УДК 654.9(075.8)

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ С ПОСТАНОВКОЙ ПОМЕЩЕНИЯ ПОД ОХРАНУ С ПОМОЩЬЮ БИОМЕТРИЧЕСКОГО ИДЕНТИФИКАТОРА

Студент гр. 113017 Раловец А.К.
Ст. преп. Владимирова Т.Л.
Белорусский национальный технический университет

Проблема точной идентификации (определения личности) возникла не сегодня и не вчера. Со временем было придумано много различных способов для того, чтобы человек мог подтвердить, что это именно он, а не кто-то другой. Развитие компьютерных технологий, появление новых материалов и математических алгоритмов обеспечило возможность создания специализированных устройств идентификации – биометрических считывателей. Биометрические системы и считыватели для систем контроля и управления доступом (СКУД) являются одними из наиболее сложных. Назначением биометрической СКУД является не просто идентификация, а аутентификация пользователя. Фактически любая биометрическая СКУД производит сличение заранее занесенного в память системы и вновь вводимого биометрических признаков.

Известно, что совместное применение СКУД и охранной сигнализации повышает уровень безопасности объекта, увеличивает эффективность противодействия преступным посягательствам нарушителя. Однако применение обычных технологий идентификации не позволяет установить, кто именно последним вышел из помещения или кто именно поставил помещение под охрану.

Предлагается СКУД с постановкой помещения под охрану с помощью дактилоскопической системы идентификации по отпечатку пальца. Данная технология является одной из самых распространенных. В основе указанной технологии лежит уникальность рисунка папиллярных линий на пальце. Высокая популярность данного метода обеспечивается, во-первых, сложностью подделки отпечатка, во-вторых, его устойчивостью (неизменность со временем), в-третьих, компактностью самого сканера и малого объема идентификационного кода, что делает возможным быстрый поиск по базе данных, в-четвертых, привычность применения данного идентификатора в криминалистике.

Предлагается использовать специализированный сканер, совмещенный с клавиатурой ввода PIN-кода, что позволит минимизировать время поиска отпечатка пальца по базе данных. В данном случае вероятность ошибки первого рода (вероятность ошибочного содержания «своего» FRR) находится в пределах от 0,01 до 0,0001 %, вероятность ошибки второго рода (вероятность ошибочного пропуска «чужого» FAR) – от 0,002 до 0,0001 %.