

Методы комбинированной идентификации сотрудников

В настоящее время, каждая организация, старается максимальным образом обеспечить защиту предприятия от несанкционированного доступа [1]. Одним из основных методов защиты является идентификация сотрудников [2].

Существует множество методов идентификации, которые предназначены для выполнения функции опознавания человека по определенным признакам. В последнее время, для обеспечения наибольшей безопасности используются комбинированные технологии идентификации, которые позволяют исключить недостатки одной технологии путем использования достоинств другой [3].

Для систем идентификации, в которых важна не только защита от несанкционированного доступа, но и пропускная способность, наибольшее распространение получили методы, основанные на радиочастотной и биометрической технологиях [4].

Достоинством радиочастотной технологии является однозначная идентификация при высокой скорости считывания [5]. Существенным недостатком данной технологии, является возможность подмены RFID-метки [6].

Методы биометрической защиты являются более надежными в плане подмены идентификатора, но обладают высокой сложностью и требуют значительных затрат ресурсов для успешной идентификации.

При комбинировании указанных методов в рамках одной системы удастся устранить недостатки каждого из подходов, сохранив при этом высокий уровень защиты от несанкционированного доступа [7].

При таком подходе требуется несколько усложнить алгоритм работы системы. На первом уровне выполняется радиочастотная идентификация, которая определяет какому объекту принадлежит RFID-метка. Если доступ по данной метке разрешен, система идентификации переходит на второй уровень. На втором уровне считываются биометрические параметры объекта и сравниваются с соответствующими параметрами объекта, идентифицированного на первом этапе. Если данные совпали, то объект считается идентифицированным.

Таким образом, комбинация разных подходов к идентификации сотрудников позволяет повысить защищенность объектов (за счет внедрения более сложных алгоритмов), сохранив при этом скорость работы системы.

Литература

1. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.
2. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие. - СПб.: Изд-во СПбГУЭФ, 2013. - 267 с.
3. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия – Телеком, 2010. – 272 с.
4. Тарасов Ю.А. Контрольно-пропускной режим на предприятии. Защита информации. Конфидент, 2002. – № 1. – С.5-10
5. Радиочастотная идентификация //URL: <http://www.ibs.ua/spravka/181/>. (дата обращения: 28.10.2016)
6. Гудин М., Зайцев В. Технология RFID: реалии и перспективы. Компоненты и технологии, 2003. №4. – С.11-13
7. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия - Телеком, 2000. – 452 с.