СПИСОК ЛИТЕРАТУРЫ:

1. *Фомин Я. А.* Распознавание образов. Теория и применение. М.: ФАЗИС, 2010

Е. В. Елистратова, М. В. Мамаев

МЕТОДИКА ПРОВЕДЕНИЯ ТЕСТА НА ПРОНИКНОВЕНИЕ В ЗАЩИЩЕННЫЕ ХРАНИЛИЩА ОС GOOGLE ANDROID МОБИЛЬНЫХ УСТРОЙСТВ

В настоящее время мобильные устройства под управлением операционной системы (ОС) Google Android в силу своих характеристик и сфер применения являются централизованными хранилищами персональных данных, потенциально представляющих интерес для злоумышленника [1]. В связи с этим важной задачей является оценка защищенности информации в рассматриваемых устройствах.

Выявление угроз защищенности проводится с использованием методов и средств, предназначенных для всестороннего исследования систем с целью обнаружения «слабых мест», которые могут привести к нарушениям безопасности данных. Эффективным способом обнаружения угроз является метод «тестирование на проникновение», основанный на моделировании несанкционированной атаки [2].

В докладе представлена разработанная автором методика проведения теста на проникновение во внутренние хранилища ОС Google Android мобильного устройства для выявления угроз безопасности персональных данных. Тестирование на проникновение основано на моделировании действий злоумышленника, имеющего физический доступ к мобильному устройству, и осуществляется по следующей схеме:

1) анализ общей информации о мобильном устройстве;

2) извлечение и анализ данных о суперпользователе ОС;

3) исследование приложений, функционирующих в ОС, особенностей хранения ими данных;

4) выбор сценария моделирования атаки (получение доступа к внутренним хранилищам ОС):

–расширенные привилегии предоставлены;

–расширенные привилегии не предоставлены.

Практическая апробация разработанной методики и реализующих ее программных средств подтвердила их пригодность для выявления угроз защищенности данных в хранилищах мобильных устройств. Установлено, что большинство приложений ОС Google Android имеют слабый механизм защиты персональных данных, не предусматривающий шифрование. В силу этого следует использовать дополнительные методы и средства для повышения защищенности хранения данных соответствующими приложениями.

СПИСОК ЛИТЕРАТУРЫ:

1. *Михайлов Д. М., Жуков И. Ю.* Защита мобильных телефонов от атак. М.: Фойлис, 2011. С. 8–10.
2. *Wilhelm T.* Professional Penetration Testing // Syngress. 2009. P. 15–18.