Биометрическая идентификация – панацея против взлома?

Понять, что такое биометрические данные, весьма просто – нестрого говоря, это любые физические (относящиеся к телу человека – например, отпечатки пальцев, сетчатка глаза и т.д.) или поведенческие (относящиеся к поведению человека – например, манера речи, походка и т.д.) данные, позволяющие определить конкретного человека. Соответственно, биометрическая идентификация – процесс определения личности по биометрическим данным. Технически это осуществляется путём сравнения представленного биометрического образца с картотекой имеющихся шаблонов и при совпадении с одним из шаблонов происходит установление соответствующей шаблону личности.

В последние годы технологии биометрической идентификации получили широкое распространение, прежде всего, для защиты информации, контроля доступа и проверки подлинности (иначе называемой аутентификацией). Сканеры отпечатков пальцев в ноутбуках, функция сканирования сетчатки глаза для входа в мобильные устройства, биометрические паспорта и пропуски, в общем-то, стали уже привычными. Означает ли столь широкое применение биометрической идентификации её неоспоримое превосходство над другими методами защиты? Прежде всего, конечно, с точки зрения надёжности защиты и удобства использования устройств с биометрической идентификацией.

Безусловно, в общем случае, биометрическая идентификация обеспечивает более высокий уровень защищённости по сравнению, например, с парольной защитой, поскольку использует «неотъемлемые» идентифицирующие признаки конкретного человека, которые подделать достаточно сложно. Радужную оболочку или сетчатку глаза нельзя «потерять», притом она уникальна, что обеспечивает очень небольшую вероятность ошибочного пропуска злоумышленника. Недостаточно сложный пароль (менее 8 символов, содержащий словарные слова и/или личные данные владельца, не содержащий спецсимволов, заглавных и строчных букв и цифр) можно подобрать, наконец, пароль можно просто украсть. С другой стороны, подделать отпечаток пальца, при наличии образца, можно, например, путём отливки формы силиконом. Кроме того, биометрическая идентификация, как и в случае использования паролей, выполняется с помощью специализированного оборудования и программного обеспечения, которое тоже можно взломать.

Но это – всё же редко встречающиеся и относительно дорогие крайности. В среднем же, повторимся, биометрическая идентификация существенно более надёжный метод защиты.

А вот с удобством использования биометрической идентификации дело обстоит хуже:

- Надёжность срабатывания функции биометрической идентификации зависит от её реализации (программной и аппаратной) производителем – в массовых устройствах вроде мобильных телефонов нередки ситуации, когда устройство выполняет идентификацию владельца неприемлемо долго, либо попросту «не узнаёт» владельца. Это, как минимум, вызывает раздражение пользователей.

  Кроме того, не столь уж редки случаи «порчи» отпечатков пальцев, которые делают идентификацию по ним практически невозможной (например, для людей, имеющих дело с химреактивами, клеями либо иными «забивающими» папиллярный рисунок пальцев веществами).
- Сменить отпечатки пальцев или сетчатку глаза не удастся (в отличие от быстрой смены пароля), поэтому в случае кражи биометрических данных (особенно удручающей будет ситуация, если будет похищена вся база таких данных, например, на стороне сервиса биометрической аутентификации) пользователь оказывается практически безоружен перед злоумышленником.

Резюмируя, приходится констатировать, что биометрическая идентификация не является панацеей от взлома – она хоть и обеспечивает повышенную защиту, но, как и любая технология, имеет ряд недостатков и не избавляет пользователя от необходимости быть внимательным и осторожным.

При пользовании устройствами со сканерами отпечатков пальцев применяйте специальные чехлы и накладки, на которых не остаются отпечатки пальцев. Хорошим вариантом дополнительной защиты является использование вместо отпечатков большого или указательного пальца отпечатка другого пальца, а также функции случайного выбора пальца, отпечаток которого в данный момент является «паролем» на устройстве (разумеется, если устройство поддерживает такую функцию). Наконец, если удобство и скорость пользования устройством не являются для вас краеугольными, используйте биометрическую идентификацию лишь как этап многофакторной аутентификации вместе с паролями и пин-кодами.