Заключение

В данной работе исследованы две стратегии классификации вредоносного ПО по графу потока выполнения. Разработана методика построения графа потока выполнения, с помощью статический и динамический анализа. Рассмотрены два расстояния близости между графами (расстояние редактирования и на основе марковских цепей) и на их основе построены два алгоритма кластеризации: k-means и DBSCAN. Экспериментальные исследования показали, что модель эволюционного развития вредоносного ПО вместе с расстоянием близости графов, построенным на основе расстояния редактирования, является более оптимальной и дает лучшие результаты.

Литература

1. Large-scale malware indexing using function-call graphs / Hu, Xin, Tzicker Chiueh, and Kang G. Shin // In *Proceedings of the 16th ACM conference on Computer and communications security.* – 2009. - P. 611-620.

2. Efficient Virus Detection Using Dynamic Instruction Sequences / Dai, Jianyong, Ratan Guha, and Joohan Lee // *Journal of Computers*. – 2009. - Vol. 4, № 5.

3. Malware classification based on call graph clustering / Kinable, Joris, and Orestis Kostakis // *Journal in computer virology.* – 2011. – Vol. 7, №4. – P. 233-245.

4. Improved call graph comparison using simulated annealing / Kostakis, Orestis, Joris Kinable, Hamed Mahmoudi, and Kimmo Mustonen // In *Proceedings of the 2011 ACM Symposium on Applied Computing.* – 2011. – P. 1516-1523.

И.И. Набиев, И.М. Шаяхметов

ИССЛЕДОВАНИЕ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ОТ ЭЛЕКТРОННЫХ СРЕДСТВ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ)

Образование электромагнитного излучения от электронных средств (ЭС), связано с изменением тока или напряжения в электрических цепях при переключениях элементов [1]. Основной сложностью проведения экспериментальных измерений электромагнитного излучения от ЭС является необходимость в полубезэховой камере. Полубезэховая камера - экранированное помещение, внутренние поверхности которого покрыты поглощающим электромагнитные волны материалом, за исключением пола (пластины заземления), который должен отражать электромагнитные волны [2]. Данное оборудование имеет очень высокую цену и имеется в наличие у ограниченного количества организаций.

Целью данной работы является разработка простой экспериментальной методики и анализ электромагнитного излучения от ЭС на месте его эксплуатации. В качестве примера ЭВС используются персональные компьютеры.

Для экспериментальных исследований применяется оборудование - приемник селективный измерительный РИАП 1.8 [3]. Диапазон рабочих частот данного прибора - 9кГц - 1,8ГГц. Основная погрешность измерения уровня – не более ± 2,5 дБ. Непосредственным приемником электромагнитных полей является антенна пассивная логопериодическая ЛПА-1 [4]. Диапазон рабочих частот – 300МГц - 1,8ГГц.

В рамках данной работы, для анализа электромагнитных излучений от ЭС, предложена следующая простая методика:

1. Выключить все источники электромагнитных излучений в области (комната, несколько комнат, этаж и т.д.), где эксплуатируются ЭС, излучение которых необходимо измерить.

2. Провести экспериментальные исследования электромагнитной обстановки в области эксплуатации ЭВС. При этом точки измерений, ориентация антенны и др. параметры могут варьироваться в соответствии с установленными требованиями к измерениям и не должны изменяться в течение последующих исследований.

3. Включаем одно или несколько ЭС, излучение которых необходимо измерить.

4. Проводим экспериментальные исследования электромагнитной обстановки в области эксплуатации ЭВС.

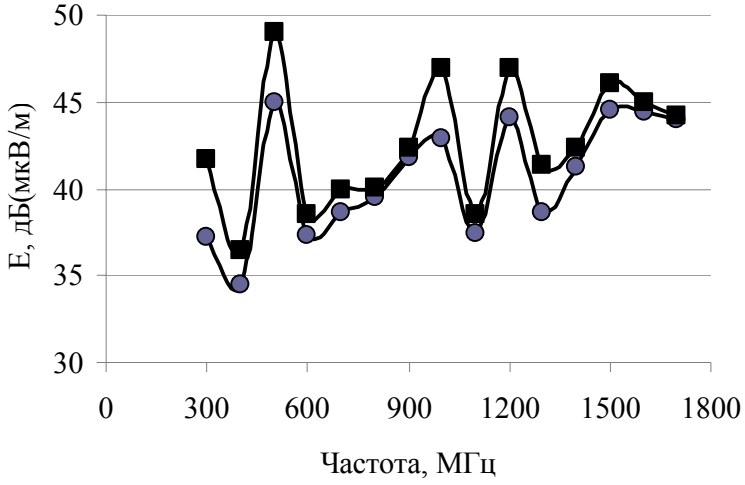
5. Вычитаем полученные результаты измерения электромагнитного излучения без включенных источников из результатов, полученных при включенных (одного или нескольких) ЭС на соответствующих частотах.

6. Повторяем измерения по п. 2 и п .4 до получения воспроизводимых результатов.

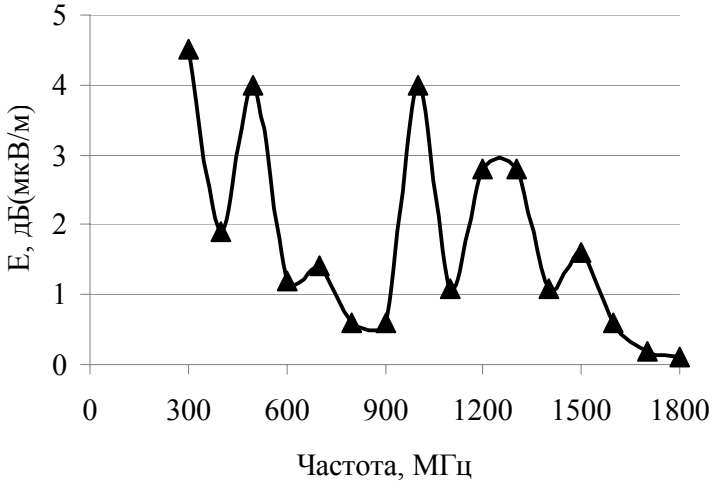
Таким образом, данная методика позволяет в целом оценить уровень электромагнитных излучений от ЭВС в области их эксплуатации. Конечно, необходимым условием для реализации данной методики является предположение о том, что внешняя электромагнитная обстановка (т.е. когда ЭС, электромагнитные излучение которых необходимо измерить) изменяется несущественно в течение выполнения измерений. Для повышения достоверности и воспроизводимости результатов можно рекомендовать повышение количества многократных повторений измерений.

Пример измерения электромагнитных излучений от нескольких ЭС (8 шт. персональных компьютеров) представлен на рис. 1. Измерения проведены в одном из лабораторий КНИТУ-КАИ.

Таким образом, в соответствии с предложенной методикой, можно предположить, что электромагнитное излучение от ЭС, в данном случае, составляет величину, равную разнице между напряженностью электромагнитного поля с выключенными и включенными персональными компьютерами.



а)



б)

Рис. 1. Измерение электромагнитного излучения от ЭС
(а – при всех выключенных и включенных персональных компьютерах;
б – разница между данными двумя случаями)

Литература

1. ГОСТ Р 51318.22-99 Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационных технологий. Нормы и методы испытаний. М.: Изд-во стандартов, 2001. 36 с.

2. ГОСТ Р 51319-99 Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний. М.: Изд-во стандартов, 2001. 57 с.

3. Приемник измерительный РИАН 1.8. Формуляр. Техническое описание**.** Руководство по эксплуатации. Н.Новгород, 2009. 30 с.

4. Антенна пассивная логопериодическая ЛПА-1. Техническое описание. Руководство по эксплуатации. Н.Новгород, 2009. 20 с.