УДК 004.49

Е.А.Гришко, Орлов Ю.К.

Донецкий национальный технический университет, г.Донецк,
кафедра системного анализа и моделирования

СИСТЕМА УПРАВЛЕНИЯ АВТОМАТИЧЕСКИМ РАСПОЗНАВАНИЕМ РЕАЛЬНОГО ПОЛЬЗОВАТЕЛЯ И КОМПЬЮТЕРНОЙ ПРОГРАММЫ

Аннотация

Е.А.Гришко, Орлов Ю.К. Система управления автоматическим распознаванием реального пользователя и компьютерной программы. *Рассмотрена немаловажная проблема, которая возникла около пятнадцати лет назад – бот-сети (ботнеты, зомби-сети) и о возможном способе борьбы с этой проблемой, которую до сих пор очень сильно недооценивают до тех пор, пока не происходит утечка ценной информации с фирмы, не пропадают деньги с банковских карточек и прочие неприятности. Предложен для рассмотрения алгоритм системы управления автоматическим распознаванием реального пользователя и компьютерной программы.*

Ключевые слова: *бот-сеть, бот, зомби-сети, кража информации, кибершантаж, алгоритм.*

Постановка проблемы.Необходимо разработать алгоритм системы управления автоматическим распознаванием реального пользователя и компьютерной программы, который направлен на борьбу с бот-сетями, которые используются для:

- рассылки спама;
- кибершантажа;
- анонимного доступа в Интернет;
- фишинга;
- кражи конфиденциальных данных.

Цель статьи – разработка алгоритма системы управления автоматическим распознаванием реального пользователя и компьютерной программы, направленного на борьбу с бот-сетями.

Решение задачи и результаты исследования.

Система управления автоматическим распознаванием реального пользователя и компьютерной программы предназначена для того, чтобы избежать кражи, потери информации, потери финансов и имиджа фирмы, а также многих других неприятных факторов. Структура данной системы представлена на рисунке 1.

На рисунке 1 рассматривается вариант атаки сети ботнетом. При входе сигнала *x* в систему управления происходит одновременный мониторинг сети Internet и компьютера при помощи программного обеспечения и технических средств контроля, которые анализируют входной сигнал. Обнаружение атаки ботнета этими системами влечет за собой сигнализирование программными и техническими средствами, блокировку ботов, а затем поиск и блокировку центра ботнета.

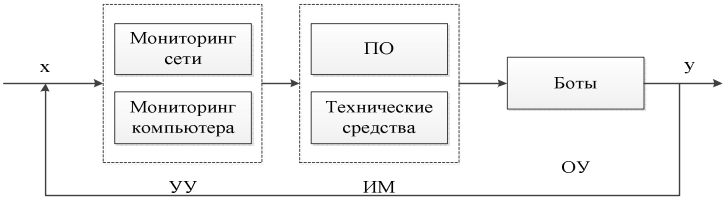

Рисунок 1 – Система управления автоматическим распознаванием реального пользователя и компьютерной программы

Система управления автоматическим распознаванием реального пользователя и компьютерной программы осуществляет двухуровневую защиту: с одной стороны на программном и техническом уровне, а с другой - мониторинг сети Интернет и рабочих машин с целью дальнейшего обнаружения и частичной или полной ликвидации бот-сети.

На рисунке 2 представлен алгоритм работы предложенной системы.

Рассмотрим более подробно данный алгоритм, начиная с алгоритма мониторинга рабочей машины(2) в двух случаях:

1) появление нового или измененного файла (рисунок 3);
2) начало работы нового процесса (и этот процесс не был включен администратором системы в список разрешенных) (рисунок 4).

Кроме существующих составляющих для этой системы предлагаются алгоритмы работы вспомогательных подсистем, которые позволят не только максимально возможно защитить работу организации (сайта), но и обнаружить источник негативного воздействия, а именно:

1) алгоритм для программного обеспечения, которое будет взаимодействовать с аппаратными средствами для сбора и анализа статистики входного трафика;
2) алгоритм для системы обнаружения командного центра бот-сети.

Обнаружение бот-сетей в первую очередь основано на анализе сетевого трафика. Совокупная информация об аномальных изменениях объемов входящего и выходящего трафика дает четкую картину о попытках нарушить

работу, осуществить кражу информации и прочих воздействий на систему. Следовательно, алгоритм для сбора и анализа статистки входного трафика является важной составляющей всей системы.

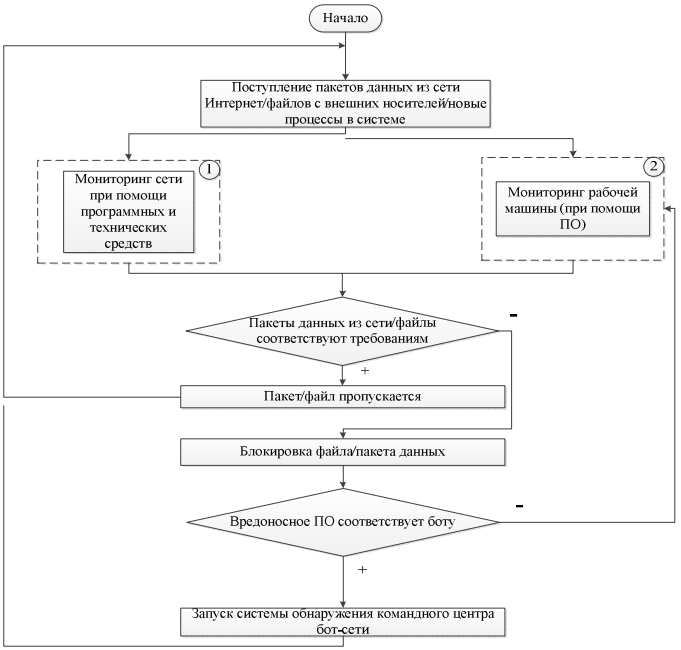

Рисунок 2 – Алгоритм работы системы управления автоматическим распознаванием реального пользователя и компьютерной программы

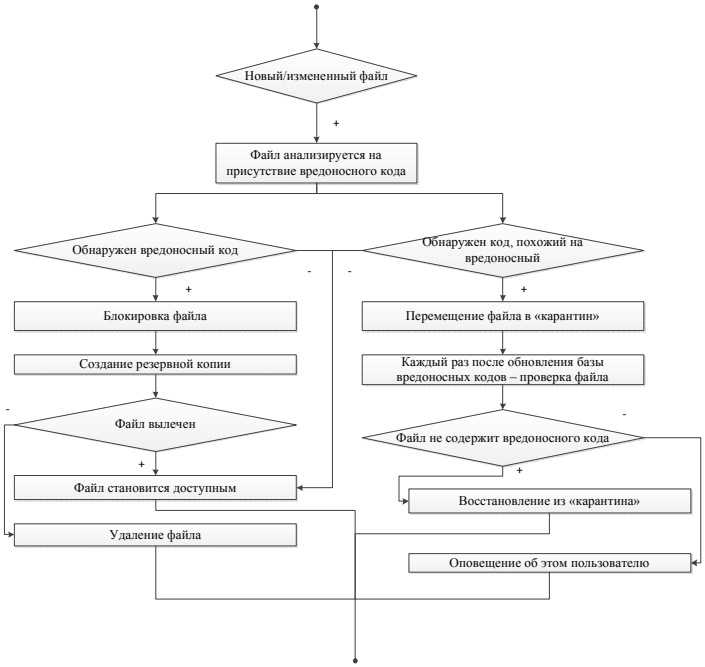

Рисунок 3 – Алгоритм мониторинга рабочей машины (в случае появления нового или измененного файла)

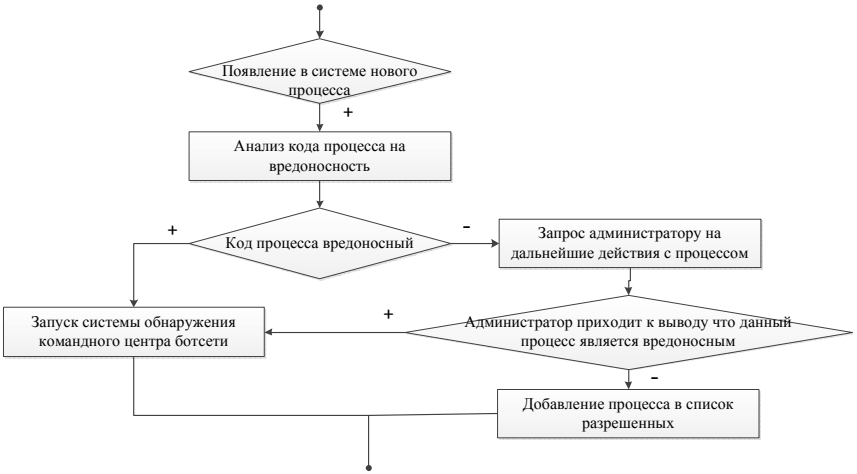

Рисунок 4 – Алгоритм работы мониторинга рабочей машины (в случае появления нового процесса)

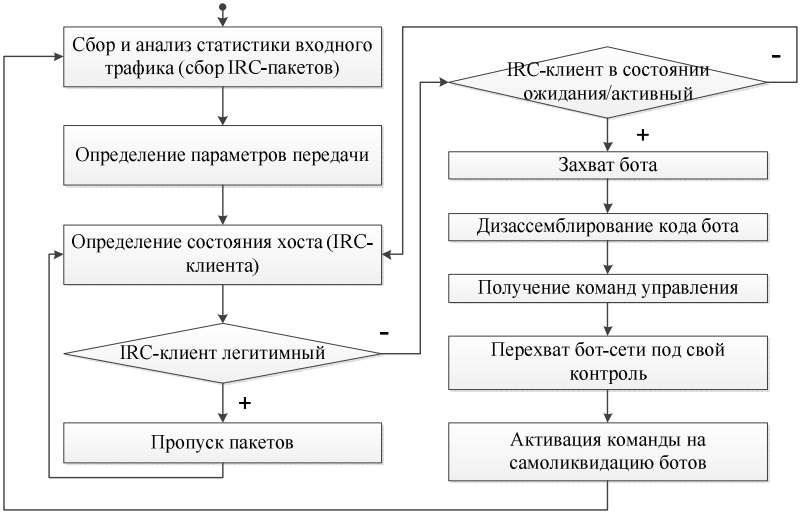

Рисунок 5 – Алгоритм обнаружения командного центра бот-сети

Выводы

В результате проведенной работы был разработан алгоритм системы управления автоматическим распознаванием реального пользователя и компьютерной программы. Дальнейшие исследования будут направлены на моделирование данной системы для изучения эффективности алгоритма.

Список литературы

1. Официальный документ Cisco, Ботнет: новый характер угроз, CiscoSystems, Inc, 2008, 9 с. – URL: http://www.cisco.com/web/RU/downloads/Botnets.pdf.
2. Богданова, И.Ф. Информационная безопасность: классификация компьютерных угроз / И.Ф. Богданова // Интернет и современное общество: Труды XI Всероссийской объединенной конференции(28-30 октября 2008 г., Санкт-Петербург). - СПб.: Факультет филологии и искусств СПбГУ, 2008. - С. 27-29. - URL: http://conf.infosoc.ru/2008/pdf_HI/BogdanovaN.pdf