Д. Е. Лимонтов, В. А. Короткевич
(*УО «ГГУ им. Ф. Скорины», Гомель*)

СРЕДСТВА ОБНАРУЖЕНИЯ ПРОГРАММ-КЕЙЛОГГЕРОВ В СРЕДЕ WINDOWS

В современное время необходимым условием применения и развития информационных технологий является обеспечение кибербезопасности, под которой понимаются меры безопасности, применяемые для защиты вычислительных устройств и компьютерных сетей. Одним из видов программ, относящихся к теме кибербезопасности, являются так называемые клавиатурные шпионы – программы, которые считывают коды нажатых пользователем на клавиатуре клавиш и сохраняют их в лог-файлах. Соответственно, другое название такого рода программ – кейлоггер, от английского "keylogger", что означает дословно "записывающий кнопки". В дальнейшем сохраненную информацию можно использовать как во благо – для информирования работодателей о рабочей деятельности сотрудников, реализации методов родительского контроля, выявления доказательств соучастия в преступлении и др., так и во зло – для перехвата конфиденциальной личной или корпоративной информации, паролей и пр.

Целью данной работы являлась разработка средств защиты от клавиатурных шпионов в среде Windows. С этой целью были изучены разновидности программ кейлоггеров и антикейлоггеров, способы их

взаимодействия со средой Windows. Были реализованы приложения, являющиеся примерами собственных кейлоггеров и антикейлоггера Реализация программ велась на языке C++, в среде C++ Builder в виде консольных приложений. Также были дополнительно написаны и задействованы командные файлы (.bat-файлы) с командами консоли Windows для упрощения управления приложениями.

Подавляющее большинство клавиатурных шпионов использует для мониторинга нажатий клавиш hook-процедуру WH_KEYBOARD. Реализованный антикейлоггер перехватывает вызов этой hook-процедуры и отменяет его, что осуществляется, путем установки своей hook-процедуры – WH_DEBUG, получающей управление при вызове других hook-процедур. Для тестирования антикейлоггера на компьютер был установлен популярный в рунете кейлоггер “Spyrix Free Keylogger”, работа которого была успешно обнаружена и заблокирована.