«SecureTower» российской компании Falcongaze [1]. В качестве эксперимента 2 тестовых файла (формат: doc, rar; объем: до 50 КБ) с конфиденциальной информацией с использованием стенографического ПО «OpenPuff» (v.4.00 /настройки качества: по умолчанию/, LSB-метод) [2] встраивались в файл-контейнер (формат: png, jpg, pdf). Эффективность перехвата оценивалась в процентах от детекции сформированной тестовой базы из 6 файлов. Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [3]).

На основании проведенного исследования можно сделать вывод, что использование DLP-системы в настоящее время не позволяет детектировать стеганографические технологии модификации файлов. Эффективность перехвата данных DLP-системой по заданному перечню стеганографических модификаций файлов составила 0 % («цифровой отпечаток» (Digital Fingerprints) / контрольная сумма (хэш)).

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. OpenPuff team // download.cnet.com [Электрон. ресурс]. – 2017. – Режим доступа: http://download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html. – Дата доступа: 23.04.2017.

3. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ ПЕРЕХВАТА ДАННЫХ DLP-СИСТЕМЫ

В.В. Маликов, Е.О. Перхальский, И.И. Лившиц

Внедрение и использование DLP-систем позволяет эффективно автоматизировать ряд задач по защите конфиденциальной информации от утечки по технических каналам. Для оценки эффективности была выбрана DLP-система «SecureTower» российской компании Falcongaze [1], которая представляет собой программный продукт, позволяющий решать задачи по защите конфиденциальной информации от утечки по технических каналам.

В рамках исследования эффективности проведено:

Тестирование программной среды функционирования DLP-системы на предмет поддерживаемых операционных систем (ОС). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [2]).

Тестирование эффективности перехвата данных DLP-системой в приложениях, использующих протоколы: POP3, SMTP, HTTP и др.). Назначение портов приложений использовались по умолчанию. Эффективность перехвата оценивалась в процентах от детекции сформированных тестовых баз из 20 файлов / сообщений в 2-х режимах DLP-системы (настройки по умолчанию / специальная настройка параметров). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro»).

На основании проведенного исследования эффективности работы DLP-системы по защите конфиденциальной информации от утечки по технических каналам можно сделать следующие выводы:

1. Программная среда функционирования DLP-системы Falcongaze «SecureTower» в настоящее время поддерживает все основные ОС семейства Microsoft «Windows».

2. Внедрение и использование DLP-системы позволяет эффективно автоматизировать задачи по защите конфиденциальной информации от утечки по технических каналам. Эффективность перехвата данных DLP-системой по заданному перечню протоколов / портов составила от 90 % до 100 %.

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.