Биометрические системы безопасности

Что такое биометрические системы безопасности?

Основная предпосылка биометрической аутентификации (термин происходит от греческого слова "био", что означает жизнь и "метрика", что означает измерение) заключается в том, что каждый человек уникален и может быть идентифицирован по его или ее телесным или поведенческим признакам. Биометрическая технология способна распознавать лица, отпечатки пальцев, подписи, ДНК или радужную оболочку глаз и на этом основании осуществлять проверку подлинности.

Таким образом, биометрические системы производят измерение и статистический анализ физических и поведенческих характеристик человека. Например, системы распознавания речи работают путем определения того, как в процессе речи воздух проходит через легкие, через гортань и выходит наружу через нос и рот человека. Программное обеспечение для идентификации посредством распознавания речи сравнивает эти характеристики с данными, которые хранятся на сервере, и если два голосовых шаблона оказываются идентичными, биометрическая система безопасности объявляет о прохождении верификации.

Сегодня биометрия - это активно развивающаяся сфера отрасли безопасности, но как наука, она не нова. Исследования возможностей использования отпечатков пальцев начались еще в конце 19-го века, а исследования относительно использования в целях идентификации радужной оболочки начались в 1936 году. Однако только во второй половине 1980-х годов разработчики смогли похвастаться крупными достижениями, в частности, возможностью применения биометрических технологий в таких областях как безопасность и видеонаблюдение.

Последние несколько лет происходит бурное развитие биометрических технологий в банковском секторе, в розничной торговле и в технологиях мобильных телефонов.

Биометрия в сравнении с другими технологиями аутентификации доступа

Очевидное преимущество биометрической технологии по сравнению с более традиционными методами аутентификации, такими как персональные идентификационные карты, магнитные карты, ключи или пароли, заключается в том, что биометрические характеристики неразрывно связаны с физическим лицом и не могут стать предметом кражи, мошенничества или утери.

Большинство биометрических систем контроля доступа или идентификации просты в использовании. Пользователям даже не нужно запоминать пароли. Для повышения безопасности можно использовать

комбинацию нескольких биометрических технологий, таких как распознавание лица и распознавание голоса.

Диапазон проблем, решение которых может быть найдено с использованием новых технологий, чрезвычайно широк:

•предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;

•ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность;

•обеспечить допуск к ответственным объектам только сертифицированных специалистов;

•избежать накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);

•исключить неудобства, связанные с утерей, порчей или элементарным забыванием ключей, карт, паролей;

•организовать учет доступа и посещаемости сотрудников.

У всех биометрических технологий существуют общие подходы к решению задачи идентификации, хотя все методы отличаются удобством применения, точностью результатов.

Любая биометрическая технология применяется поэтапно:

•сканирование объекта;

•извлечение индивидуальной информации;

•формирование шаблона;

•сравнение текущего шаблона с базой данных.