



Принуждение к безопасности

Николай Федотов,
главный аналитик компании InfoWatch

Среднестатистический человек в состоянии запомнить три нормальных пароля. Но большинство «информ-защитников» с удивительным упрямством требуют придумывать, запоминать и ни в коем случае не записывать длинные стойкие пароли. А ведь под ними может храниться как коммерческая тайна на миллион долларов, так и единственная реплика на веб-форуме. Но каждый ресурс предъявляет к паролю одни и те же требования: длина, отсутствие в словаре, состав символов, хранение в голове. В реальном мире удалось как-то договориться о признании удостоверений личности, выданных другими. Например, авиакомпании массово перешли на электронный билет, который фактически заменяется паспортом. Сфера торговли и обслуживания также тяготеет к коллективным бонусным картам взамен корпоративных — ведь в стандартном бумажнике мест для таких карточек четыре-пять, не больше. В виртуальном мире объединение систем аутентификации пользователей идет с большим скрипом. Без государственного сетевого паспорта единая точка аутентификации рождаться не хочет. Да и проекты упомянутого паспорта пользователя Интернета больше ориентированы на государственный контроль и цензуру, чем на избавление пользователя от регистрации и хранения логинов и паролей для сотен мелких сайтов и крупных систем.

Пока что единственной нормальной реакцией пользователя на столь неадекватные требования к паролям может стать такой подход. Следует запомнить три пароля: один — для важных ресурсов (например, финансовых), другой — для менее значимых и третий — для прочих. А если сам выступаешь в роли администратора, то нельзя забывать, что память человеческая не резиновая. На эксклюзив здесь претендовать нельзя. Самое скверное, что можно сделать для безопасности, — автоматически генерировать стойкий пароль и не позволять пользователю его менять. Примерно так, как это проделывают банки с пин-кодом для банковских карт. Такое принуждение к безопасности ведет к прямо противоположному результату, а именно записыванию пин-кода на карте, бумажнике или в мобильном телефоне. И виноват в подобном нарушении безопасности отнюдь не клиент, а «информ-защитник», игнорирующий реальность.