Все мы без проблем узнаем друг друга в обычной жизни. Знакомые узнаются в лицо, а незнакомые - по паспорту или же другому документу, где есть фотография, подтверждающая личность. Но как опознать человека, который находится за компьютером по другую сторону Сети? Эта задача намного сложнее, и здесь применяется специфический метод – аутентификация. Это способ подтверждения личности в сети Интернет.

Для аутентификации пользователей обычно используют некий программный модуль, который находится непосредственно на том компьютере, к которому человек хочет получить удаленный или прямой доступ. Условно работа такого модуля делится на два этапа. Давайте их рассмотрим:

– предварительный. Здесь формируется «эталонный образец». К примеру, может запрашиваться пароль. Также проверочный код может назначаться системой;

– завершающий этап. Это прохождение аутентификации. Здесь запрашиваемая идентификационная информация сравнивается с эталоном. По результатам такой проверки пользователь считается опознанным или неопознанным.

Аутентификация - это процедура, которая проводится с использованием информации трех основных видов:

– пользователь демонстрирует компьютеру нечто уникальное, что он знает заранее. Самый распространенный вид – парольная аутентификация. Это простой, но не самый надежный способ;

– у пользователя есть предмет с уникальными характеристиками или содержимым. В качестве такого объекта может выступать сим-карта, карта с магнитной полоской и т.д.. Каждый такой предмет содержит информацию, которая определяет его уникальность.

– в другом случае информация для проверки пользователя – неотъемлемая его часть. По такому принципу построена биометрическая аутентификация. Здесь в качестве информации может применяться, к примеру, отпечаток пальца.

О последней - биометрической - аутентификации стоит поговорить отдельно. Встречавшиеся когда-то лишь в фантастических произведениях, эти технологии в наше время находятся на этапе бурного развития. Здесь как аутентификаторы используются оригинальные характеристики человека, которые присущи только ему. Особенно часто применяются отпечатки пальцев, карта радужной оболочки глаза, черты лица.

Недостатки аутентификации

Самое большое количество недостатков у парольной аутентификации. Секретное слово могут похитить у владельца или взломать его. Часто пользователи выбирают легкоугадываемые простые пароли: производная от идентификатора (часто она является самим идентификатором), слово какого-либо языка и т. п.

Не лишена недостатков и предметная аутентификация. Это похищение или отнятие предмета у владельца.

Я считаю , прежде чем начать внедрение систем аутентификации, необходимо соответствующим образом скорректировать (или же создать) политику информационной безопасности компании. Её основная задача стать рабочим инструментом, повышающим надёжность и эффективность защиты информационных рубежей компании, в связи с чем она должна чётко определять регламенты работы с конфиденциальными данными, а также условия использования персональных идентификаторов при получении доступа из локальной сети или через Интернет.