К ВОПРОСУ БЕЗОПАСНОГО ПРИМЕНЕНИЯ ПАРОЛЕЙ

канд. экон. наук, доц. М.И. Главчев, магистр А.Д. Аннануров,
Национальный технический университет "Харьковский политехнический институт", г. Харьков.

Парольная защита – секретная процедура, предназначенная для подтверждения личности или полномочий. Пароли часто используют для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация "имя пользователя – пароль" используется для подтверждения прав пользователя.

Исследования показывают, что более 40% всех пользователей выбирают пароли, которые легко подбираются. Рекомендуется использовать пароли, генерируемые стойкими хэш-алгоритмами (MD5, SHA-1 и т.п.) от псевдослучайных последовательностей.

Многочисленные виды простых паролей могут быть скомпрометированы и способствовали развитию других альтернативных методов контроля доступа, таких как:

Одноразовые пароли. Это пароли действительны только для одного сеанса аутентификации.

Пароли на основе алгоритма. Знание не набора символов, а алгоритма преобразования выражения.

Биометрия. Предполагает систему распознавания людей по одной или более физических или поведенческих черт.

Технология единого входа – технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации.

OpenID – это открытая децентрализованная система, которая позволяет пользователю использовать единую учётную запись для аутентификации на множестве не связанных друг с другом сайтов, порталов, блогов и форумов.

Применение паролей в настоящий момент все больше не соответствует требованиям безопасности, так как с ростом сложности пароля и количества паролей для запоминания будет усиливаться роль человеческого фактора. Пользователи выбирают наиболее простые с их точки зрения пароли, а при ужесточении политики безопасности пользователи идут на всяческие ухищрения, облегчающие им заботу о паролях, но снижающие их качество.

Обеспечение безопасного хранения паролей, сгенерированных специальными средствами, и является основной задачей проводимого исследования.