(cc) BY

Автор:

Завгородний Станислав Дмитриевич

студент

ФГАОУ ВО «Самарский национальный исследовательский

университет им. академика С.П. Королева»

г. Самара, Самарская область

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ. ВИДЫ ИДЕНТИФИКАЦИИ

Аннотация*: в статье рассматриваются общие принципы идентификации пользователей в системах. В основе работы лежат понятия о PIN-кодах, биометрии и считывателях.*

Ключевые слова*: PIN-код, биометрия, считыватель.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. PIN-код – персональный идентификационный номер, который в ходе процесса авторизации используется как секретный ключ для электронной цифровой подписи запроса и как пароль доступа владельца карты к терминалу.

Определение 2. Биометрия – система распознавания людей по характерным для каждого человека физическим и поведенческим чертам. Биометрические данные в информационной сфере используются в качестве формы управления идентификаторами контроля доступа и самого доступа.

Определение 3. Считыватель – устройство, находящееся обычно в непосредственной близости к двери или другим преграждающим устройствам, предназначенное для чтения идентификационного кода с карт пользователей.

Введение

Идентификация и аутентификация являются основой программно-технических средств безопасности, так как остальные сервисы предназначены на обслуживание именованных субъектов. Именно поэтому зачастую идентификацию

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

вместе с аутентификацией называются «первой линией обороны» информационного пространства организации.

Идентификация пользователя позволяет субъекту обозначить себя в информационной системе. С помощью процесса аутентификации информационная система убеждается, что субъект – это действительно то, за кого он себя пытается выдать. При этом процесс аутентификации бывает односторонним и двусторонним.

Идентификация по PIN-коду

Недорогая система, которая может ограничивать доступ в защищаемое помещение или информационную систему посредством знания определенного персонального идентификационного номера, который может быть общим или индивидуальным. Такой подход имеет существенный недостаток. Злоумышленник может легко узнать код и проникнуть в защищаемое помещение или информационную систему.

Идентификация по биометрическим данным

Все люди на земле имеют уникальный папиллярный узор отпечатков пальцев. Именно благодаря нему возможна идентификация. Чаще всего современны алгоритмы используют характерные точки на самих отпечатках пальцев: начало и окончание линии узора, одиночные точки, разветвление линии. Особенности папиллярного узора превращаются в уникальный код, сохраняющий информацию с отпечатков пальцев. Такой подход обладает высоким быстродействием и достоверностью. Статистические показатели такого метода лучше способов идентификации по голосу, лицу и росписи.

Также очень точным методом распознавания является идентификация личности по радужной оболочке, так как радужная оболочка глаза является уникальной характеристикой человека. С точки зрения логики устройства системы идентификации личности по радужной оболочке делятся на: устройства захвата изображения, с первоначальным преобразованием и передачи вычислителю и вычислитель, осуществляющий сравнение изображения с теми, что находятся в базе

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

данных, передающий сигнал исполнительному устройству о разрешении на право доступа.

Кроме того, существуют другие виды биометрической идентификации, обладающие меньшей точностью: по венам рук, сетчатке, голосу и лицу.

	Устойчивость к подделке	Устойчивость к окружающей среде	Простота использования	Стоимость	Скорость	Стабильность признака во времени
Рад. оболочка	10	9	8	7	10	10
Дактилоскопия	6	10	9	10	10	9
Лицо 2D/3D	4|9	6|8	6|10	10|5	10|7	8|10
Вены руки	10	7	9	7	8	7
Сетчатка	10	10	6	3	6	9

Рис. 1. Сравнение эффективности биометрических способов идентификации

Идентификация с помощью считывателей

При таком способе идентификации используются чаще всего контактные и бесконтактные карты-таблетки. Устройство активизируется в момент контакта со считывателем. Процесс считывания и записи информации осуществляется практически мгновенно во время самого контакта. Наиболее распространяем считывателем типа Touch Memory являются ключи для домофона. Другим распространяем контактным типом считывателя является магнитный карт-ридер, который внешне напоминает прямоугольник с прорезью по середине. С точки зрения функционала он представляет магнитную головку, к которой прижимается магнитная карта посредством специального голика. При бесконтактном способе считывания информации чаще всего применяется технология RFID. Это способ автоматической идентификации объектов, в котором с помощью радио сигналов считываются или записываются данные, хранимые в RFID-метках.

Список литературы

1. Гладких А.А. Базовые принципы информационной безопасности вычислительных сетей / А.А. Гладких, В.Е. Дементьев. – Ульяновск: УлГТУ, 2009. – С. 156.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)