УДК 004.056.53

АНАЛІЗ СУЧАСНИХ КОМПЛЕКСНИХ СИСТЕМ САНКЦІОНОВАНОГО ДОСТУПУ ДЛЯ ПІДПРИЄМСТВА

Лукіянюк Я.В.
Мандрона М.М. канд. техн. наук
Львівський державний університет безпеки життєдіяльності

На сьогоднішній день актуальним питанням є безпека підприємств, створення їх систем захисту від несанкціонованого доступу та контролю за працівниками. Це зумовлено тим, що сучасні інформаційні та комп'ютерні технології, засоби несанкціонованого доступу до інформації, засоби електронного обміну та засоби захисту інформації – стрімко розвиваються. Внаслідок цього постійно вдосконалюються вже існуючі та з'являються нові організаційні, програмні та технічні способи, які б допомогли побудові комплексних систем санкціонованого доступу та в захисті інформації загалом.

Для розв'язання завдань комплексної безпеки підприємства найефективнішим методом є використання комплексних систем санкціонованого доступу (КССД).

Санкціонований доступ на підприємстві переважно створюється для захисту від антропогенних джерел загроз, якими являються суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини.

Системи санкціонованого доступу використовуються для вирішення таких завдань, як розмежування прав доступу в приміщення, облік робочого часу та моніторинг місцезнаходження працівників [1]. Їх класифікацію наведено на рис. 1.

Сучасна система управління і контролю санкціонованим доступом повинна [2]:

- забезпечувати контроль доступу та управління ним на різних типах контрольно-пропускних пунктів (людських, автомобільних, залізничних);
- унеможливити перевезення заборонених предметів (зброї, вибухових речовин, матеріалів і т. п.);
- перешкодити проникнення потенційних порушників;
- для покращення ефективності систему потрібно оснащувати багаторівневими видами ідентифікації осіб (парольна, біометрична, магнітні картки, кодова;
- володіти високими адаптивними властивостями;
- забезпечувати автоматизацію процесів управління службами безпеки об'єкта та координацію їх діяльності;
- функціонувати в умовах ураження компонентів системи і в інших надзвичайних ситуаціях.

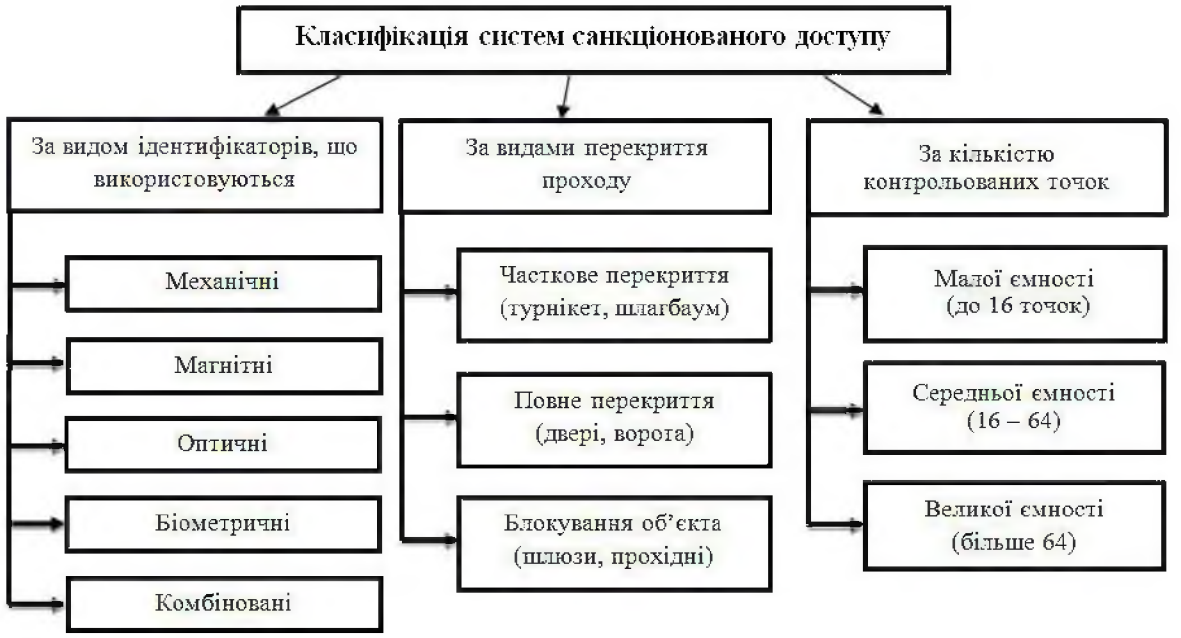

Рис. 1. *Класифікація систем санкціонованого доступу*

Види ідентифікаторів, що використовуються для КССД [1]:

- *механічний* – використання елементів конструкції у приміщенні (елементи механічних ключів, турнікети);
- *магнітний* – використання намагнічених ділянок поверхні (магнітні катки та картки Віганда);
- *оптичний* – використання різноманітного маркування ідентифікатора, які мають різні оптичні характеристики (голографічні мітки чи картки з штрих-кодом);
- *біометричний* – використання фізіологічних характеристик людини (відбитки пальців, колір очей, геометрія руки, сітківка ока, тощо);
- *комбінований* – вид ідентифікації, який побудовано на основі декількох методів ідентифікації одночасно.

Грамотне створення та коректна експлуатація КССД на підприємстві дає змогу вберегти його від несанкціонованого доступу на територію, у будівлю організації та окремі кабінети. В той час експлуатація системи не стає завадою для повноцінної роботи персоналу, не перешкоджаючи їхньому доступу на підприємство.

Література

1. Гарасимчук О.І. Комплексні системи санкціонованого доступу: навч. посібник / Гарасимчук О.І., Дудикевич В.Б., Ромака В.А. – Львів : Вид-во НУ «Львівська політехніка», 2010. – 212 с.

2. Системи контролю та управління доступом. [Електронний ресурс]. – Доступно з: http://sheriff.com.ua/uk/uslugi_ua/sistemi-kontrolia-dostupa-2.