ИДЕНТИФИКАЦИЯ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Каптурович М.Г., Ковалевич О.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Биометрическая идентификация – это предъявление пользователем своего уникального биометрического параметра и процесс сравнения его со всей базой имеющихся данных. Для извлечения такого рода персональных данных используются биометрические считыватели.

Биометрические системы контроля доступа удобны для пользователей тем, что носители информации находятся всегда при них, не могут быть утеряны либо украдены. Биометрический контроль доступа считается более надёжным, т.к. идентификаторы не могут быть переданы третьим лицам или скопированы.

В основе биометрии лежит совокупность физиологических и поведенческих характеристик человека. В связи с этим методы биометрической идентификации подразделяют на:

– *статические* (основанные на физиологических признаках человека, присутствующих с ним на протяжении всей его жизни);

– *динамические* (берут за основу поведенческие характеристики людей).

К статическим относятидентификацию по отпечатку пальца, идентификацию по лицу, идентификацию по радужной оболочке глаза, идентификацию по геометрии руки, идентификацию по термограмме лица, идентификацию по ДНК, идентификацию на основе акустических характеристик уха, идентификацию по рисунку вен.

К динамическим относят идентификацию по голосу, идентификацию по рукописному почерку, идентификацию по клавиатурному почерку и др.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создаётся и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных. При этом исходные данные, такие как результат сканирования пальца или роговицы глаза, обычно не хранятся.В дальнейшем для идентификации и одновременно аутентификации пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов.В случае успешного поиска личность пользователя и её подлинность считаются установленными. Для аутентификации достаточно

произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введённых данных.

Главными, для оценки любой биометрической системы, являются два параметра:

1) FAR (FalseAcceptanceRate) – коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе.

2) FRR (FalseRejectionRate) – коэффициент ложного отказа, т.е. отказ в доступе настоящему пользователю системы.

Обе характеристики получают расчётным путём на основе методов математической статистики. Чем ниже эти показатели, тем точнее распознавание объекта.

Но для построения эффективной системы контроля доступа необходимо использовать и другие данные. В первую очередь, к ним следует отнести возможность подделки биометрических данных для идентификации в системе и способы повышения уровня безопасности. Во-вторых, стабильность биометрических факторов: их неизменность со временем и независимость от условий окружающей среды. В-третьих, скорость аутентификации, возможность быстрого бесконтактного снятия биометрических данных для идентификации. И, конечно, стоимость реализации биометрической системы контроля и управления доступом (СКУД) на основе рассматриваемого метода аутентификации и доступность составляющих.

Помимо вышеупомянутых методов биометрической идентификации в данной сфере ведутся разработки по применению новых биометрических характеристик, например, таких как пот, запах, микровибрация пальцев и геометрия сердца.

В последнее время спрос на биометрические продукты, в первую очередь в связи с бурным развитием электронной коммерции, постоянно и весьма интенсивно растёт. Биометрическая аутентификация к 2020 г. будет внедрена в 86% компаний в Северной Америке и Европе. Такие данные приводят аналитики ИТ-сети Spiceworks по итогам опроса 500 своих членов в этих регионах. Итоги исследования свидетельствуют о том, что 62% компаний уже внедрили такой способ аутентификации, а еще 24% придут к этому в ближайшие два года. Наиболее популярным среди респондентов способом биометрической аутентификации стало сканирование отпечатков пальцев, его используют 57% компаний. Далее следуют распознавание лица (14%), геометрии руки (5%), сканеры радужной оболочки глаза (3%), распознавание голоса (2%) и сканеры ладоней (2%).