УДК 004.056.53

# РОЗРОБКА МОДУЛЯ ЗАХИСТУ ПРОГРАМ ВІД КЛАВІАТУРНИХ ШПИГУНІВ

Вітюк В. О.
Науковий керівник – ст. викладач Каплун В. А

Клавіатурний шпигун – це програмний або апаратний засіб для непомітного запису інформації під час натискання клавіш користувачем. А отже, у певних ситуаціях клавіатурні шпигуни можуть вважатися шкідливим програмним забезпечення і служити для зламу захищених програм.

Основними принципами побудови клавіатурних шпигунів є такі: а) стандартна клавіатурна пастка – хук перехоплення повідомлення від клавіатури; б) періодичне опитування стану клавіатури – циклічне опитування стану клавіатури з великою швидкістю; в) установлення драйвера-фільтра – підключення до стеку клавіатури; г) шпигун-руткіт – перехоплення обміну процесу csrss.exe драйвером клавіатури або стеження за викликами API-функцій; д) апаратний «жучок» – пристрій для непомітного запису інформації при натисканні клавіш користувачем.

Сучасні кейлогери в процесі своєї роботи використовують бібліотеки або драйвери, опитують клавіатуру, перехоплюють процеси, мають можливість передавання виявленої інформації по мережі Інтернет та використовують руткіт-метод для забезпечення своєї непомітності в системі.

Основні методи виявлення клавіатурних шпигунів:

- пошук по сигнатурах – перевірка сигнатур файлів;
- евристичні алгоритми – перевірка програми по ознаках, що характерні шпигунам;
- моніторинг API-функцій – перехоплення ряду функцій, що зазвичай використовуються клавіатурними шпигунами;
- відстеження використовуваних системою драйверів, процесів і сервісів.

Найпопулярніші антикейлогери не забезпечують повного захисту від клавіатурних шпигунів. Крім того, вони далеко не ідеальні у тому сенсі, що при їх роботі можливі помилкові спрацювання, оскільки такі самі функції використовуються й у багатьох звичайних програмах.

Для мінімізації помилкових спрацювань розроблено модуль захисту від клавіатурних шпигунів. Захист працює лише при введені важливої інформації, а яка інформація є важливою, визначає розробник програмного продукту та вбудовує у свою програму певний фрагмент коду для впровадження та зняття захисту. Захист реалізовано методом моніторингу API-функцій. Для забезпечення більш надійного захисту можна побудувати систему, в якій будуть поєднанні і деякі інші методи захисту, щоб вони перевіряли і доповнювали один одного.