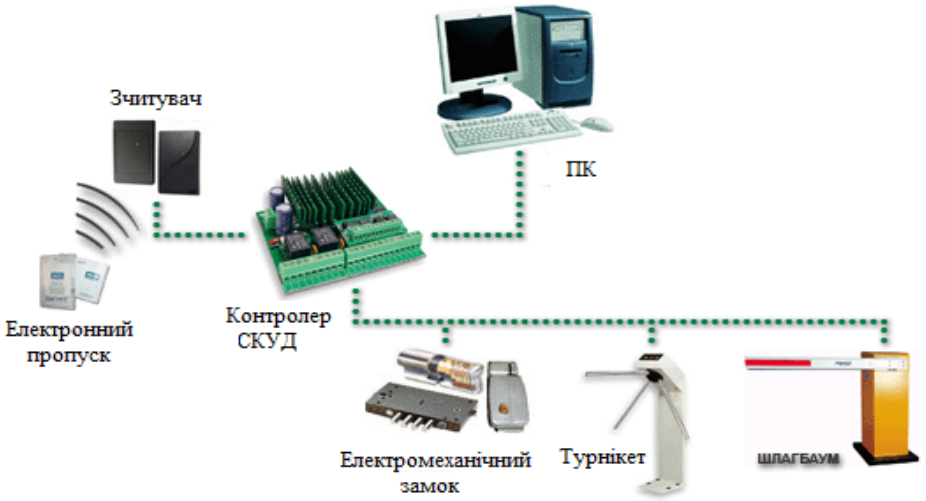

Рис. 1. Схема системи СКУД

Точка контролю. Точка входу, де необхідний бар’єр. Поширені приклади фізичного контролю доступу до точок доступу включають ворота, турнікети та дверні замки. Захищений простір може мати одну точку доступу, наприклад офіс всередині більшого комплексу, або багато точок доступу.

Особисті облікові дані. Більшість СКУД вимагають, щоб користувач мав ідентифікаційні облікові дані, щоб ввести об'єкт або отримати доступ до даних. Прикладами фізичного контролю доступу є облікові дані, зокрема (карти, ключі, токени) та системи введення карток, зашифровані носії, мобільні пристрої, PIN-коди та паролі. Особисті дані відповідають користувачу, який намагається отримати доступ.

Зчитувачі розташовуються у точці доступу і надсилають дані з облікових даних на панель керування для автентифікації облікових даних та запиту на авторизацію доступу. Якщо використовується клавіатура або біометричний термінал (наприклад, сканування відбитків пальців, ідентифікатор обличчя або сканування сітківки ока), користувачі вводять свій PIN-код або виконують сканування для отримання доступу.

Панель керування. Панель керування СКУД отримує облікові дані від пристрою зчитування та перевіряє, чи є такі дані дійсними. Якщо облікові дані підтверджуються, панель управління передає дані авторизації до точки доступу через сервер контролю доступу, і двері відчиняться. Якщо дані не підтверджені, користувач не зможе отримати доступ.

Сервер контролю доступу. Сервер контролю доступу зберігає дані користувача, привілеї доступу та журнали аудиту. Залежно від вашої системи, сервер може бути локальним або керованим у хмарі. Необхідно регулярно проводити технічне обслуговування системи та оновлення програмного забезпечення, щоб захистити систему від злому та можливих порушень безпеки.

Допоміжне обладнання. Це блоки безперебійного живлення, датчики, кнопки, проводка і т.д.

Програмне забезпечення - здійснює настройку і управління обладнанням, моніторинг його параметрів, систематизацію та архівування всієї інформації системи. Воно також здійснює підтримку обміну даними між контролерами і комп'ютером моніторингу, управління доступом і моніторинг пунктів проходу, роботу з базами даних і реєстрацію власників ідентифікаторів, дозволяють здійснювати візуальну ідентифікацію власників "електронних перепусток" на прохідній і для формування різних звітів, а також виконувати додатковий набір функцій.

Вимоги до перспективної системи контролю та управління доступом.

Коли справа доходить до вибору системи контролю доступу, слід враховувати багато факторів. Це може варіюватися від того, як система впроваджена, а також від того, як користувачі виглядають для управління та доступу до своєї системи контролю доступу.

Формати карток користувачів

Окрім технічної оцінки систем контролю доступу, організації також повинні враховувати типи облікових даних та методи побудови доступу, які вони будуть використовувати у своїх фізичних просторах. Починаючи з форматів зчитувачів карток, таких як Wiegand та OSDP, розширюючи широкий спектр форматів карток на вибір, захист вашої організації часто починається з тих самих облікових даних, якими володіють користувачі.

Хмарні сервіси

Впровадження та управління системою доступу до організації починається з вибору між локальною системою контролю доступу та хмарним рішенням. Різниця між двома факторами полягає в тому, як ваша організація буде керувати, масштабувати та керувати своїм повсякденним доступом до будівель.

Інтеграція систем доступу

Хоча побудова систем контролю доступу відіграє ключову роль у забезпеченні фізичних просторів, більшість систем традиційно вирішують лише половину проблем. На додаток до знання ситуації за дверима, система може бути більш корисною в інтеграції з іншими системами фізичного захисту, такими як відеоспостереження. Однак різниця між технічними рішеннями щодо відеоспостереження та контролю доступу може призвести до несумісності різних систем.

Ціна

Є багато факторів, які відіграють значну роль у визначенні ціни на систему контролю доступу до організації. Основні витрати, такі як обладнання та програмне забезпечення контролера, можуть складати більшу частину витрат організації, однак існують різні інші витрати, пов'язані з такими речами, як зчитування карток ключів, обслуговування системи та встановлення системи контролю доступу.

Масштабованість

На початковому етапі досить важко визначити основні параметри системи і тому бажано, щоб система була масштабованою. На додаток до того, як знати, скільки дверей та зареєстрованих користувачів вам знадобиться для побудови доступу, необхідно також врахувати, як системи будуть взаємодіяти між собою під час управління декількома системами контролю доступу або місцями.

Безпека

На додаток до фізичної безпеки, яку забезпечує контроль доступу, важливо також оцінити додаткові міркування щодо безпеки. Це може варіюватися від того, як ваші контролери доступу до дверей підключаються до системи, а також від вибору правильної форми RFID / безконтактних карток, щоб найкраще захистити вашу організацію.

СКУД повинна забезпечувати виконання таких основних функцій [4]**:**

відкривання перерегороджуючих пристроїв контролю (ППК) при зчитуванні ідентифікаційної картки, доступ за яким дозволено в дану зону доступу (приміщення) в заданий часовий інтервал або по команді оператора СКУД;

заборона відкривання ППК при зчитуванні ідентифікаційної картки, доступ за яким не дозволено у дану зону доступу (приміщення) в заданий часовий інтервал;

санкціонована зміна (додавання, видалення) ідентифікаційних карток в пристроях керування (ПК) і зв'язок їх з зонами доступу (приміщеннями) і часовими інтервалами доступу;

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

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

збереження налаштувань і бази даних ідентифікаційних карток при відключенні електроживлення; ручне, напівавтоматичне або автоматичне відкривання ППК для проходу при аварійних ситуаціях, пожежі, технічні несправності відповідно до правил установлених режимом і правилами протипожежної безпеки;

автоматичне закриття ППК за відсутності факту проходу через певний час після зчитування дозволеної ідентифікаційної картки;

видачу сигналу тривоги (або блокування ППК на певний час) при спробах підбору ідентифікаційних карток (коду);

реєстрацію і протоколювання поточних і тривожних подій;

автономну роботу зчитувача з ППК в кожній точці доступу при відмові зв'язку з ПК.

На об'єктах підприємства, де необхідний контроль збереження предметів, слід встановлювати СКУД, контролюючих несанкціонований винос даних предметів з ОІД по спеціальних ідентифікаційних мітках.

Перегороджуючі пристрої контролю з виконавчими пристроями повинні забезпечувати:

часткове або повне перекриття отвору проходу;

автоматичне і ручне (в аварійних ситуаціях) відкривання;

блокування людини всередині ППК (для шлюзів, прохідних кабін);

необхідну пропускну спроможність.

Зчитувачі пристроїв введення ідентифікаційних об'єктів (ПВІО) повинні забезпечувати:

зчитування ідентифікаційної картки;

порівняння введеної ідентифікаційної інформації зі збереженням в пам'яті або базі даних ПК;

формування сигналу на відкривання ППК при ідентифікації користувача;

обмін інформацією з ПК.

ПВІО повинні бути захищені від маніпулювання шляхом перебору або підбору ідентифікаційних даних.

Ідентифікатори ПВІО повинні забезпечити зберігання ідентифікаційних даних протягом усього терміну експлуатації для ідентифікаторів без вбудованих елементів електроживлення та не менше 3 років – для ідентифікаторів з вбудованими елементами електроживлення.

Конструкція, зовнішній вигляд і написи на ідентифікаторі і зчитувачі не повинні призводити до розкриття застосовуваних кодів.

Пристрої керування мають забезпечувати:

прийом інформації від ПВІО, її обробку, відображення в заданому вигляді і вироблення сигналів управління ППК;

ведення баз даних співробітників і відвідувачів ОІД з можливістю завдання характеристик їх доступу (коду, часового інтервалу доступу, рівня доступу та інші);

ведення електронного журналу реєстрації проходів співробітників і відвідувачів через точки доступу;

пріоритетний висновок інформації про тривожних ситуаціях в точках доступу.

Висновок

Таким чином, з проведеного розгляду можна зробити висновок, що системи контролю та управління доступом є невід'ємною частиною інтегрованої системи підприємства та одним з найважливіших компонентів забезпечення інформаційної та фізичної безпеки на об’єктах інформаційної діяльності.

Перелік посилань

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом.- М.: Горячая линия- Телеком, 2010. - 272 е.: ил. – 5с., 16-24с., 27-30

2. [Електронний ресурс]http://studopedia.com.ua/1_30311_sistema-kontrolyu-dostupu.html

3. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / ДержНДІ Спецзв’язку УДК 004.056 /– 2015 –58-60с.

4. Дурденко В.А. Разработка классификация и архитетуры построения интегрированых систем безопасности / Дурденко В.А. Рогожин А.А. – К.: Информационно-вычеслительные управляющие и сетевые системы – 2012/

Надійшла: 10.12.2020 Рецензент: д.т.н., професор Гайдур Г.І.