УДК 004.09

Р.Р. ФАТКИЕВА, Д.К. ЛЕВОНЕВСКИЙ

ДЕТЕКТИРОВАНИЕ КОМПЬЮТЕРНЫХ АТАК МЕТОДОМ СИНГУЛЯРНОГО СПЕКТАЛЬНОГО РАЗЛОЖЕНИЯ

Фаткиева Р.Р., Левоневский Д.К. **Детектирование компьютерных атак методом сингулярного спектрального разложения.**

Аннотация. Рассмотрен метод анализа сингулярного спектра («гусеница») и его применение в области анализа временных рядов сетевого трафика на Web-сервере с целью выявления DDoS-атак на сервер. Выполнено разложение исходных рядов, выявлены особенности собственных функций и главных компонент рядов в разных режимах работы системы.

Ключевые слова: информационная безопасность, Distributed Denial of Service, DDoS, сетевой трафик, временные ряды, сингулярное спектральное разложение, HTTP-flood, главные компоненты.

Fatkieva R.R., Levonevskiy D.K. **Attack detection by means of singular spectrum analysis.**

Abstract. The paper considers the technique of singular spectrum analysis (“the caterpillar”) and its application in the sphere of network traffic time series analysis in order to detect DDoS-attacks against the Web-server. A decomposition of the source time series was carried out. Features of the eigenfunctions and major constituents of the series under different working conditions were revealed.

Keywords: information security, Distributed Denial of Service, DDoS, network traffic, time series, singular spectrum analysis, HTTP-flood, major constituents.

1. Введение. В настоящее время велика популярность компьютерных атак класса отказ в обслуживании (DDoS-атаки, Distributed Denial of Service). Их цель – вывести объект (вычислительную систему) из рабочего состояния, лишить пользователей возможности доступа к серверу или затруднить этот доступ. Грамотно организованная масштабная DDoS-атака в большинстве случаев приводит к значительным финансовым потерям со стороны жертвы. При отсутствии средств обнаружения вторжений ресурс информационной системы тратится на обслуживание DDoS запросов и стоимость использования ресурса многократно возрастает. Такие нападения отличаются простотой организации и высокой эффективностью. Именно эти особенности привлекают к DDoS внимание как специалистов по сетевой безопасности, так и злоумышленников, и обусловливают актуальность исследования DDoS-атак. В частности, представляет интерес статистическое исследование временных рядов сетевого трафика как в штатных ситуациях, так и при наличии атак, что позволяет в дальнейшем выявлять факт вторжения на основе поведенческих сигнатур. Статистические методы исследования предполагают количественный анализ трафика.

Системы защиты, основанные на статистических методах, производят мониторинг поведения системы и контролируют значения характеристических величин. Особенность данных систем в том, что они способны к обнаружению принципиально новых видов атак. Применение анализа сингулярного спектра (SSA – Singular Spectrum Analysis), называемого также «Гусеницей», позволяет преобразовать одномерный временной ряд в многомерный и исследовать полученные составляющие методом главных компонент. При этом не требуется стационарности ряда, знания математической модели тренда и периодических составляющих [1]. Как правило, при этом возможно выделить характерные слагаемые исследуемого ряда – тренд (медленно меняющаяся величина), периодические составляющие разных частот, случайные отклонения. Часто при применении метода можно выявить особенности составляющих ряда, не являющиеся на первый взгляд очевидными [2].

2. Описание метода. Рассмотрим одномерный временной ряд $\{x_i\}$ – последовательность из N значений некоторой величины, снятых с равными промежутками времени Δt:

$$x_i = f((i-1)\Delta t),\ i = 1,...N.$$

Применение метода «Гусеница» выполняется в несколько этапов. На первом этапе производится *формирование матрицы исходных данных из временного ряда*. Для построения матрицы необходимо выбрать число m $(2 \le m \le N/2)$, называемое длиной «Гусеницы». Первая строка матрицы X будет содержать элементы ряда $x_1,...x_m$, вторая – x_2, ... , x_{m+1} и т. д. Последняя строка матрицы под номером $k = N - m + 1$ будет содержать последние m элементов ряда. Построенная матрица будет иметь вид:

$$\begin{vmatrix} x_1 & x_2 & \dots & x_m \\ x_2 & x_3 & \dots & x_{m+1} \\ \dots & \dots & \dots & \dots \\ x_{N-m+1} & x_{N-m+2} & \dots & x_N \end{vmatrix}.$$

Определяющим параметром этого преобразования является длина «Гусеницы», выбор длины которой сильно зависит от решаемой задачи. Так как решается задача анализа исходных временных рядов с целью отыскания их скрытых характеристик, то для повышения точно-

сти следует брать наибольшую возможную длину «Гусеницы» (в идеале равную половине длины ряда). В случае анализа длинных рядов при выборе числа m необходимо достигнуть компромисса между точностью вычислений и ограничениями в вычислительных ресурсах.

Вторым этапом является *анализ главных компонент*. Выполняется центрирование матрицы X. Для этого вычисляются средние арифметические $\overline{x}_j$ и стандартные отклонения s_j для каждого j-го столбца, которые также являются скользящими средними и стандартами временного ряда:

$$\overline{x}_j = \frac{1}{k}\sum_{i=1}^{k} x_{i+j-1},\ j = 1...m,$$

$$s_j = \sqrt{\frac{1}{k}\sum_{i=1}^{k}(x_{i+j-1} - \overline{x}_j)^2},\ j = 1...m.$$

Центрированную и нормированную матрицу обозначим X'. Её элементы вычисляются по формуле:

$$x'_{ij} = (x_{ij} - \overline{x}_j)/s_j,\ i = 1...k,\ j = 1...m.$$

Затем вычисляется выборочная корреляционная матрица V:

$$V = \frac{1}{k}X'X'^T.$$

При выполнении процедуры сингулярного разложения матрица V представляется как:

$$V = PLP^T.$$

где L — диагональная матрица собственных чисел матрицы V $\lambda_1, \lambda_2, ..., \lambda_m$, упорядоченных по убыванию, а P — матрица, столбцы которой представляют собой соответствующие собственные вектора матрицы V $p_1, ...p_m$.

При этом собственные вектора являются ортогональным базисом, набором функций, по которому можно разложить исходный ряд $x_1, ...x_N$:

$$X' = X'PP^T.$$

При этом, в отличие от других методов (например, спектрального анализа), вид базисных функций не задан, а может быть произвольным [2]. При этом погрешность восстановления минимизируется [3].

На третьем этапе производится *восстановление главных компонент*. Матрица, отвечающая любой главной компоненте (или суперпо-

зиции нескольких главных компонент), может быть восстановлена по формуле:

$$X'' = Y^* P^T,$$

где матрица Y^* получена из матрицы главных компонент Y обнулением всех компонент, кроме необходимых для восстановления.

При этом в матрице X'' только первый и последний элементы ряда определены единственным способом — это элементы X_{11}'' и X_{km}''. Все остальные элементы ряда присутствуют в матрице X'', восстановленные как минимум двумя способами. Для однозначного восстановления этих элементов применяют усреднение, например:

$$x_2'' = \frac{x_{12}'' + x_{21}''}{2},$$

$$x_3'' = \frac{x_{13}'' + x_{22}'' + x_{31}''}{3}.$$

Отметим, что при применении метода значительное количество информации можно извлечь из следующих данных:

-собственные числа корреляционной матрицы V, отражающие степень влияния компонент на временной ряд;

-собственные векторы корреляционной матрицы V, которые можно интерпретировать как функции времени;

-главные компоненты m-мерного представления временного ряда;

-временные ряды, полученные восстановлением различных комбинаций главных компонент.

3. Детектирование компьютерных атак на примере Web-серевера. В качестве исходных данных для проведения исследования взят сетевой трафик Web-сервера, содержащий сайт, построенный с помощью PHP/MySQL. Трафик снят в двух режимах: в режиме регулярного взаимодействия с клиентами по сети и в режиме DDoS-атаки класса HTTP-flood. Для каждого случая сняты характеристики интенсивности отдельно для входящего и исходящего трафиков (рис.1, 2).

Для определения длины гусеницы m воспользуемся информационной интерпретацией собственных чисел корреляционной матрицы V, представляющей выборочные дисперсии соответствующих главных компонент [1]. Учитывая, что в сумме они дают m, можно заключить, что величины вида $c_i = \frac{\lambda_i}{m} \cdot 100\%$ представляют собой процент-

ные доли дисперсии главных компонент и могут интерпретироваться как доли общей информации, вносимые i -й компонентой.

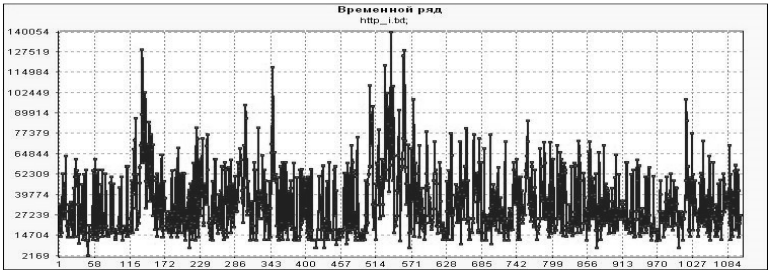

Рис.1. Входящий трафик 1.

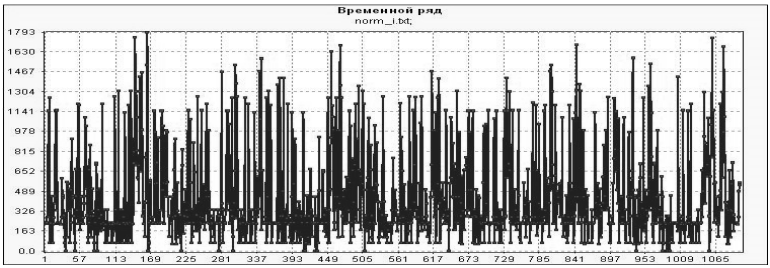

Рис.1 Входящий трафик при атаке HTTP-flood.

Величины $c_i = \sum_{k=1}^{i} c_k$ являются накопленными процентами и отражают долю информации, вносимую первыми i главными компонентами. Для определения m предлагается установить пороговое значение c^* накопленного процента, провести пробное разложение ряда при некотором достаточно большом m_0 [2] и принять за m такое количество главных компонент, что $c_m \geq c^*$.

При $c^* = 99\%$, $m_0 = 100$ для четырёх рассматриваемых рядов получаем следующие значения длины гусеницы (табл.1).

Таблица 1. **Значение длины гусеницы**

Длина гусеницы	Входящий трафик в «штатном режиме»	Входящий трафик в режиме HTTP-flood	Исходящий трафик в «штатном режиме»	Исходящий трафик в режиме HTTP-flood
m	93	91	92	91

В этом случае за длину гусеницы m можно принять максимальное значение из таблицы 1, равное 93.

Применение разложения даёт ряд собственных векторов и соответствующих главных компонент. Приведём диаграммы собственных векторов корреляционной матрицы входящего трафика (рис. 3, 4) и его главные компоненты (рис. 5, 6).

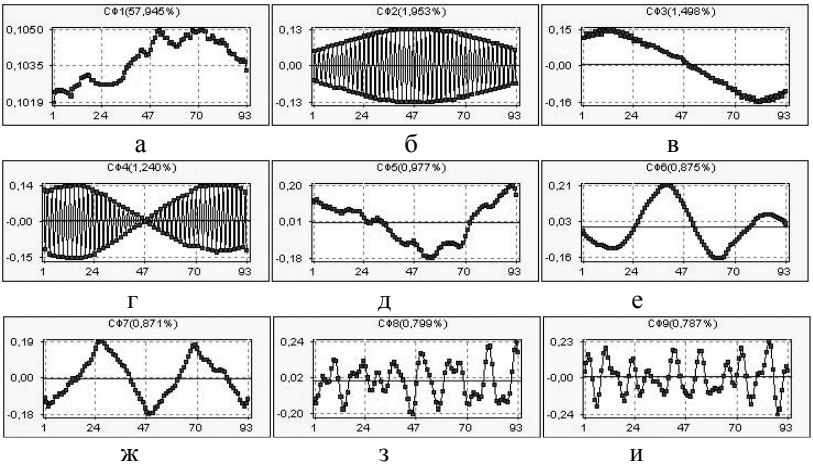

Рис. 3. Собственные функции (СФ) для входящего трафика в нормальном режиме (а – собственная функция, отвечающая за тренд; б, г – высокочастотные функции; в – периодическая функция с малым периодом; д, з, и – хаотические функции; е, ж – периодические функции).

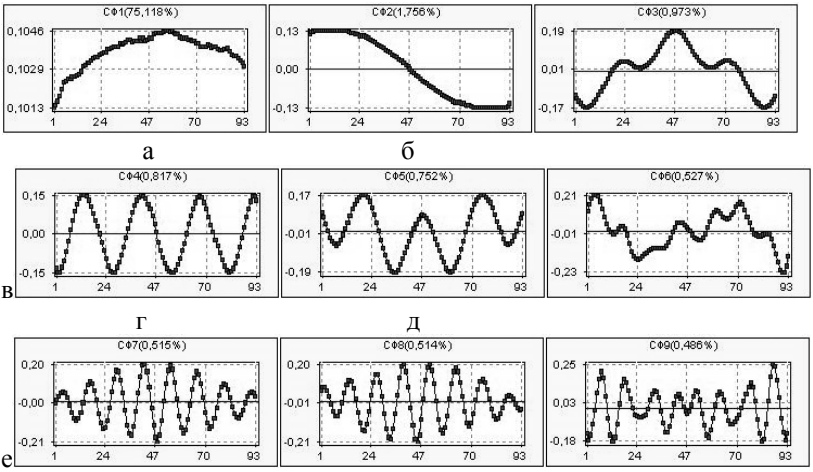

Рис. 4. Собственные функции для входящего трафика в режиме HTTP-flood (а – собственная функция, отвечающая за тренд; б – периодическая функция с малым периодом; в-и – гармонические функции разного спектра и частоты).

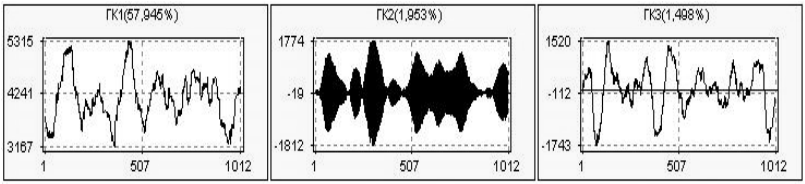

Рис. 5. Главные компоненты входящего трафика в нормальном режиме (а – тренд; б – высокочастотные вариации; в – низкочастотные вариации)

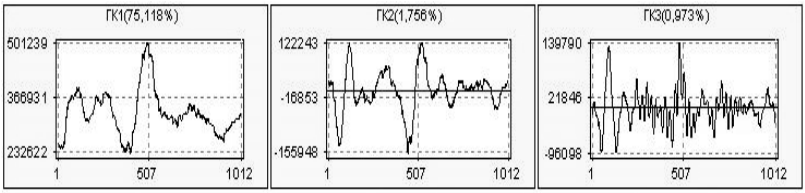

Рис. 6. Главные компоненты входящего трафика в режиме HTTP-flood (а – тренд; б, в – вариации различных частот).

Из визуального анализа графиков на рис. 3, 4 очевидны качественные различия в базисе разложения исходного ряда. Собственные функции в режиме HTTP-flood являются более регулярными и имеют ярко выраженный синусоидальный характер, тогда как в нормальном режиме функции, как правило, либо выглядят хаотично, либо имеют составляющие очень высокой частоты. Тот же эффект можно видеть на двумерных графиках собственных функций (рис. 7, 8). Это может объясняться тем, что в режиме HTTP-flood система приближается к одному из предельных состояний и продолжает находиться в этом состоянии, тогда как в нормальном режиме запросы легитимных пользователей к серверу носят случайный характер, и хаотическое изменение состояния системы соответствующим образом сказывается на параметрах потоков данных.

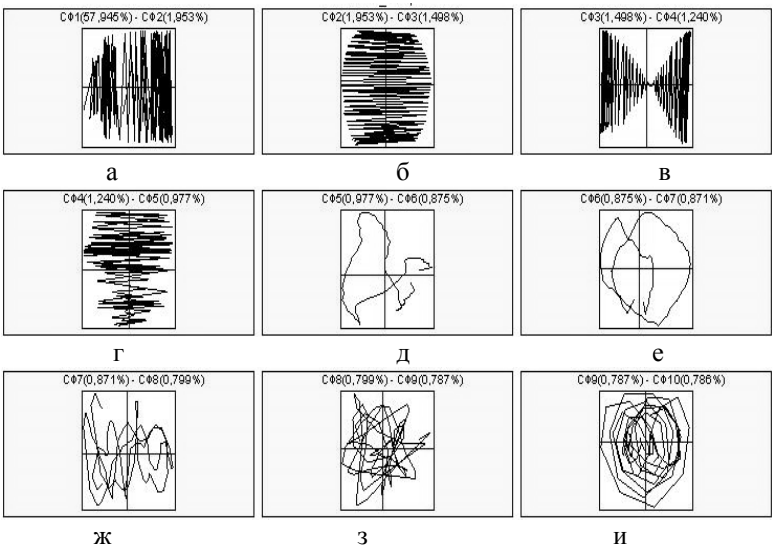

Рис. 7. Диаграммы собственных функций (СФ) в нормальном режиме (а – СФ1-СФ2, б – СФ2-СФ3, в – СФ3-СФ4, г – СФ4-СФ5, д – СФ5-СФ6, е – СФ6-СФ7, ж – СФ7-СФ8, з – СФ8-СФ9, и – СФ9-СФ10).

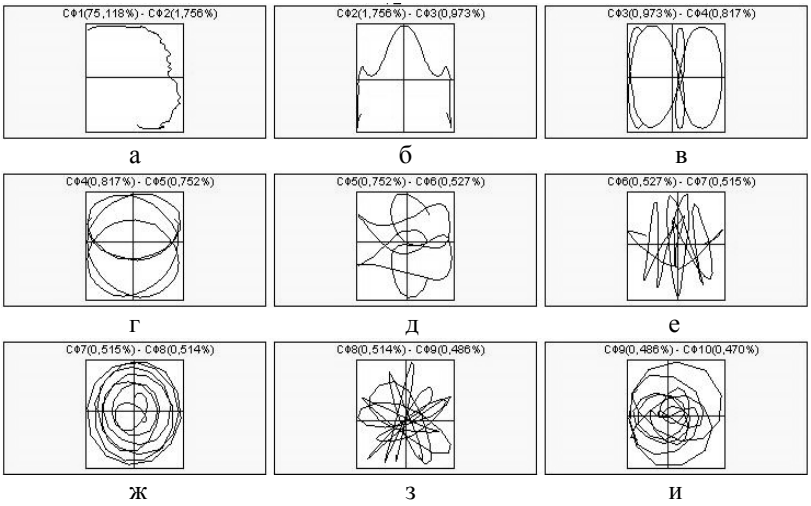

Рис. 8. Диаграммы собственных функций (СФ) в режиме HTTP-flood (а – СФ1-СФ2, б – СФ2-СФ3, в – СФ3-СФ4, г – СФ4-СФ5, д – СФ5-СФ6, е – СФ6-СФ7, ж – СФ7-СФ8, з – СФ8-СФ9, и – СФ9-СФ10).

Интерес представляют также значения процентного вклада компонент в исходные ряды – приведённые собственные числа (табл. 2).

Таблица 2. **Вклад главных компонент в исходные ряды**

Главная компонента	Входящий трафик в «штатном режиме»	Входящий трафик в режиме HTTP-flood	Исходящий трафик в «штатном режиме»	Исходящий трафик в режиме HTTP-flood
1	57,94	75,12	40,10	55,97
2	1,95	1,76	3,66	4,02
3	1,50	0,97	2,27	2,21
4	1,24	0,82	1,92	1,64
5	0,98	0,75	1,90	1,57
6	0,88	0,53	1,67	1,20
…	…	…	…	…
93	0,14	0,10	0,12	0,11

Можно обратить внимание на то, что первая главная компонента (тренд) при HTTP-flood вносит больший вклад по сравнению с остальными компонентами.

4. Заключение. В статье рассмотрен метод сингулярного спектрального анализа («Гусеница») и его применение для детектирования DDoS-атак на сервер. Выполнено разложение исходных временных рядов входящего и исходящего трафика, в результате чего выявлены особенности собственных функций и главных компонент рядов в разных режимах работы системы. Показано, что степень влияния трендовой компоненты на временной ряд значительно различается в случаях, когда сервер работает в штатном режиме, и когда он подвержен атаке: в режиме атаки влияние трендовой компоненты увеличивается в среднем на 35%. Также отмечены качественные различия в характере собственных функций: в режиме атаки они имеют гармонический характер и компактный спектр, тогда как собственные функции штатного режима характеризуются наличием высокочастотных составляющих и большим влиянием случайных вариаций.

Литература

1. Главные компоненты временных рядов: метод "Гусеница" /под ред. Д.Л.Данилова, А.А.Жиглявского. СПб: Пресском, 1997. 308 с.
2. *Голяндина Н.Э.* Метод «Гусеница»-SSA: анализ временных рядов. СПб.:2004. 76 с.
3. *Пичугин Ю.А.* Итерационный анализ сингулярного спектра в оценке естественных цикличностей данных метеорологических наблюдений // Метеорология и гидрология, № 10, 2001 г.С 34–39.
4. *Пичугин Ю.А.* Выборочные главные компоненты скользящего отрезка в анализе временных рядов метеорологических данных // Метеорология и гидрология, №8, 1999 г.С31–36.

Фаткиева Роза Равильевна — канд. техн. наук; старший научный сотрудник лаборатории информационно-вычислительных систем СПИИРАН. Область научных интересов: моделирование информационных систем. Число научных публикаций — 26. rikki2@yandex.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-4369, факс +7(812)328-4450.

Fatkieva Rosa Ravilievna— senior researcher, Laboratory of Computer and Information Systems, SPIIRAS. Research interests: modeling of information systems. Number of publications — 26. rikki2@yandex.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-4369, fax +7(812)328-4450.

Левоневский Дмитрий Константинович — бакалавр информационных систем, младший научный сотрудник лаборатории информационно-вычислительных систем СПИИРАН. Область научных интересов: исследование DDoS-атак, статистический анализ и моделирование трафика локальных сетей. DLewonewski.8781@gmail.com; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-4369, факс +7(812)328-4450.

Levonevskiy Dmitriy Konstantinovich — bachelor on information systems, researcher, Laboratory of Computer and Information Systems, SPIIRAS. Scientific interests: research of

DDoS attacks, statistical analysis and modeling of the network traffic. DLewonewski.8781@gmail.com; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-4369, fax +7(812)328-4450.

Рекомендовано лабораторией информационно-вычислительных систем СПИИРАН, заведующий лабораторией Воробьев В.И, д-р техн. наук, проф.
Статья поступила в редакцию 01.02.2013.

РЕФЕРАТ

Фаткиева Р.Р., Левоневский Д.К. **Детектирование компьютерных атак методом сингулярного спектрального разложения.**

В настоящее время многие организации, использующие интернет-технологии, сталкиваются с проблемой DDoS-атак. Грамотно спланированная масштабная DDoS-атака в большинстве случаев приводит к значительным финансовым потерям со стороны жертвы, при этом оставаясь несложной в организации. По этой причине представляет интерес статистическое исследование временных рядов сетевого трафика как в штатных режимах, так и при наличии атак, что позволяет в дальнейшем программными средствами выявлять факт вторжения на основе поведенческих сигнатур.

В статье рассмотрено применение анализа сингулярного спектра (SSA – Singular Spectrum Analysis), позволяющего преобразовать одномерный временной ряд в многомерный и исследовать полученные составляющие методом главных компонент. Метод не требует стационарности ряда, знания математической модели тренда и периодических составляющих.

В качестве исходных данных для проведения исследования взят запротоколированный сетевой трафик Web-сервера в двух режимах: регулярной работы и наличия атаки HTTP-flood. Применение разложения позволяет выявить качественные различия в наборе собственных функций корелляционной матрицы исходных рядов. Собственные функции в режиме HTTP-flood являются более регулярными и имеют ярко выраженный синусоидальный характер, тогда как в нормальном режиме функции, как правило, либо выглядят хаотично, либо имеют составляющие очень высокой частоты. Интерес представляют также значения процентного вклада компонент в исходные ряды (т. е. приведённые собственные числа корреляционной матрицы). Первая главная компонента (тренд) при наличии HTTP-flood вносит в среднем на 35% больший вклад по сравнению с остальными компонентами. В режиме HTTP-flood система приближается к некоторому предельному состоянию и продолжает находиться в этом состоянии, тогда как в нормальном режиме запросы легитимных пользователей к серверу носят случайный характер, и хаотическое изменение состояния системы соответствующим образом сказывается на параметрах потоков данных.

Таким образом, приведённые выше отличия могут служить математической базой для построения программного средства обнаружения вторжений, ориентированного на DDoS-атаки.

SUMMARY

Fatkieva R.R, Levonevskiy D.K. **Attack detection by means of singular spectrum analysis**

Nowadays a lot of organizations that use Internet technologies face the problem of DDoS-attacks. A competently designed, large-scale DDoS-attack leads in most cases to a considerable financial loss on the victim's side being not difficult in implementation. Therefore statistical research of time series of the network traffic both in standard modes and under attack is of considerable interest. So it will be possible to detect an intrusion by means of software based on behavioral signatures.

The paper considers the implementation of the singular spectrum analysis (SSA), that enables transformation of one-dimensional time series into multidimensional ones and analysis of the derived constituents by the method of major components. This technique requires neither time invariance of the series nor knowledge of the mathematical model of the trend as well as its periodical constituents.

As a source data for the research we take the recorded network traffic from a Web-server working in two modes: regular mode and HTTP-flood mode. The decomposition makes it possible to find out the qualitative difference in the sets of eigenfunctions of the source series' correlation matrix. The eigenfunctions in the HTTP-flood mode are more regular and possess a strongly pronounced sinusoidal nature, while in the regular mode the functions, as a rule, look either chaotically, or contain constituents of a very high frequency. It is also interesting to examine the values of the constituents' contribution to the source series (that are the reduced eigenvalues of the correlation matrix). The contribution of the first major constituent (the trend) during the HTTP-flood is at the average 35% greater as compared with the regular mode. During the attack the system comes nearer to some extreme state and remains in this state while the requests of legitimate users to the server in the regular mode have a random nature, and the chaotic changes of the system conditions affect accordingly the features of data flows.

Thereby the behavioral differences described above can serve as a mathematical basis for development of an intrusion detection system specialized in DDoS-attacks.