BC/NW 2012; №1 (20): 9.1

**РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ С ДИСКРЕЦИОННЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА**

А.Е. Киреенко, П.Б. Хорев

РГСУ

Автоматизированные системы обработки информации в настоящее время применяются для решения важных для безопасности государства и общества задач (охрана государственных секретов, управление атомными станциями, электронные банковские расчеты). В связи с этим появляется необходимость решения задач защиты данных систем, в частности решение задачи управления доступом пользователей и активизированных ими процессов к хранящейся в таких системах информации. Традиционно для этого используется дискреционная (избирательная) модель разграничения доступа. Она отличается хорошей изученностью, простотой реализации и низкими требованиями к вычислительным ресурсам, но ее недостатком является отсутствие средств слежения за передачей информации: пользователь может одновременно работать с объектами, имеющими разный уровень конфиденциальности, при этом перенос данных из защищенного объекта, содержащего конфиденциальную информацию, в общедоступный объект не контролируется. Штатные средства контроля доступа операционных систем (защищенные системы семейства Windows) не позволяют отслеживать подобные ситуации.

Предлагается метод, позволяющий контролировать и предотвращать возможность утечки конфиденциальной информации в операционных системах. Метод основан на мандатной модели управления доступом и заключается в присвоении всем субъектам и объектам специальных меток (уровня допуска и грифа секретности соответственно). Монитор безопасности отслеживает все обращения субъектов к объектам и, на основании правил «не читать выше» и «не записывать ниже», применяет необходимые меры по разрешению или блокировке доступа.

В основе реализации предлагается использовать технологию перехвата системных вызовов System Call Hooking. Реализация данного метода позволит существенно повысить защищенность рассматриваемых систем без ущерба для производительности и простоты определения прав доступа.

**Литература**

1. **Гайдамакин Н.А.** Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Издательство Урал. университета, 2003.

3. **Девянин П.Н.** Модели безопасности компьютерных систем. – М.: Издательский центр “Академия”, 2005.

3. **Домарев В.В.** Безопасность информационных технологий. Методология создания систем защиты. – Diasoft, 2001.