На правах рукописи

Терновой Олег Степанович

# МЕТОДИКА И СРЕДСТВА РАННЕГО ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ DDOS-АТАКАХ

Специальность:
05.13.19 – Методы и системы защиты информации, информационная безопасность

**АВТОРЕФЕРАТ**
диссертации на соискание ученой степени
кандидата технических наук

Барнаул – 2016

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Алтайский государственный университет» (г. Барнаул)

**Научный руководитель –** Шатохин Александр Семенович, кандидат технических наук, доцент

**Официальные оппоненты:** Захаров Александр Анатольевич, доктор технических наук, профессор, заведующий кафедрой информационной безопасности Тюменского государственного университета

Рева Иван Леонидович, кандидат технических наук, доцент, доцент кафедры защиты информации, декан факультета автоматики и вычислительной техники Новосибирского государственного технического университета

**Ведущая организация –** федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технологический университет»

Защита состоится «23» марта 2017 г. в 15-15 часов на заседании диссертационного совета Д 212.268.03 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу: 634050, г.Томск, пр. Ленина 40.

С диссертацией можно ознакомиться в библиотеке ТУСУРа по адресу: 634045, г. Томск, ул. Красноармейская, 164 и на сайте https://tusur.ru/urls/mv3r2mws

Автореферат разослан «___» _____ 2017 г.

Ученый секретарь
диссертационного совета Д.Д. Зыков

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы диссертации**

DDoS-атака – распределенная атака, направленная на отказ в обслуживании. В результате атаки такого типа атакуемый сетевой ресурс получает лавинообразно нарастающее количество запросов, которые не успевает обработать. Источником вредоносных запросов являются так называемые зомби-сети, состоящие, большей частью, из компьютеров обычных пользователей, в силу каких-то причин зараженных вредоносным ПО.

Крупным DDoS-атакам подвергаются сайты правительства и органов власти, сайты ведущих IT-корпораций, таких как Amazon, Yahoo, Microsoft и т.д. Эти сайты, имеющие огромные ресурсы, не всегда могут справиться с атаками и отразить нападение.

Ежегодно различные компании, предоставляющие услуги в области обеспечения информационной безопасности и противодействия кибер-атакам, фиксируют увеличение количества DDoS-атак и их мощности. Периодические сообщения в средствах массовой информации о недоступности тех или иных ресурсов в результате распределенных атак, направленных на отказ в обслуживании, говорят о неэффективности средств противодействия такого рода атакам. На фоне указанных выше атак на ресурсы ведущих IT-корпораций, также увеличивается количество атак и к небольшим, средним сайтам, которые до недавнего времени не представляли интереса для злоумышленников. Однако, в настоящее время, в связи с увеличением важности и востребованности таких сайтов, перебои в их работе могут быть критичными. Вместе с этим меняются и мотивы, которые движут злоумышленниками, если раньше среди причин возникновения DDoS-атак можно было выделить протест, хулиганство и т.д., то сегодня все чаще DDoS-атаки являются орудием шантажа и способом вымогательства денег. Это переводит DDoS-атаки из плоскости единичных протестных акций в область криминального бизнеса, который не ограничивается вымогательством, но и становятся инструментом экстремистских и террористических организаций. Сегодня во всем мире стали обычной ситуацией атаки на сайты государственной власти накануне выборов или важных политических событий.

Причём, если вызвать отказ в работе крупного ресурса, имеющего в своем арсенале активные средства противодействия, можно, пожалуй, только заполнением всей полосы пропускания канала связи, что влечет необходимость в создании и поддержании достаточно большой бот-сети, то для парализации небольшого регионального ресурса достаточно небольшой по мощности атаки и, как следствие, небольшой бот-сети. Обслуживание и поддержание таких бот-сетей является менее затратным, и потенциально создать такие сети может большее количество злоумышленников. Этот факт на фоне отсутствия адекватных средств противодействия делает угрозы безопасности региональных ресурсов в результате DDoS-атак особенно значимым. С одной стороны, для противодействия таким атакам могут быть эффективно применены средства, предназначенные для отражения крупных атак. С другой – внедрение и

поддержание таких средств экономически затратно и не по карману региональным ресурсам. Средства противодействия, специализированные именно на обеспечение безопасности небольших и средних ресурсов, получили меньшее развитие из-за преобладания в прошлом именно крупных атак и в настоящее время отстают от эволюции самих DDoS-атак.

**Целью диссертационного исследования** является создание актуальной методики и инструментария для раннего обнаружения распределенных атак, направленных на отказ в обслуживании, их последующего обнаружения и блокирования вредоносного трафика на стороне атакуемого ресурса и его собственными силами.

Для достижения указанной цели в диссертационной работе поставлены и решены следующие задачи:

1. Проведен мониторинг современных DDoS-атак. Выявлена тенденция к развитию атак средней и малой мощности, направленных на региональные ресурсы.
2. Рассмотрены средства противодействия. Зафиксировано отсутствие эффективных средств противодействия атакам небольшой мощности.
3. Исследованы особенности DDoS-атак регионального уровня. Выработаны требования к методике и средству по обнаружению атак и дальнейшему противодействию им.
4. Решены задачи по созданию методики и программного комплекса по обнаружению DDoS–атак и вредоносных запросов.

**Объектом исследования** являются компьютерные сети и распределенные атаки, направленные на отказ в обслуживании осуществляемые в этих сетях.

**Предметом исследования** выступают модели и методы обнаружения распределенных атак, направленных на отказ в обслуживании, и выделение вредоносного трафика этих атак.

**В качестве основных методов** исследования, использованных в диссертационной работе, применялись методы теории вероятности и математической статистики, кластерного и системного анализа, методы машинного обучения.

**Научная новизна исследований** заключается в следующем:

1. Разработана оригинальная методика раннего обнаружения и противодействия распределенным атакам, направленным на отказ в обслуживании. Особенностями методики, являются: учет сезонных периодов, ориентация использования на конечном ресурсе, универсальность.
2. Впервые разработано формальное описание сезонности сетевого трафика для различной его периодичности, отличающиеся учетом неопределенного начала и завершения периода.
3. Впервые предложена критериальная оценка успешности работы кластеризаторов, позволяющая классифицировать трафик как легитимный и вредоносный.

4. Разработан алгоритм раннего обнаружения начала распределенных атак, направленных на отказ в обслуживании, особенностью алгоритма является учет сезонности в работе сетевого ресурса, который был применен впервые.

**Основными результатами**, выносимыми на защиту, являются:

1. Методика обнаружения и блокирования вредоносного трафика DDoS–атак основывается на анализе данных сетевого трафика и формальном описании сезонности. Методика позволяет определять вредоносный трафик на раннем этапе начала атаки и с высокой точностью. (соответствует пункту 2 паспорта специальности 05.13.19)
2. Формальное описание сезонности сетевого трафика позволяет фиксировать сезоны различной периодичности, отличающиеся учетом неопределенного начала и завершения периода.
   (соответствует пункту 14 паспорта специальности 05.13.19)
3. Алгоритм раннего обнаружения начала DDoS–атаки лидирует по времени обнаружения атаки среди аналогов, в среднем обнаружение происходит в четыре раза быстрее.
   (соответствует пункту 14 паспорта специальности 05.13.19)
4. Предложенные критерии успешности классификации сетевого трафика являются универсальными и позволяют оценить результаты работы различных классификаторов.
   (соответствует пункту 14 паспорта специальности 05.13.19)
5. Программное средство для обнаружения начала атаки и блокирования вредоносного трафика, разработанное на основе указанных алгоритмов, позволяет организовать эффективную защиту от DDoS–атак средней мощности силами атакуемого сервера. В среднем в 5 раз точнее и в 4 раза быстрее определяется вредоносный трафик при аналогичном количестве ложных срабатываний, по сравнению с аналогами.
   (соответствует пункту 5 паспорта специальности 05.13.19)

**Обоснованность и достоверность** представленных в диссертационной работе научных положений и результатов обеспечивается за счет корректной постановки задачи, тщательного анализа текущего состояния исследований в данной области, строгостью применения математических моделей и непротиворечивостью полученных результатов, а также теоретической апробацией в результате научных публикаций, выступлений и практическим применением полученных результатов.

**Практическая значимость** диссертационной работы заключается в создании методики и алгоритмов обеспечения безопасности сетевых ресурсов от DDoS–атак, позволяющих проводить активное противодействие непосредственно на стороне атакуемого ресурса, и в возможности практического использования разработанных методов и алгоритмов для поддержки безопасности работы сетевых ресурсов. Это подтверждено разработкой и последующим внедрением разработанного программного комплекса по обнаружению распределенных атак, направленных на отказ в обслуживании, и последующей блокировки вредоносных запросов на площадках различных уровней. Полученные результаты могут быть использованы при исследованиях в смежных областях, а также при разработке и

создании новых программных и программно-аппаратных комплексов по обеспечению безопасности от DDoS–атак.

**Личный вклад.** Все исследования в данной диссертационной работе проведены автором в процессе научной деятельности. Полученные результаты, в том числе выносимые на защиту, принадлежат лично автору. Заимствованный материал обозначен в работе ссылками.

**Апробация результатов работы.** Основные положения диссертационной работы докладывались на десяти научных конференциях различных уровней, в том числе на международных и специализированных конференциях, посвященных вопросам информационной безопасности. Среди основных конференций можно выделить следующие:

- Всероссийский конкурс студентов и аспирантов по информационной безопасности «SIBINFO-2013», Томск, 17 апреля 2013 г.
- XIII Всероссийская научно-практическая конференция «Проблемы информационной безопасности государства, общества и личности», Новосибирск, 5–9 июня 2012 г.
- XXV Региональная конференция по математике (МАК–2012), Барнаул 16–19 июня 2012 г.
- VI Международная научно-практическая конференция «Перспективы развития информационных технологий», Новосибирск 2 февраля 2012 г.
- XIX Всероссийская научно-методическая конференция «Телематика–2012», 25–28 июня 2012 г.

**Реализация результатов диссертационной работы.** Результаты диссертационной работы внедрены в деятельность ООО «Медиа группа Сфера влияния», КАУ «Алтайский государственный дом народного творчества», ООО «МЕМ» и используются для обеспечения безопасности сетевых ресурсов указанных организаций. Результаты диссертационной работы используются в учебном процессе, а также в научно-исследовательской деятельности студентов в ведущих высших учебных заведениях Алтайского края: ФГБУ ВО Алтайский государственный технический университет им. Ползунова, ФГБУ ВО Алтайский государственный университет. В рамках диссертационной работы разработано два программных средства: «Система раннего обнаружения DDoS-атак и вредоносного трафика» (Свидетельство о государственной регистрации в реестре программ для ЭВМ № 2013617238 от 06 августа 2013 г.; «Система управления сжимающим прокси сервером» (Свидетельство о государственной регистрации в реестре программ для ЭВМ № 2013660609 от 12 ноября 2013 г.

**Публикации.** Всего по теме диссертационной работы издано 15 научных публикаций, в том числе пять публикаций в ведущих рецензируемых журналах, рекомендованных для публикации результатов кандидатских и докторских работ ВАК. Вышла в свет глава в коллективной монографии, посвященной региональным аспектам технической и правовой защиты информации.

**Конкурсы и выставки.** Разработанное по результатам диссертационной работы программное средство по противодействию DDoS-атакам и обнаружению вредоносного трафика этих атак было представлено на региональной выставке

«IT-форум Алтайского края–2013» и заняло первое место. Также разработанное программное средство участвовало в краевом конкурсе «Лучший проект информатизации Алтайского края–2013 г.», организованного Торгово-промышленной палатой Алтайского края, где также одержало победу, заняв первое место. Разработанная методика раннего обнаружения DDoS-атак и вредоносного трафика была представлена на XIII Всероссийском конкурсе студентов и аспирантов в области информационной безопасности – «SIBINFO–2013» г. Томск, по результатам которого была отмечена дипломом финалиста. За исследования в области кибер-атак автор работы награжден профессиональной премией в области информационной безопасности национального форума по информационной безопасности «ИНФОФОРУМ–2013 – НОВОЕ ПОКОЛЕНИЕ», г. Москва, в номинации «Молодой специалист года».

**Структура и объем диссертационной работы.** Диссертационная работа выполнена на 130 страницах машинописного текста, содержит введение, четыре главы, заключение и приложение, список литературы, содержащий 96 наименований источников, 10 таблиц, 24 рисунка, 2 схемы.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

**Во введении** показана актуальность темы диссертации, сформированы цели и задачи исследования, представлены основные научные результаты, определена их научная новизна и практическая значимость, приведено краткое содержание по главам.

**В первой главе** исследуется текущее состояние проблемы распределенных атак, направленных на отказ в обслуживании, проводится мониторинг последних DDoS-атак. Данные для изучения вопроса берутся из официальных отчетов компаний, занимающихся вопросами обеспечения информационной безопасности и, в частности, вопросами противодействия DDoS-атакам. Среди этих отчетов можно выделить ежегодные отчеты компании «Лаборатория Касперского» и компании Prolexic Technologies. Данные из этих отчетов подтверждают друг друга и позволяют сделать вывод о возникновении новой группы DDoS-атак небольшой мощности, которые по своему количеству приближаются к крупным атакам. Самым популярным видом DDoS-атак продолжает оставаться http-flood. Вместе с этим аналитики отмечают эволюцию и усложнение этого вида атак. Современные клиенты бот-сети при обращении к атакуемому ресурсу пытаются имитировать поведение легитимных пользователей.

Мониторинг средств массовой информации показал, что за последние два года участились случаи проведения атак на небольшие и средние региональные сайты. Эти атаки также небольшой мощности в связи с отсутствием эффективных средств противодействия достигают своей цели. Данный процесс является вполне предсказуемым. Если несколько лет назад критичность в работе имели только крупные международные порталы, то на сегодняшний день с развитием глобальной сети и информационных технологий в регионах появляются небольшие, по мировым меркам, Интернет-ресурсы, которые, однако, имеют большую важность, и недоступность которых в результате DDoS-атак имеет большую критичность. Среди таких ресурсов можно выделить: региональные

новостные ресурсы, ресурсы региональных государственных учреждений, коммерческие Интернет-магазины и т.д.

Сообщение об успешных атаках на региональные сайты говорит об отсутствии эффективных средств противодействия для данной группы Интернет-ресурсов. Действительно, мониторинг современных аппаратных и программных средств противодействия и обнаружения DDoS-атак показал, что в основном эти средства предназначены для предотвращения мощных атак и использования крупными провайдерами или центрами. Использование этих средств для обеспечения безопасности регионального ресурса нецелесообразно.

Всего в первой главе рассмотрено около 15 различных методов, по обнаружению начала атаки и выделению вредоносного трафика. Среди этих методов, методы как российских, так и зарубежных авторов. К наиболее популярным методам можно отнести: MULTOPS, MIB variables, Network-aware clustering и т.д. При этом ни один из рассмотренных методов не учитывает сезонность. Многие методы предназначены для анализа данных «низкого уровня», доступ к которым из режима «виртуального хостинга» может быть затруднен.

**Во второй главе** предложена методика и алгоритмы раннего обнаружения начавшейся атаки и последующей блокировки вредоносного трафика. Особенностью разработанного алгоритма работы программного средства является его универсальность и возможность работы с различными данными. Определение начала атаки происходит с помощью расчета среднеквадратичного отклонения с учетом сезонности.

На примере статистических данных, характеризующих нагрузку различных сетевых ресурсов, приведено обоснование наличия сезонности и её уникальности для каждого конкретного ресурса (рис. 1,2).

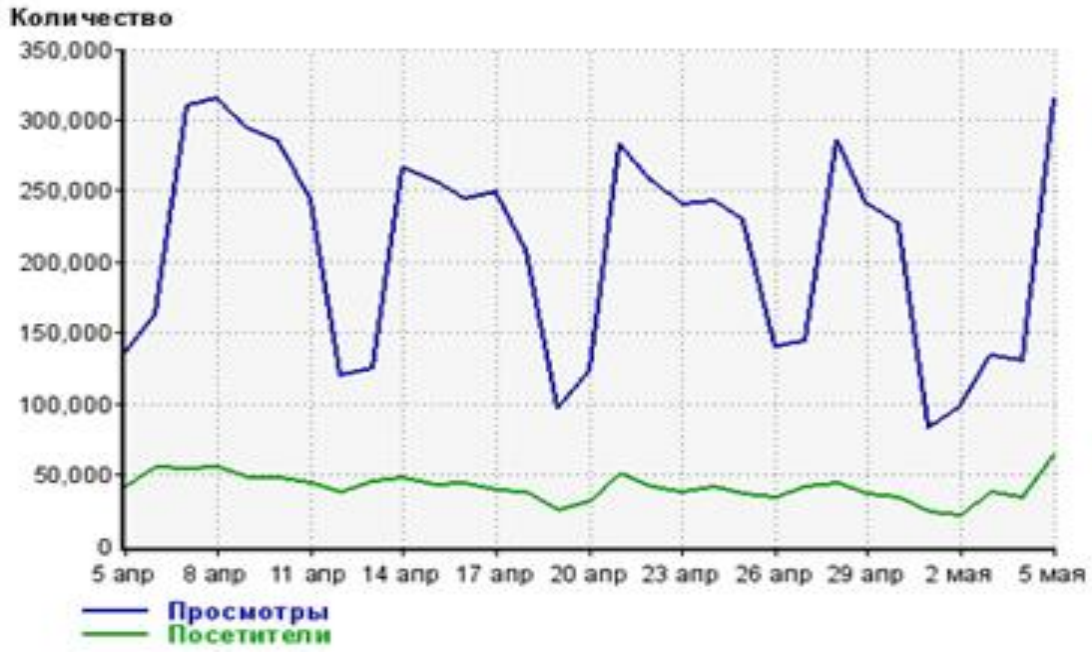


Рис. 1. Месячный график посещаемости и просмотра страниц, сайта ИА «Амител»

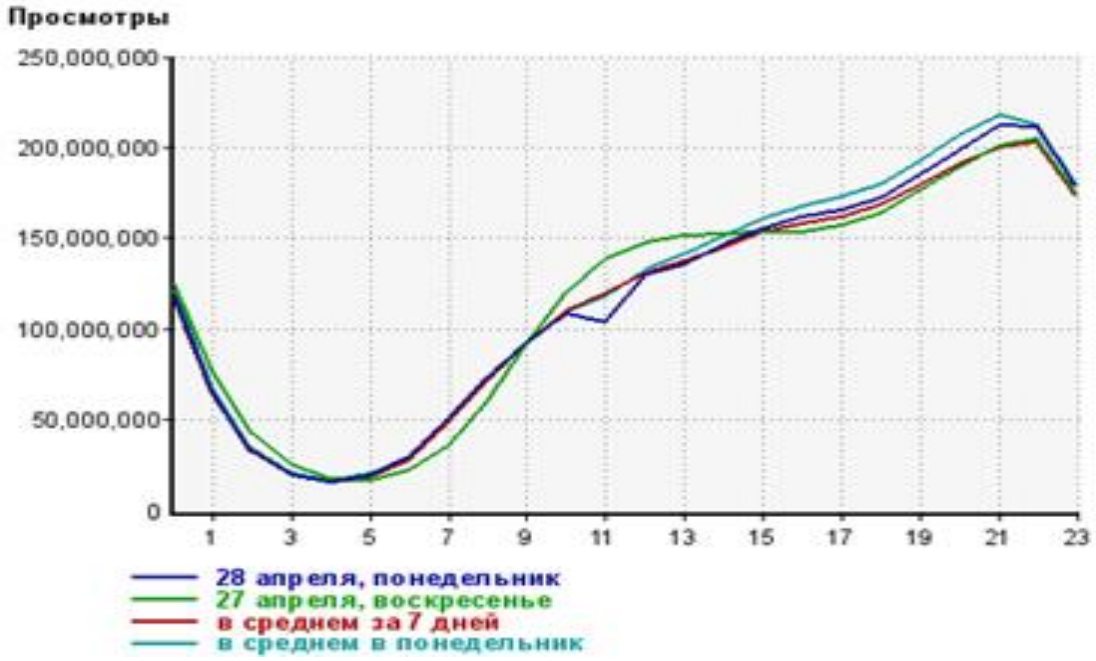


Рис. 2. Количество просмотров страниц, социальной сети «ВКонтакте», по часам

Учет сезонности нагрузки в работе сетевого ресурса позволяет проводить обнаружение атаки на самых ранних сроках, при этом повышается точность определения вредоносных запросов.

Для формального описания и математического обоснования выбора актуальных сезонных периодов применен метод Херста (1). Впервые метод был применен Херстом при проектировании плотины, для определения сезонных периодов разлива Нила. Метод отличается минимальными требованиями к вычислительным ресурсам.

| $r_1$ | $r_2$ | $r_3$ | $r_4$ | $r_5$ | $r_6$ | $r_7$ | $r_8$ | $r_9$ | … | $r_{T-3}$ | $r_{T-2}$ | $r_{T-1}$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\overline{r_1^2}, S_1^2, R_1^2$ $R_1^2/S_1^2$ | | $\overline{r_2^2}, S_2^2, R_2^2$ $R_2^2/S_2^2$ | | $\overline{r_3^2}, S_3^2, R_3^2$ $R_3^2/S_3^2$ | | $\overline{r_4^2}, S_4^2, R_4^2$ $R_4^2/S_4^2$ | | ..... | | | $\overline{r_{T_2}^2}, S_{T_2}^2, R_{T_2}^2$ $R_{T_2}^2/S_{T_2}^2$ | | $(R/S)_2 = \frac{\sum_{i=1}^{T_2} R_i^2/S_i^2}{T_2}$ |
| $\overline{r_1^3}, S_1^3, R_1^3$ $R_1^3/S_1^3$ | | | $\overline{r_2^3}, S_2^3, R_2^3$ $R_2^3/S_2^3$ | | | $\overline{r_3^3}, S_3^3, R_3^3$ $R_3^3/S_3^3$ | | | … | | $\overline{r_{T_3}^3}, S_{T_3}^3, R_{T_3}^3$ $R_{T_3}^3/S_{T_3}^3$ | | $(R/S)_3 = \frac{\sum_{i=1}^{T_3} R_i^3/S_i^3}{T_3}$ |
| ..... | | | | | | | | | | | | | |
| $\overline{r_1^N}, S_1^N, R_1^N$ $R_1^N/S_1^N$ | | | | ..... | | | | | | | $\overline{r_{T_N}^N}, S_{T_N}^N, R_{T_N}^N$ $R_{T_N}^N/S_{T_N}^N$ | | $(R/S)_N = \frac{\sum_{i=1}^{T_N} R_i^N/S_i^N}{T_N}$ |

(1)

где,

- $\bar{r}_j$ – среднее $j$ значений
- $S_j^2$ – дисперсия $j$ значений
- $X(t,j) = \sum_{i=1}^{t}(r_i - \bar{r}_j), t < j$ – накопленное отклонение
- $R(j) = \max_{1 \le t \le j} X(t,j) - \min_{1 \le t \le j} X(t,j)$ – размах
- $T_n$ = [($T$-1)/$n$]-число блоков, где $n$ = 2 .. [$T$/2]

Для каждого значения t строится график зависимости $Ln\ (R/S)_n$ от $Ln(n)$ (рис. 3). График линейно аппроксимируется. Коэффициент наклона кривой даёт оценку показателя Херста(H).

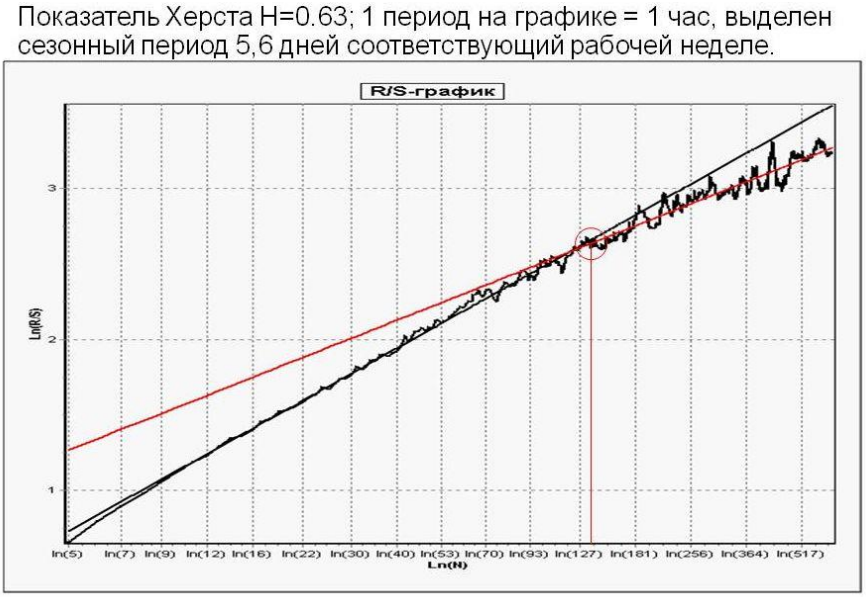


Рис. 3. График зависимости $Ln\ (R/S)_n$ от $Ln(n)$.

Применительно к анализу сетевого трафика данный метод дает возможность выявлять сезонные периоды в условиях неопределённости.

Методика обнаружения начала атаки и вредоносного трафика, учитывающая сезонные колебания, сводится к следующим шагам:

1. Определяются актуальные сезонные периоды.
2. С учетом сезонности определяется точка начала атаки.
3. Весь предшествующий началу атаки трафик помечается как благонадежный.
4. Смешанный трафик классифицируется на благонадежный и вредоносный.
5. Благонадежный трафик, выделенный из смешанного, сравнивается с трафиком, поступающим до начала атаки.
6. На основании результатов, полученных в предыдущем шаге, и выработанных критериев успешности выполняется корректировка выборки.
7. В дальнейшем весь поступающий трафик анализируется с учетом полученных данных.

Для более точного определения начала атаки используется скользящая оценка (2), характеризующая текущую сетевую активность. На основании этой оценки

устанавливается динамическая граница, актуальная для периода возможного начала атаки. В качестве скользящей оценки используется среднеквадратичное отклонение:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}\ , \qquad (2)$$

Для повышения точности скользящей оценки, расчет среднеквадратичного отклонения происходит с учетом сезонности.

Пусть сетевой ресурс испытывает сезонную суточную нагрузку.

$x_i$ – количество запросов к сетевому ресурсу за один час.

Количество суточных периодов $n$. Тогда запросы к сетевому ресурсу записываются в виде следующей матрицы:

$x_{1\,1}, x_{1\,2}, x_{1\,3} \ldots x_{1\,24}$

$x_{2\,1}, x_{2\,2}, x_{2\,3} \ldots x_{2\,24}$

……

$x_{n\,1}, x_{n\,2}, x_{n\,3} \ldots x_{n\,24}$

Каждая строка матрицы включает суточные данные о количестве запросов. Первая строка отражает данные текущих суток, в этой связи она может быть заполнена не до конца. Расчет среднеквадратичного отклонения в этом случае проводиться двумя способами.

1. Обычным способом с учетом определенного числа последних значений, например, так:

$x_{2\,1}, x_{2\,2}, x_{2\,3} \ldots x_{2\,24}, x_{1\,1}, x_{1\,2}, x_{1\,3}, x_{1\,4}.$

Значения берутся из строк матрицы.

2. С учетом сезонности расчет проводится по столбцам.

$x_{n\,1}, \ldots x_{2\,1}, x_{1\,1}.$

При нахождении в i-периоде, можно рассчитать границу для i+1 периода, используя значение i+1 столбца. При этом если сетевой ресурс испытывает нагрузку, связанную с недельными или суточными циклами, то необходимо исключить строки, которые соответствуют праздничным и выходным дням. Такой подход позволяет формировать достаточно точную верхнюю границу, нарушение которой может быть истолковано, как возникновение сетевой аномалии. Увеличение точности позволяет уменьшить время, необходимое для обнаружения атаки, и достаточно точно зафиксировать ее начало (рис. 4). При этом данный подход позволяет избежать одной из самых распространённых проблем в фильтрации трафика, связанной с негативным обучением фильтров. В ряде случаев злоумышленник может начать постепенно наращивать мощность атаки, таким образом, вредоносные запросы будут подмешиваться к легитимным, и так как мощность атаки ещё не большая, и не достаточна для фиксации её начала, вредоносные запросы будут помечаться, как благонадежные. В дальнейшем, при увеличении количества таких запросов, они смогут вызвать отказ в обслуживании. В предложенном способе количественная граница запросов рассчитывается для каждого сезонного периода, и в случае попытки негативного обучения фильтра, будет зафиксирована уже в следующем сезонном периоде, расположенном за периодом, в котором началась атака.

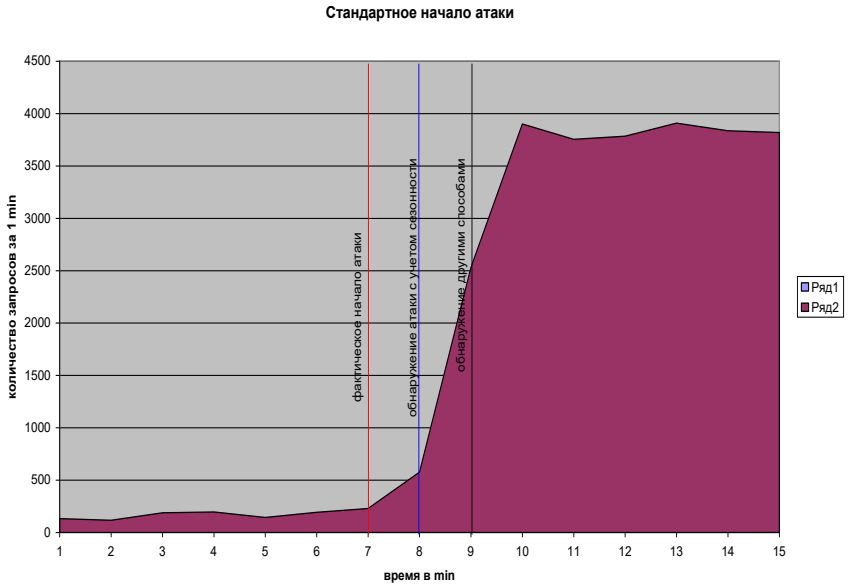


Рис. 4. Стандартное начало атаки

Кроме того, в рамках такого подхода исключаются возможности негативного обучения фильтров и срабатывания системы обнаружения с запозданием, путем постепенного наращивания мощности атаки (рис. 5) так как граница в этом случае будет строиться по сходным сезонным периодам. Например, постепенное наращивание мощности атаки в течение дня будет зафиксировано при сравнении количества запросов за текущие стуки с количеством запросов актуальных сезонных периодов за прошлые сутки.

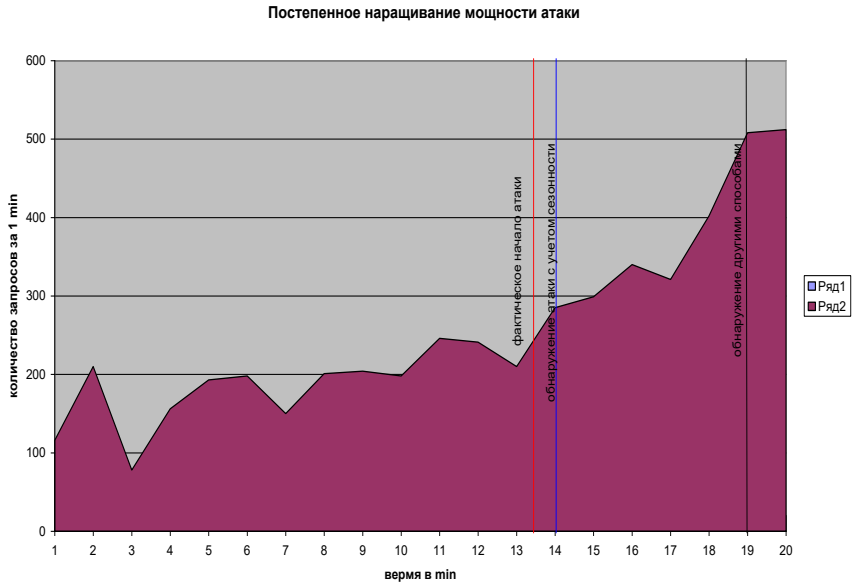


Рис. 5. Постепенное наращивание мощности атаки

Для последующего выявления вредоносного трафика используется решение, основанное на анализе аномалий, в результате которого происходит сравнение текущего состояния системы с ее нормальным состоянием. Сравнение состояний системы в контексте DDoS-атак проводится путем сравнения различных свойств сетевой активности. К этим свойствам могут быть отнесены: количество запросов,

тип запросов, количество запросов определенного типа или протокола, IP адрес источника, скорость поступления запросов, их время и т.д.

Пусть множество $A(a_1,a_2,a_3,\ldots a_n)$ – это набор всех возможных свойств для всех сетевых клиентов. Множество $B(b_1,b_2,b_3,\ldots b_m)$ – это множество благонадежных клиентов конкретного сетевого ресурса. Каждый сетевой клиент обладает набором индивидуальных свойств. Например, клиент $b_1$ имеет свойства $A1(a_4,a_{14}\ a_8,a_{10})$, клиент $b_2$ имеет свойства $A2(a_3,\ a_8,a_{11},\ a_{14})$ и т.д. Эти свойства представляют набор подмножеств множества A. Пересечение всех этих подмножеств характеризует клиентов сетевого ресурса, по которым они могут быть классифицированы. Точно так же неблагонадежные клиенты будут иметь свой набор свойств, по которому они также могут быть классифицированы.

Знание момента начала атаки в дальнейшем позволяет отнести весь предшествующий началу атаки трафик к благонадежному, после начала атаки - к смешанному. Первичное разделение смешанного трафика на благонадежный и вредоносный осуществляется с помощью алгоритма k-means:

$$V = \sum_{i=1}^{k} \sum_{x_j \in S_i} (x_j - \mu_i)^2 \qquad (3)$$

где $k$ — число кластеров; $S_i$ — полученные кластеры; $i = 1, 2, \ldots, k$ и $\mu_i$ – центры масс векторов $x_j \in S_i$.

В результате работы алгоритма смешанный трафик будет разделен на два кластера, соответствующих благонадежному и вредоносному трафику. Таким образом, на данном этапе доступны для анализа и обработки всего три группы трафика:

1. Характеризующая благонадежный трафик, предшествующий началу атаки
2. Характеризующая благонадежный трафик, выделенная из смешенного
3. Характеризующая вредоносный трафик, выделенная из смешенного.

Коррекция полученных выборок происходит с учетом выработанных критериев успешности:

1. **Критерий размерности полученных кластеров.** Если в текущем периоде, относящемся к атаке, количество запросов n, а в аналогичных сезонных периодах, относящихся к благонадежному трафику m. То количество вредоносных запросов будет приближенно равно n-m. Это же справедливо и для различных свойств сетевой активности (количество запросов к целевой странице, целевому порту, по определенному протоколу и т.д.)
2. **Критерий схожести благонадежных выборок.** Максимальная схожесть благонадежной выборки, предшествующей началу атаки, с благонадежной выборкой, выделенной из смешанного трафика.
3. **Критерий соответствия центров масс.** Центр масс благонадежной выборки, выделенной из смешанного трафика, должен соответствовать аналогичному сезонному периоду благонадежного трафика, предшествующего началу атаки.

Разработанная методика протестирована на данных из набора KDD Cup 99. Результаты тестирования приведены в Таблице 1.

Таблица 1 – Тестирование методики на данных из набора KDD cup 99

| **Вид запросов** | **Полнота** | **Точность** |
|---|---|---|
| Легитимные запросы | 0,9991 | 0,9811 |
| Вредоносные запросы | 0,9975 | 0,9924 |

**В третьей главе** описывается создание программного комплекса по обнаружению и противодействию распределенным атакам. В основе программного комплекса лежат разработанные во второй главе методы по обнаружению вредоносного трафика и точки начала атаки. На основании этих методов создан алгоритм работы программного комплекса.

1. С заданным интервалом времени актуальные данные извлекаются из файла access.log, проходят обработку и загружаются в базу данных.
2. Данные, загруженные в базу данных, постоянно анализируются на предмет начала атаки.
3. В случае обнаружения начала атаки выполняются следующие действия:
    - проходит оповещение заинтересованных лиц посредством рассылки электронной почты;
    - в автоматическом режиме выполняются скрипты, подготовленные системным администратором;
    - запускается механизм классификации трафика.
4. В результате работы механизма классификации трафика:
    - В базе данных создаются две таблицы, соответствующие благонадежному и вредоносному трафику.
    - Проходит первичное заполнение таблиц на основании проведенной кластеризации.
    - Вновь приходящие запросы классифицируются.
    - На основании этой классификации уточняются обучающие выборки.
5. Трафик, помеченный как вредоносный, блокируется.

Для создания гибкости и кроссплатформенности разрабатываемое программное средство разделено на три модуля:

1. модуль обработки данных и их загрузки в базу данных;
2. модуль обнаружения начала атаки;
3. модуль фильтрации трафика.

Универсальность в работе комплекса достигается с помощью возможности адаптации одного или нескольких модулей к работе с конкретными данными без вмешательства в основную часть программного комплекса. Программные модули создаются с помощью скриптового языка программирования общего назначения – PHP, что в свою очередь позволяет добиться кроссплатформенности. В связи с наметившейся тенденцией развития атак средней и малой интенсивности, преобладанием атак типа HTTP-flood и отсутствием эффективных средств противодействия, разработанное программное средство специализируется, прежде всего, на решении данных задач, и имеет следующие особенности:

1. Разрабатываемое средство ориентировано на противодействие атакам типа HTTP-flood.

2. В случае необходимости средство может быть использовано для противодействия DDoS-атак различных типов.
3. В своей работе средство основывается только на тех данных, которые могут быть получены в рамках работы физического или виртуального хостинга.
4. Для блокировки вредоносного трафика используются средства и инструменты, доступные в рамках физического или виртуального хостинга.
5. Средство отвечает требованиям кроссплатформенности. Может использоваться на разных операционных системах, с различными web-серверами и сетевыми сервисами.
6. Так как в результате DDoS-атаки сетевой ресурс может испытывать недостаток в свободных ресурсах, в процессе работы средство генерирует минимальную нагрузку на ресурсы сервера.

В данной реализации весь программный комплекс, состоящий из трех модулей, размещается на конечном сетевом ресурсе. В случае необходимости, модули программы могут быть размещены в различных местах. Так, например, на конечном сервере может находиться только средство загрузки данных.

Средства обнаружения атаки и фильтрации трафика могут быть установлены на отдельном сервере, недоступном для атаки из внешней сети. При такой установке программное средство сможет нормально функционировать и проводить классификацию трафика даже в случае отказа атакуемого сервера. Возможен вариант инсталляции, когда на узле, безопасность которого требуется поддерживать, вообще не установлено никаких модулей программного средства. В этом случае данные для анализа могут быть получены от сетевых локаторов или вышестоящих маршрутизаторов. Блокировка трафика может быть осуществлена на вышестоящем узле.

Также программный комплекс поддерживает мультиинсталляцию при одновременном запуске нескольких одноименных модулей. Так, например, данные для анализа могут поступать в базу данных из нескольких источников. Данные о вредоносном трафике могут быть переданы для блокировки на разные уровни.

**Четвертая глава** посвящена практической апробации полученных результатов. Тестирование разработанного программного комплекса происходит в специально созданной, крупной нагрузочной сети. Всего в рамках практической апробации результатов в нагрузочной сети проведено около 300 тестов. Проводимые тесты представляют упрощенные копии, созданные по мотивам реальных DDoS-атак. По результатам четвертой главы данные тестов обобщаются, происходит сравнение эффективности разработанного программного комплекса с аналогичными программами и результатами сторонних исследований в этой области. В результате этих тестов разработанное программное средство подтверждает свою эффективность (таблица 2).

Необходимо учитывать, что созданная нагрузочная сеть может влиять на результаты проведенных тестов. Это влияние может быть обусловлено количеством компьютеров нагрузочной сети, их характеристиками, доступными ресурсами и т.д. Поэтому для объективной оценки и для сравнения результатов

работы программного средства с результатами, полученными в аналогичных исследованиях, была проведена серия «эталонных» тестов, которые описываются в сторонних работах (таблица 3).

Таблица 2 – Сводные результаты работы различных средств противодействия и обнаружения, по итогам нагрузочных тестов – копий DDoS-атак типа http-flood, максимально приближенных к реальным условиям.

| Система | Ложные срабатывания, % | Необнаруженные вредоносные запросы, % | Среднее время между началом и обнаружением атаки, мин. |
|---|---|---|---|
| Kaspersky Anti-Haker | 0,4 | 12,5 | 47 |
| Snort | 1,9 | 11,4 | 62 |
| Symantec | 2,3 | 10,9 | 43 |
| DDOS deflate | 1,7 | 20 | 60 |
| Разработанное средство | 2 | 7,4 | 12 |

Таблица 3 – Результаты «эталонных» тестов по сравнению эффективности

| Система | Ложные срабатывания, % | Необнаруженные вредоносные запросы, % |
|---|---|---|
| Kaspersky Anti-Haker | 0,1 | 10,3 |
| Snort | 4,4 | 10,1 |
| Symantec | 3,4 | 11,9 |
| DDOS deflate | 5,7 | 20 |
| Разработанное средство | 0,9 | 2,8 |

Далее, в четвертой главе приводятся данные об эффективности, полученные в результате внедрения разработанного программного комплекса на площадках различных организаций (таблица 4).

Таблица 4 – Сводные показатели эффективности разработанного программного средства по результатам внедрения на различных площадках

| № п/п | Название показателя | Результат |
|---|---|---|
| 1. | Сокращение времени реакции на атаку | в 5 раз |
| 2. | Сокращение экономических затрат на обеспечение информационной безопасности | на 20% |
| 3. | Увеличение времени доступности ресурса во время атаки | в 4 раза |

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

Диссертационная работа является законченным научным трудом, в котором решены все поставленные задачи и достигнута цель научного исследования.
Получены следующие основные результаты:

1. Проведен мониторинг современных распределенных атак, направленных на отказ в обслуживании. Выделена новая группа атак средней и малой интенсивности, направленных, в основном, на региональные ресурсы. Проведен мониторинг различных программных и аппаратных средств противодействия и средств обнаружения атак такого типа. Выявлено отсутствие средств, позволяющих адекватно решать поставленные задачи по обнаружению и противодействию для данной группы атак.
2. Предложена и обоснована гипотеза о существовании сезонности в работе различных сетевых ресурсов. Выяснены причины, влияющие на формирования и особенности сезонных периодов.
3. Предложено формальное описание сезонности сетевой нагрузки, которое позволяет выявлять сезоны различной периодичности, отличающиеся учетом неопределенного начала и завершения периода.
4. Исследование модели атаки позволило создать методику раннего обнаружения и противодействия DDoS-атакам средней и малой интенсивности. Методика является универсальной, учитывает, как региональные особенности, так и другие факторы, и может быть применена для обнаружения и противодействия DDoS-атакам различных типов и различной мощности. А также для обнаружения аномальных данных в различных сферах деятельности.
5. В процессе разработки методики создано два алгоритма: алгоритм определения точки начала атаки и алгоритм разделения смешанного трафика на благонадежный и вредоносный. Отличительной чертой алгоритмов является учет сезонных колебаний сетевой нагрузки.
6. Для алгоритма по разделению трафика выработаны критерии успешности. Данные критерии являются универсальными и позволяют не только оценить успешность работы алгоритма, но и других, сторонних средств по фильтрации трафика.
7. На основе предложенной методики разработано программное средство по обнаружению начала атаки и последующего обнаружения и блокировки вредоносных запросов. Разработанное средство отвечает требованиям кроссплатформенности, универсальности, открытости. Отличительной чертой разработанного средства является модульность и универсальность. При незначительном изменении отдельных модулей средство может быть применено для обеспечения безопасности сетевых ресурсов любых видов и их защиты от атак различных типов.
8. Для апробации результатов диссертационной работы и проведения экспериментов по изучению распределенных атак, направленных на отказ в обслуживании, на базе реальных компьютеров была создана крупная специализированная нагрузочная сеть. В рамках сети возможно проведение нагрузочных тестов, эмулирующих DDoS-атаки. Нагрузочная сеть

поддерживает создание сценариев и проведение упрощенных DDoS-атак на основе данных о реальных атаках. В этом случае проводимые атаки, по сути, являются уменьшенными копиями реальных атак. Проводимые нагрузочные тесты отвечают основным требованиям эксперимента. Возможно повторение теста необходимое количество раз, фиксация его результатов.

9. По результатам проводимых в нагрузочной сети тестов, также разработана методика по выявлению уязвимых DDoS-атакам скриптов и модулей в системах управления содержанием и последующей оптимизации.

## ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИОННОЙ РАБОТЫ ОТРАЖЕНЫ В СЛЕДУЮЩИХ ПУБЛИКАЦИЯХ

Статьи в ведущих рецензируемых журналах, рекомендованных Высшей аттестационной комиссией (ВАК) для публикации результатов кандидатских и докторских диссертационных работ:

1. Терновой О.С., Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате DDOS атак // «Известия Алтайского государственного университета». –2013 №1/2(77).
2. Терновой О.С., Шатохин А.С. Снижение ошибки обнаружения DDoS-атак статистическими методами при учете сезонности // Ползуновский вестник. – 2012. №3/2.
3. Терновой О.С., Шатохин А.С. Методика обнаружения уязвимостей к DDoS-атакам систем управления контентом на примере системы Wordpress // «Известия Алтайского государственного университета». –2012. №1/2(73).
4. Терновой О.С., Шатохин А.С. Раннее обнаружение DDoS-атак статистическими методами при учете сезонности // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. №1(25).
5. Терновой О.С., Шатохин А.С. Использование байесовского классификатора для получения обучающих выборок при определении вредоносного трафика на коротких интервалах // Известия Алтайского государственного университета. – 2013. №1/2(74).

**Глава в коллективной монографии:**

6. О.С. Терновой, А.С. Шатохин. Методики и средства выявления и противодействия угрозам информационной безопасности в контексте региональных web-ресурсов // В.В. Поляков // Региональные аспекты технической и правовой защиты информации. – Барнаул, 2013.

**Свидетельства о регистрации программных продуктов:**

7. О.С. Терновой Система раннего обнаружения DDoS атак и вредоносного трафика / О.С. Терновой, А.С. Шатохин // Свидетельство о государственной регистрации в реестре программ для ЭВМ № 2013617238 от 06 августа 2013
8. О.С. Терновой Система управления сжимающим прокси-сервером / О.С. Терновой // Свидетельство о государственной регистрации в реестре программ для ЭВМ № 2013660609 от 12 ноября 2013

**В других изданиях, сборниках трудов и тезисов конференций.**

9. О.С. Терновой, А.С. Шатохин. Имитация и исследование DDOS-атак в лабораторных условиях // Труды XIX Всероссийской научно-методической конференции «Телематика–2012». Санкт-Петербург, 25–28 июня 2012 г. / под ред. Кривошеева А.О. – Санкт-Петербург, 2012.
10. Терновой О.С. Разработка средства противодействия DDoS атакам типа HTTP-flood средней интенсивности // «SIBINFO–2013» : Материалы XIII Всероссийской конференции студентов и аспирантов по информационной безопасности «SIBINFO–2013». Томск, апрель 2013 г.
11. Терновой О.С. Раннее обнаружение DDoS-атак на основе статистического анализа // Перспективы развития информационных технологий: Сборник материалов VI Международной научно-практической конференции «Перспективы развития информационных технологий». Новосибирск, 3 февраля 2012 г. / под ред. Чернова С.С. – Новосибирск, 2012.
12. Терновой О.С. Обнаружение источников вредоносного трафика DDoS-атак методами статистического анализа // «МАК–2012» : Материалы XV Региональной конференции «МАК–2012». Барнаул, июнь 2012 г. / под ред. Н.М. Оскорбина. – Барнаул, 2012.