Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ

Аннотация: *в данной работе рассматриваются системы аутентификации, основанные на биометрических параметрах, их преимущества и недостатки.*

Ключевые слова: *базы данных, аутентификация, биометрия, безопасность.*

При построении системы аутентификации основанной на проверке характеристик, часто используют биометрические характеристики человека (отпечатки пальцев, сетчатка глаза, термограмма лица и т. п.). Преимущество данного подхода заключается в том, что аутентифицирующий предмет не может быть потерян и его невозможно передать.

Все методы биометрической аутентификации можно разделить на два класса:

1. Статические методы. В их основе находятся физиологические характеристики человека, присутствующие на протяжении всей жизни.

2. Динамические методы. Основаны на поведенческих характеристиках людей.

Можно выделить несколько критериев, которым должны соответствовать биометрические параметры:

1. Всеобщность: Данным признаком должны обладать все люди без исключения.

2. Уникальность: Отсутствие одинаковых физических и поведенческих параметров у двух разных людей.

3. Постоянство: Для корректной работы системы аутентификации признак не должен изменяться во времени.

4. Измеряемость: Должна быть возможность измерить признак каким-либо устройством для корректного занесения в базу данных.

5. Приемлемость: Обладатели биометрического параметра должны быть не против сбора и измерения.

Для построения эффективной системы аутентификации пользователей информационной системы необходимо учитывать экономическую оправданность применяемых технологий и мер.

Каждый человек обладает уникальным набором биометрических характеристик, которые могут быть использованы для аутентификации пользователя. При использовании такого подхода угрозы кражи и подбора ключевой информации значительно уменьшаются – подделка биометрических характеристик на практике требует больших затрат, которые, как правило, превышают выгоду от такого проникновения. Таким образом, механизм аутентификации пользователя на основе биометрических характеристик создаёт в большинстве случаев непреодолимую защиту на этапе аутентификации.

В то же время стоит учитывать, что большинство технологий основанных на биометрических характеристиках обладают рядом недостатков.

1. Так как псевдопользователи не являются людьми и не обладают биометрическими характеристиками, для их аутентификации должен быть предусмотрен отдельный механизм, который не будет использоваться для аутентификации обычных пользователей.

2. Биометрические характеристики одного и того же человека при двух последовательных входах никогда в точности не совпадают, поэтому в процессе аутентификации используется математический аппарат теории распознавания образов, при этом не исключены ошибки первого (успешный вход от чужого имени) и второго (отказ в доступе легальному пользователю) рода.

3. Большинство биометрических характеристик непостоянны во времени, что требует регулярной корректировки эталонного образа идентифицирующей информации.

4. Биометрические характеристики могут кратковременно изменяться ввиду физических особенностей организма (порез пальца, изменение голоса при болезни).

5. Для построения системы аутентификации на основе биометрических параметров необходимо дорогостоящее оборудования, которое применяется при получении образа используемой характеристики и в вычислительных алгоритмах для сравнения образа с эталонным. Это приводит к большим затратам ресурсов, как финансовых, так и вычислительных.

В заключении следует отметить, что существуют комбинированные биометрические системы аутентификации, которые применяю различные дополнения для использования нескольких типов биометрических характеристик. Такой подход позволяет повысить эффективность системы аутентификации.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.