УДК 004.09

Д.К. Левоневский, Ю.А. Пичугин, Р.Р. Фаткиева

ИССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ АТАК МЕТОДОМ СИНГУЛЯРНОГО СПЕКТАЛЬНОГО РАЗЛОЖЕНИЯ СЕТЕВОГО ТРАФИКА

Левоневский Д.К., Пичугин Ю.А., Фаткиева Р.Р. **Исследование компьютерных атак методом сингулярного спектрального разложения сетевого трафика.**
Аннотация. Рассматривается метод анализа сингулярного спектра («гусеница») применительно к метрикам, базирующимся на значениях сетевого трафика и загрузки системы, с целью определения влияния DDoS-атак на главные компоненты временных рядов этих метрик. Выявленное поведение главных компонент в момент начала атаки и при её продолжении может использоваться при разработке средств обнаружения вторжений.
Ключевые слова: информационная безопасность, Distributed Denial of Service (DDoS), сетевой трафик, временные ряды, сингулярное спектральное разложение, HTTP-flood, главные компоненты.

Levonevskiy D.K., Pichugin Y.A., Fatkieva R.R. **Investigation of computer attacks by analysis of observed traffic singular spectrum.**
Abstract. The paper considers the technique of singular spectrum analysis (“the caterpillar”) and its application to 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. Characteristics of the eigenfunctions and principal components 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, principal component.

1. Введение. Сетевые атаки вида Distributed Denial of Service (DDoS) благодаря простоте и эффективности представляют собой одну из самых значительных угроз для сервисов, размещённых в сети Internet. Существующие на данный момент средства защиты далеко не всегда справляются с всё более профессионально организованными атаками, что объясняет необходимость исследований в области защиты от атак такого типа. В данной статье речь идёт об использовании статистического метода «гусеница» анализа временных рядов для исследования сетевого трафика. Этот метод нашёл применение во многих прикладных задачах [1] и даёт возможность углубиться в структуру исходных данных и выявить скрытые поведенческие характеристики системы [2, 3], что может быть полезно для построения систем проактивной защиты от атак.

2. Организация измерений. Исследования проводились с использованием специализированной системы сбора и управления трафиком, позволяющей контролировать его характеристики в реальном времени. В качестве исходных данных для проведения исследования

выбран сетевой трафик Web-сервера, содержащий сайт, построенный с использованием скриптового языка программирования PHP. Трафик снят в двух режимах: в режиме регулярного взаимодействия с клиентами по сети и в режиме DDoS-атаки классов SYN-flood, UDP-flood, HTTP-flood. Сервер выполняет хостинг сайта, реализующего Web-интерфейс для системы инженерных вычислений Octave. Для оценки возможностей обнаружения атаки на сетевой трафик, измерения проводились в двух режимах: в штатном режиме работы сервера с обменом HTTP-трафика с условно легитимными клиентами и в режиме реализации атаки. При этом фиксировались значения сетевого трафика и системных характеристик (объем оперативной памяти, время загрузки процессора и т.п.). Наблюдаемые изменения значений указанных характеристик может не свидетельствовать об атаке. Для более адекватной оценки состояния системы необходимо проанализировать структуру трафика детально и определить наиболее информативные метрики, позволяющие идентифицировать атаку. Примеры таких метрик приведены в таблице 1.

Таблица 1. **Метрики, идентифицирующие атаку**

Метрика	Типы атак	Комментарии
Отношение числа входящих и исходящих пакетов	Все	Характеризует способность сервера отвечать на запросы
Число потоков Web-сервера	HTTP-flood (возрастает)	Характеризует загрузку Web-сервера
Число исходящих флагов ACK минус число входящих флагов ACK	HTTP-flood, SYN-flood (снижается до отрицательного значения)	Характеризует способность сервера отвечать на запросы
Доля UDP в IP-трафике	SYN-flood (снижается), UDP-flood, HTTP-flood (возрастает)	Характеризует степень загрузки сети однонаправленным UDP-трафиком
Отношение числа SYN-флагов к объёму входящего трафика	SYN-flood (возрастает)	Характеризует неэффективность передачи данных (доля накладных расходов)
Отношение числа PSH-флагов к объёму входящего трафика	SYN-flood (снижается)	Характеризует эффективность передачи данных

Рассмотрим более подробно метрики, представленные в таблице.

1. Отношение числа входящих и исходящих пакетов в единицу времени:

$$R_{ip} = \frac{T_i}{T_o},$$

где T_i и T_o — объёмы, соответственно, входящего и исходящего IP-трафика в единицу времени. Целесообразность выбора данной величины в качестве метрики объясняется тем, что при наличии DDoS-атаки сервер теряет способность отвечать на запросы. Повышение скорости входящего трафика без соразмерного повышения скорости исходящего трафика ведёт к росту величины R_{ip}, что означает более высокую вероятность наличия атаки.

2. Число потоков, критических для атаки приложений, можно использовать для определения (обнаружения) атак прикладного уровня. Так как в качестве прикладной атаки на Web-сервер выступает HTTP-flood, необходимо измерять число потоков приложения Apache N_{web}. Если Web-сервер обращается к другим приложениям (например, к базе данных, системе инженерных вычислений), целесообразно измерить количество потоков и этих приложений.

3. Разница между количеством входящих и исходящих TCP-пакетов с установленным флагом ACK, прошедших через сетевой интерфейс сервера, характеризует способность сервера отвечать на запросы:

$$R_{ack} = N_{acko} - N_{acki},$$

где N_{acko} — количество исходящих ACK-пакетов, N_{acki} — количество входящих. При наличии атаки число исходящих ACK-пакетов снижается, и значение характеристики R_{ack} уходит в отрицательную область.

4. Частоты флагов SYN и PSH во входящих пакетах позволяют определить эффективность передачи данных. Пакеты с флагом SYN пересылаются между клиентом и сервером в ходе установления TCP-соединения, после чего начинается обмен данными с помощью пакетов без SYN-флага. Таким образом, число SYN-флагов, пришедших на сервер, равно числу запросов на соединение, а частота SYN-флагов определяет долю служебных пакетов этого типа в TCP-трафике. При атаке класса SYN-flood субъект атаки не намерен передавать какие-либо данные серверу и пытается перегрузить его очередь соединений с

помощью служебных пакетов. Частота флагов SYN измеряется соотношением:

$$R_{syn} = \frac{N_{syn}}{N},$$

где R_{syn} — частота флагов SYN, N_{syn} — количество SYN-флагов во входящих пакетах, N — общее количество входящих пакетов.

Установленный флаг PSH означает, что данные, содержащиеся в пакете, должны быть переданы программе прикладного уровня. В случае Web-сервера, эти данные представляют собой HTTP-запросы и HTTP-ответы, содержащие Web-страницы. Частота PSH-флагов, напротив, характеризует полезную загрузку канала:

$$R_{psh} = \frac{N_{psh}}{N},$$

где R_{psh} — частота флагов PSH, N_{psh} — количество PSH-флагов во входящих пакетах, N — общее количество входящих пакетов.

5. Коэффициент влияния UDP-трафика определяется соотношением:

$$R_{udp} = \frac{T_{udp}}{T_{tcp}},$$

где T_{udp} — объём входящего UDP-трафика, T_{tcp} — объём входящего TCP-трафика. Этот коэффициент характеризует наличие атаки класса UDP-flood, UDP — протокол односторонней передачи данных.

В трафике Web-сервера обычно присутствует небольшое количество пакетов, принадлежащих протоколу UDP, который для HTTP-соединений нехарактерен, поэтому многократное превышение UDP-трафика над TCP-трафиком позволяет обнаружить атаку класса UDP-flood.

3. Применение метода «гусеница». Применение анализа главных компонент, т.е. метода «гусеница», позволяет выполнить разложение исходного временного ряда по базису, состоящему собственных функций корелляционной матрицы этого ряда, которые имеют произвольный характер [3].

Для перечисленных выше метрик при наличии атаки SYN-flood метод даёт следующие результаты. Первая главная компонента всех метрик представляет собой тренд, отфильтрованный от высокочастотных составляющих, и несёт более 90% информации (дисперсии) исходного ряда (рис. 1-2, а). Эта компонента изменяется скачкообразно во время начала DDoS-атаки.

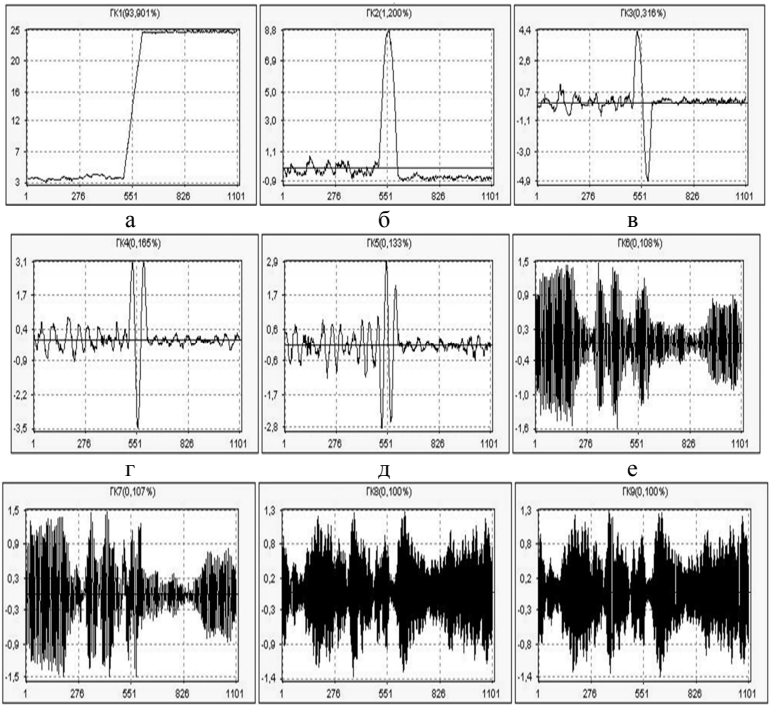


Рис. 1. Графики первых 9 главных компонент для R_{ip}, атаки SYN-flood.

Несколько следующих главных компонент указанных метрик (рис. 1-2, б-д), несут на себе существенно меньшую долю общей дисперсии и испытывают, как это видно из рисунка, наибольшие отклонения во время начала атаки с последующим снижением амплитуды и, соответственно, дисперсии.

Компоненты, начиная с шестой, представляют собой, согласно методу главных компонент, высокочастотные шумы. Для некоторых метрик (R_{syn}, R_{udp}) такие компоненты характеризуются уменьшением дисперсии после начала атаки.

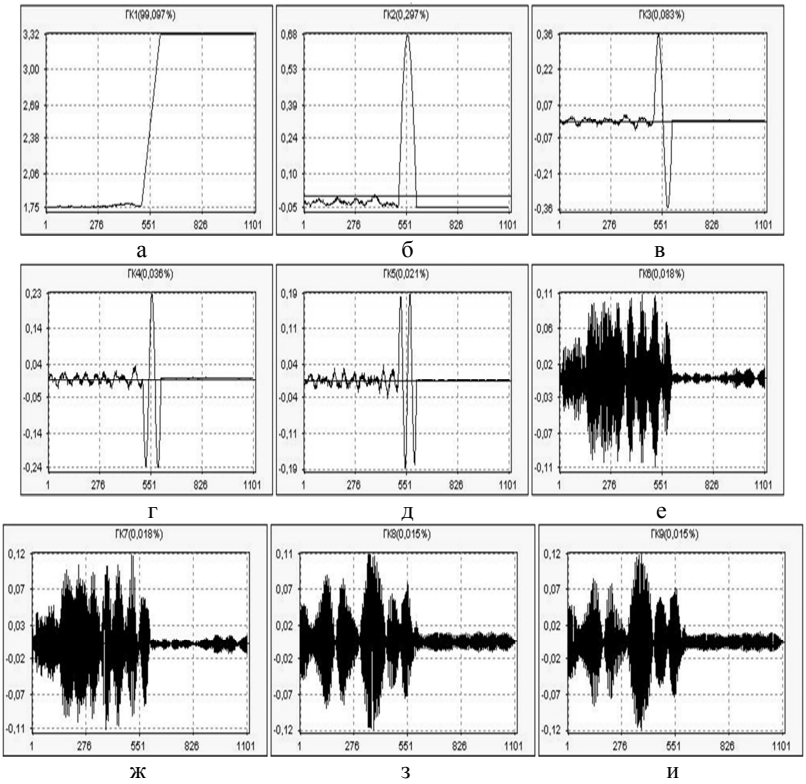


Рис. 2. Графики первых 9 главных компонент для R_{syn}, атаки SYN-flood.

Ниже приведены разложения для других классов DDoS-атак. На рис. 3, 4 представлены разложения наиболее характерных метрик для атаки типа UDP-flood. В частности, графики для метрики R_{udp} показывают, что тренд в момент появления атаки меняется скачкообразно, а другие главные компоненты изменяются с большей дисперсией.

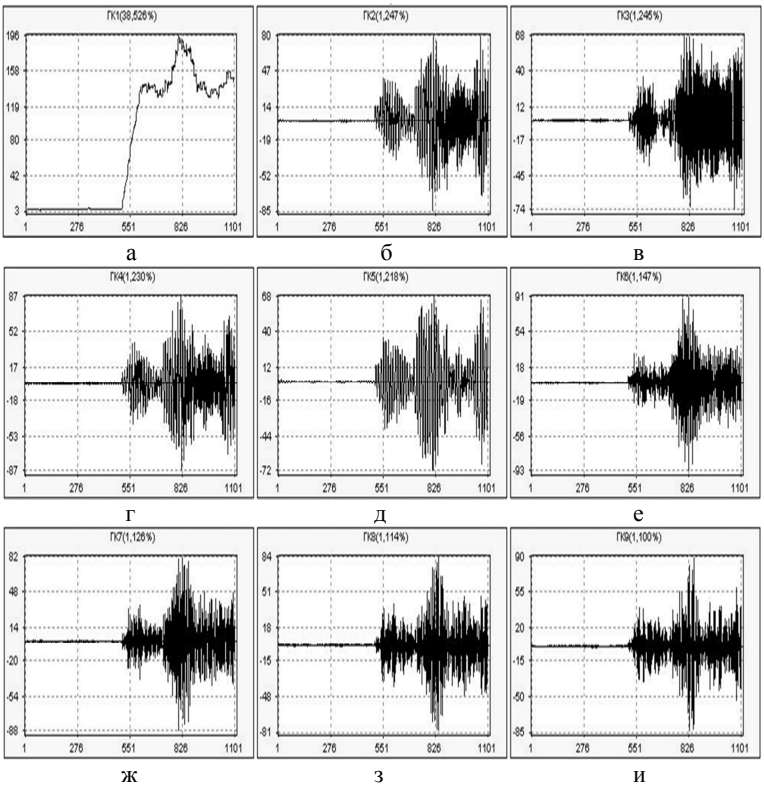


Рис. 3. Главные компоненты для R_{ip}, атаки UDP-flood.

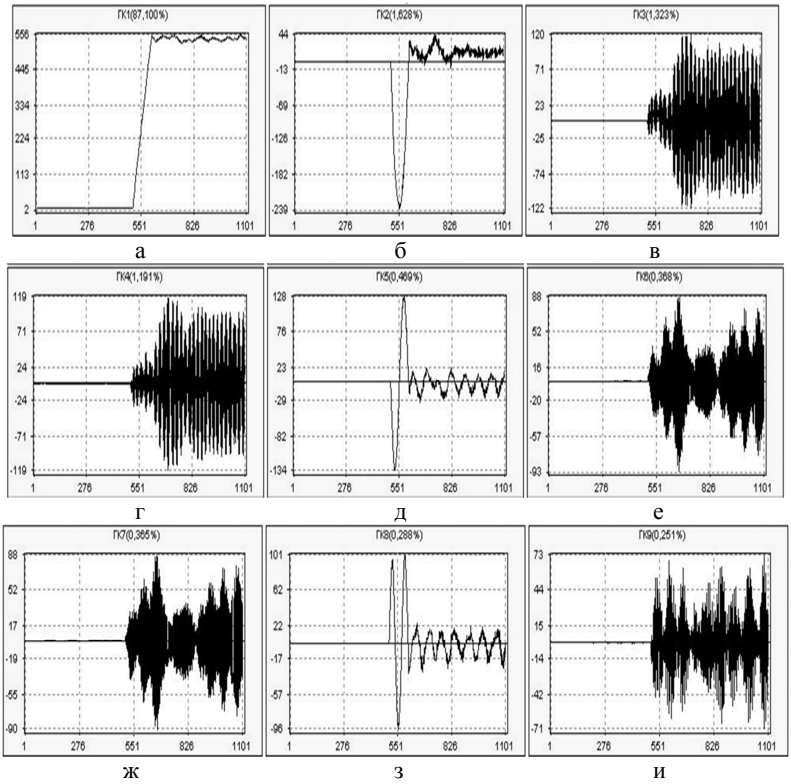
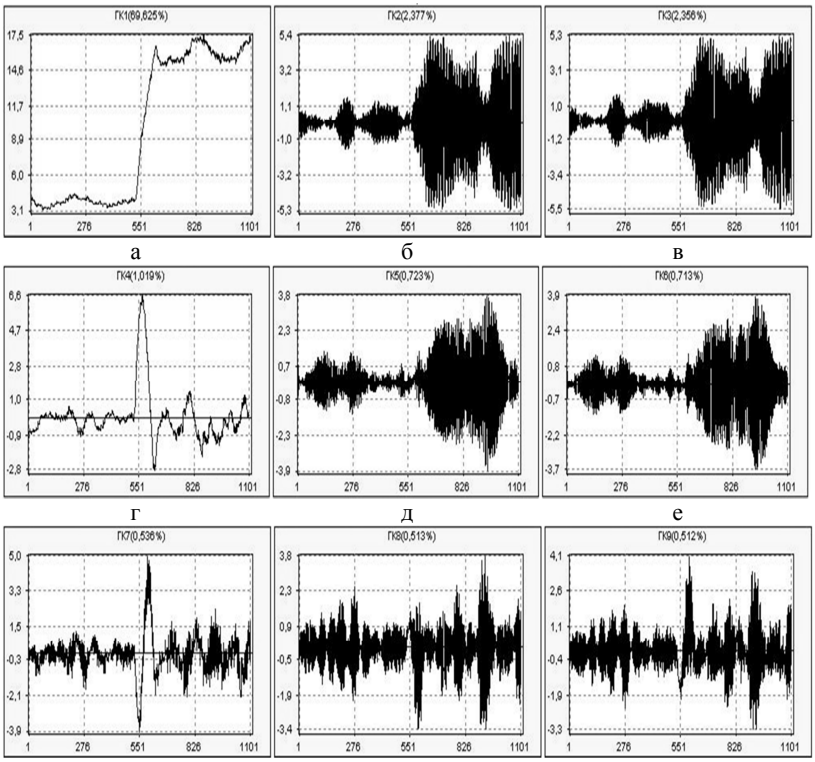


Рис. 4. Главные компоненты для R_{udp} атаки UDP-flood.

Аналогичные результаты получаются и для атаки HTTP-flood (рис. 5, 6).



а б в г д е ж з и

Рис. 5. Главные компоненты R_{ip} атаки HTTP-flood.

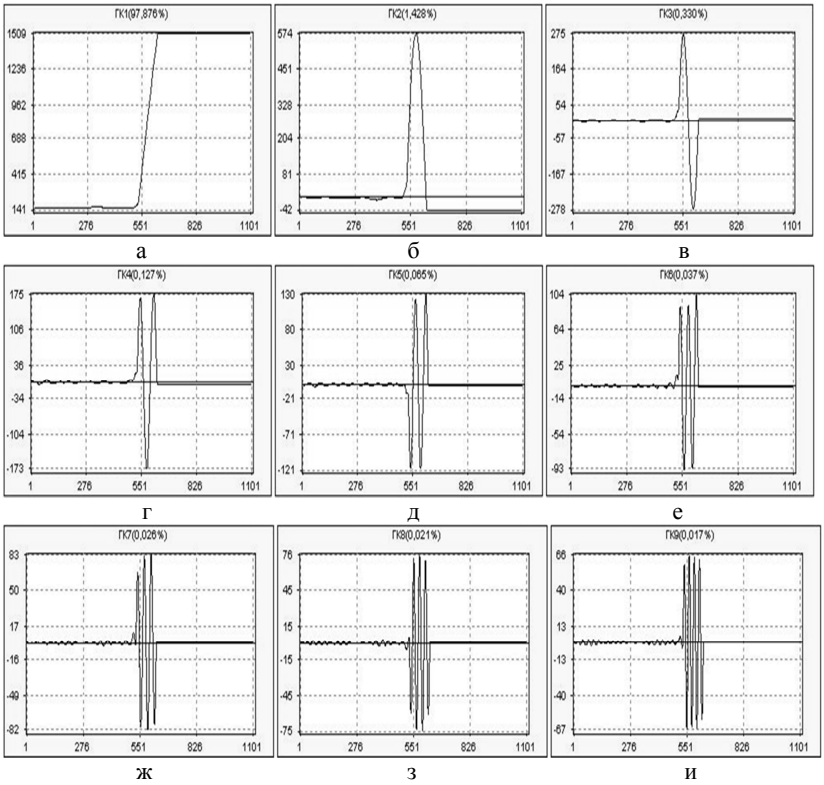


Рис. 6. Главные компоненты N_{web}, атаки HTTP-flood.

Таким образом, появление DDoS-атаки любого вида отражается на динамике главных компонент временного ряда.

4. Заключение. Обнаруженные закономерности открывают перспективу разработки системы обнаружения несанкционированных вторжений. Система перехватывает IP-трафик с помощью библиотек libpcap/WinPCap, в реальном времени рассчитывает значения приведённых выше метрик и выполняет разложение на главные компоненты. Принимать решение о наличии атаки можно, анализируя скорость изменения первой главной компоненты (тренда), анализируя дисперсию следующих главных компонент и фиксируя в них всплески амплитуды сигнала.

Литература

1. *Пичугин Ю.А.* Выборочные главные компоненты скользящего отрезка в анализе временных рядов метеорологических данных // Метеорология и гидрология, №8, 1999 г.С. 31–36.
2. Главные компоненты временных рядов: метод "Гусеница" /под ред. Д.Л.Данилова, А.А.Жиглявского. СПб: Пресском, 1997. 308 с.
3. *Голяндина Н.Э.* Метод «Гусеница»-SSA: анализ временных рядов. СПб.:2004. 76 с.
4. Фаткиева Р.Р. Корреляционный анализ аномального сетевого трафика // Труды СПИИРАН. 2012. Вып. 23. С. 93–100.

Пичугин Юрий Александрович — д-р физ.-мат. наук; профессор кафедры прикладной математики Российского педагогического университета (РГПУ) им. А.И. Герцена. Область научных интересов: разработка и использование статистических и динамических моделей для анализа и прогноза нестационарных многомерных временных рядов. Число научных публикаций — 81; РГПУ им. А.И. Герцена, ул. Казанская 6, 191186, Санкт-Петербург, РФ; р.т. +7(812) 314-48-85.

Pichugin Yury Alexandrovich — PhD in Physics and Mathematics, Dr. of. Sc., Prof.; Professor of Herzen State Pedagogical University of Russia (Department of Applied Mathematics). Scientific interests: design and application of statistical and dynamical models for multidimensional non-stationary time-series analysis and forecast. Number of publications — 81; yury-pichugin@mail.ru; Herzen State Pedagogical University of Russia, 6 Kazanskaya st. 191186, St. Petersburg, Russia; office phone +7(812) 314-48-85.

Фаткиева Роза Равильевна — канд. техн. наук; старший научный сотрудник лаборатории информационно-вычислительных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации РАН (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 — Ph.D., senior researcher, Laboratory of Computer and Information Systems, St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (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 Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: DDoS-атакb, 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 — BSc in Information Systems, junior researcher, Laboratory of Computer and Information Systems, St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Scientific interests: DDoS attacks, statistical analysis and modeling of the network traffic. DLe-

wonewski.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 10.03.2013.

РЕФЕРАТ

Левоневский Д.К., Пичугин Ю.А., Фаткиева Р.Р. **Исследование компьютерных атак методом сингулярного спектрального разложения сетевого трафика.**

Сетевые атаки вида Distributed Denial of Service (DDoS) благодаря простоте и эффективности представляют собой одну из самых значимых угроз для Web-сервисов. Существующие средства защиты часто не справляются с всё более профессионально организованными атаками, что объясняет необходимость исследований в области защиты от этих атак. В данной статье речь идёт об использовании статистического метода «Гусеница» для исследования сетевого трафика. Этот метод даёт возможность изучить структуру исходных данных и выявить скрытые поведенческие характеристики системы, что может быть полезно для построения систем проактивной защиты от атак.

В ходе работы было проведено моделирование DDoS-атак различных видов. На атакуемом Web-сервере в реальном времени измерялись величины, характеризующие загрузку системы: сетевой трафик и его отдельные составляющие (количество пакетов различных протоколов, количество флагов в TCP-заголовках). Для оценки состояния системы были определены наиболее информативные метрики, позволяющие идентифицировать атаку: отношение исходящего трафика к входящему, частоты TCP-флагов SYN и PSH, количество потоков критических приложений и некоторые другие. Временные ряды, построенные по этим метрикам, были взяты в качестве исходных данных для метода «гусеница».

Применение метода показывает, что появление DDoS-атаки любого вида сказывается на поведении главных компонент достаточно явно. Например, для SYN-flood первая главная компонента всех метрик (тренд) изменяется скачкообразно во время начала DDoS-атаки, а 4 следующие главные компоненты имеют всплески во время начала атаки с последующим снижением амплитуды и, соответственно, дисперсии. Компоненты, начиная с шестой, представляют собой высокочастотные шумы. Для некоторых метрик они также характеризуются уменьшением дисперсии после начала атаки.

Обнаруженные закономерности открывают перспективу разработки системы обнаружения несанкционированных вторжений. Система перехватывает IP-трафик с помощью библиотек операционной системы, в реальном времени рассчитывает значения приведённых выше метрик и выполняет разложение на главные компоненты. Принимать решение о наличии атаки можно, анализируя скорость изменения первой главной компоненты (тренда), дисперсию следующих главных компонент и фиксируя в них всплески амплитуды сигнала.

SUMMARY

Levonevskiy D.K., Pichugin Y.A., Fatkieva R.R. **Investigation of computer attacks by analysis of observed traffic singular spectrum.**

DDoS-attacks are among the most significant threats for the Web-services due to their simplicity and effectiveness. Existing defense measures often can't cope with more and more competently organized attacks, so the research in the area of intrusion detection is necessary. This paper considers the application of the "caterpillar" statistical technique to the investigation of the network traffic. This technique makes it possible to examine the structure of the source data and to reveal some hidden behavioral features of the system. This may be useful for development of the proactive defense systems.

During the research a simulation the various DDoS-attacks was performed. The values defining system load level, network traffic and its separate constituents (number of packages of different network protocols, number of TCP headers flags) were measured on the attacked Web-server in the real time. In order to estimate the system state the most informative metrics for the identification of an attack were defined. The examples are: the ratio of the out coming traffic to the incoming, frequencies of SYN and PSH flags in TCP headers, number of critical applications threads. Time series of these metrics were taken as input data for the "caterpillar" technique.

Application of the technique illustrates that the appearance of a DDoS-attack of any kind affects the behavior of the principal components. For example, during SYN-flood the first principal components (the trend) of all metrics changes greatly at the beginning of the DDoS-attack, and the next 4 constituents have single peaks at this moment with the increasing amplitude and decreasing variance. 6^{th} and higher component represent high-pitched noise. For some metrics their variance also decreases with the beginning of attack.

The revealed patterns give an opportunity to develop an intrusion detection system. Operation system's libraries capture the IP-traffic, evaluate the foregoing metrics in the real time and decompose them into the principal components. One can make decisions about the occurrence of the attack case on the base of dynamics of the first principal component and the variance of the other principal components.