

К ВОПРОСУ СОЗДАНИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

Главчев М.И., Аннануров А.Д.

*Национальный технический университет
«Харьковский политехнический институт»,
г. Харьков*

Парольная защита – самая распространенная защита для программного обеспечения. Она характеризуется простотой и дешевизной реализации, малыми затратами машинного времени и не требует больших объемов памяти. Однако она часто не дает достаточного эффекта и основные причины этого таковы:

- Задаются слишком длинные пароли. Будучи не в состоянии запомнить пароль, пользователь записывает его на клочке бумаги, в записной книжке и т. п., что сразу делает пароль уязвимым.
- Пользователи склонны к выбору тривиальных паролей, которые можно подобрать после небольшого числа попыток.
- Процесс ввода пароля в систему поддается наблюдению даже в том случае, когда вводимые символы не отображаются на экране.
- Таблица паролей, которая входит обычно в состав программного обеспечения операционной системы, может быть изменена, что нередко и происходит. Поэтому таблица паролей должна быть закодирована, а ключ алгоритма декодирования должен находиться только у лица, отвечающего за безопасность информации.
- В систему может быть внесен "троянский конь", перехватывающий вводимые пароли и записывающий их в отдельный файл (такие случаи известны). Поэтому при работе с новыми программными продуктами необходима большая осторожность.

Основная задача составителя защитного механизма парольной защиты – скрыть эталонный пароль или спрятать механизм сравнения эталонного пароля с введенным. Эталонный пароль может быть спрятан в разных местах – как в самой программе, так и вне ее. Основными способами усложнения подбора защит являются:

- Использовать различные символы (верхний-нижний регистр, цифры, спецсимволы) и обеспечивать достаточную длину пароля.
- Увеличение времени, за которое может быть произведен подбор пароля (например, сделать задержку между каждым введением пароля и т.д.).
- Использовать защиту, где пароль или хеш-функция пароля является ключом для шифрования некоего кодового блока. В этом случае злоумышленнику придется производить дешифрацию кода.

Выбор способа для обеспечения безопасного хранения паролей и является основной задачей проводимого исследования.