

**А.В.Аграновский, А.А.Коваль, И.В.Мамай** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Анализ методов хранения и степени защищенности парольно-адресной информации в FTP-клиентах.**

Протокол FTP (англ. File Transfer Protocol) — протокол передачи файлов, предназначенный для их передачи в компьютерных сетях [1]. Данный протокол позволяет подключаться к файловым серверам, просматривать содержимое каталогов и загружать файлы с сервера или на сервер. Использование протокола FTP подразумевает передачу при аутентификации сведений об учетной записи (включая и пароль) открытым текстом. Для работы по протоколу FTP используются FTP-клиенты — сервисные программы, с помощью которых можно произвести соединение с FTP-сервером. При использовании FTP-клиентов возможно использование встроенного менеджера сохранения парольно-адресной информации. Одним из факторов отвечающих за качество FTP-клиента является степень защищенности этих данных [2]. Средства и способы сохранения парольной информации различны для каждого клиента.

Нами было произведено сравнение методов безопасного хранения парольно-адресной информации в наиболее популярных FTP клиентах. Данный анализ проводился для программ SmartFTP Client, CuteFTP, WS\_FTP, FileZilla по следующим критериям: метод хранения парольно-адресной информации; метод шифрования сохраненных данных.

В виду того, что протокол FTP обладает требованием передачи в открытом виде парольной информации, ее хранение у клиентов осуществляется обратимым способом [3]. Так, например, клиенты FileZilla, SmartFTP и CuteFTP защищают парольную информацию наложением гаммы и сохраняют их в файле непосредственно вместе с остальными данными. Клиент WS\_FTP сохраняет пароли практически в открытом виде, переводя символы пароля в шестнадцатеричный код.

Таким образом, должный уровень безопасности наиболее распространенные клиенты не предоставляют. Их популярность объясняется бесплатностью распространения (FileZilla) и удобным, интуитивно понятным интерфейсом (WS\_FTP, SmartFTP и CuteFTP).

#### СПИСОК ЛИТЕРАТУРЫ

1. *Найк В.* Стандарты и протоколы Интернета. Русская Редакция, 2000, 356 с.
2. *Аним Б. Ю.* Защита компьютерной информации. БХВ-Петербург, 2000, 384 с.
3. *Шнайер Б.* Прикладная криптография. М.: Триумф, 2002, 816 с.