ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
Алтайский государственный университет

УДК 004.056.5

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

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:
к.т.н., доцент А.С. Шатохин

Барнаул – 2016

ОГЛАВЛЕНИЕ

Введение

Актуальность темы диссертации

DDoS-атака – распределенная атака, направленная на отказ в обслуживании. В результате атаки такого типа атакуемый сетевой ресурс получает лавинообразное 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 [1]. Крупным DDoS-атакам подвергаются сайты правительства и органов власти, сайты ведущих IT-корпорация Amazon, Yahoo, Microsoft и т.д. Эти мощные корпорации, имеющие огромные ресурсы, не всегда могут справиться с атаками и отразить нападение [2,88].

Ежегодно различные компании, предоставляющие услуги в области обеспечения информационной безопасности и противодействия кибер-атакам, фиксируют увеличение количества DDoS-атак и их мощность. 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 к ведущим IT-корпорациям 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 их важности и востребованности, 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 следствием шантажа и способом вымогательства денег. Это переводит DDoS-атаки из плоскости единичных протестных акций в область криминального бизнеса, который не ограничивается

вымогательством, но и является инструментом экстремистских и террористических организаций [89]. Сегодня во всем мире стали обычной ситуацией атаки на сайты государственной власти накануне выборов или важных политических событий [90].

Причем 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 [91].

Целью диссертационного исследования является создание актуальной методики и инструментария для раннего обнаружения распределенных атак, направленных на отказ в обслуживании, и последующего обнаружения вредоносного трафика на стороне атакуемого ресурса и его блокировки 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 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. Среди основных публикаций можно выделить:

- О.С. Терновой, А.С. Шатохин Снижение ошибки обнаружения DDoS-атак статистическими методами при учете сезонности // Ползуновский вестник. – 2012. №3/2.
- 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). – С. 123–126.
- О.С. Терновой, А.С. Шатохин. Методики и средства выявления и противодействия угрозам информационной безопасности в контексте региональных web-ресурсов // Региональные аспекты технической и правовой защиты информации. – Барнаул, 2013.
- 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).
- 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.
- 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.
- 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.

- 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).
- 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).

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.

Краткое содержание работы. 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 количеству атак на крупные сайты. 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 дата–центрами. Использование этих средств для обеспечения безопасности регионального ресурса нецелесообразно.

Во второй главе предложена методика и алгоритмы раннего обнаружения начавшейся атаки и последующей блокировки вредоносного трафика. Особенностью разработанного алгоритма является учет сезонных колебаний в нагрузке сетевого ресурса, примененный впервые, также алгоритм и методика отличаются универсальностью и возможностью 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 наличие сезонности и её уникальности для каждого конкретного ресурса. Учет сезонности нагрузки в работе сетевого ресурса позволяет проводить обнаружение атаки на самых ранних сроках, при этом повышается точность определения вредоносных запросов. Знание 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 кластерного анализа, в дальнейшем происходит уточнение полученных кластеров с помощью специально выработанных критериев успешности. Классификация вновь поступающих запросов может происходить с использованием различных классификаторов при помощи полученных обучающих выборок и выработанных критериев успешности.

В третьей главе описывается создание программного комплекса по обнаружению и противодействию распределенным атакам. В основе программного комплекса лежат разработанные во второй главе алгоритмы. Приводится обоснование выбора среды разработки и вспомогательных

средств. Особое внимание при проектировке программного комплекса уделяется кроссплатформенности и возможности использования для анализа различных типов данных в рамках обеспечения безопасности различных приложений. Для обеспечения этих требований программное средство разделяется на несколько программных модулей, которые и составляют комплекс по обнаружению начала атаки и последующему выделению вредоносного трафика. Универсальность в работе комплекса достигается возможностью 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.

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 собой 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. Также в четвертой главе приводятся данные об эффективности, полученные в результате внедрения разработанного программного комплекса на площадках различных организаций.

Глава 1. Обзор современных DDoS-атак, методов и средств противодействия

1.1. Основные определения

DDoS-атака – аббревиатура от английского Distributed Denial of Service, распределенная атака, направленная на отказ в обслуживании. Атаки такого типа могут быстро истощить сетевые ресурсы или мощности сервера, что приведет к невозможности получить доступ к ресурсу и вызовет серию негативных последствий: упущенная прибыль, невозможность воспользоваться услугами и произвести различные транзакции и т.д. [1].

В DDoS-атаке в роли атакующего выступает так называемая бот-сеть, или зомби-сеть. Зомби-сеть может насчитывать от нескольких десятков до тысяч хостов. Обычно это нейтральные компьютеры, которые в силу каких-то причин (отсутствие файрвола, устаревшие базы антивируса и т.д.) были заражены, вредоносными программами. Программы, работая в фоновом режиме, непрерывно посылают запросы на атакуемый сервер, выводя его таким образом из строя [2].

В настоящий момент не существует какого-то универсального средства для противодействия DDoS-атакам. Даже такие крупные компании, как Microsoft, eBay, Amazon, Yahoo, страдают от DDoS-атак и не всегда могут с ними справиться [2].

1.2. Анализ и мониторинг современных DDoS-атак

В соответствии с отчетом, опубликованным компанией «Лаборатория Касперского», число DDoS-атак постоянно увеличивается [3,4]. Так, например, за второе полугодие 2011 г. значительно увеличилось количество атак. При этом увеличилась и мощность проводимых атак, по сравнению с первым полугодием она выросла на 57%.

- Во втором полугодии 2011 г. максимальная мощность атак, отраженных Kaspersky DDoS Prevention по сравнению с первым полугодием, увеличилась на 20% и составила 600 Мбит/с, или 1 100 000 пакетов/секунду (UDP-flood короткими пакетами по 64 байта).
- Средняя мощность отраженных Kaspersky DDoS Prevention-атак во втором полугодии 2011г. выросла на 57% и составила 110 Мбит/с.
- Самая протяженная DDoS-атака, зафиксированная во втором полугодии, продолжалась 80 дней 19 часов 13 минут 05 секунд и была нацелена на туристический сайт.
- Средняя продолжительность DDoS-атак составила 9 часов 29 минут.
- Больше всего DDoS-атак в течение второго полугодия – 384 – было нацелено на сайт одного из кибер-криминальных порталов.
- DDoS-атаки осуществлялись с компьютеров, находящихся в 201 стране мира.

Вместе с количеством и мощностью постоянно растет и сложность самих атак. Злоумышленники ищут принципиально новые методы проведения атак, и очень часто существующие средства защиты оказываются бессильными перед ними. Так, например, сравнительно новый вид DDoS-атак — THC-SSL-DOS эксплуатирует особенности SSL протокола и дает возможность одному компьютеру сделать недоступным сервер средней конфигурации [3].

14 февраля 2012 г. был атакован сайт американской биржи Nasdaq. В результате атаки сайт полностью перестал реагировать на запросы. При этом биржа Nasdaq является крупнейшей электронной фондовой биржей США и второй в мире по величине рыночной капитализации [5].

20 марта 2013 г. началась одна из крупнейших DDoS-атак в истории Интернета. Атака в основном коснулась европейских пользователей, вызывая перебои с доступам к различным ресурсам. В пиковые моменты атака достигала 300 гигабит в секунду. Результаты атаки наблюдали мировые

точки обмена трафиком и провайдеры первого уровня. Примечательно, что эта атака стала следствием конфликта между двумя Интернет-организациями [6].

Российская Федерации также не отстает от мировой тенденции роста DDoS-атак, а по некоторым позициям занимает даже первые места. По сообщениям средств массовой информации, с февраля по март 2013 г. из Российской Федерации было произведено более 2,4 миллиона кибер-атак, что делает ее безусловным лидером в этой области [7].

4 декабря 2011 г. многие российские Интернет-СМИ не смогли в рабочем режиме освещать думские выборы из-за беспрецедентных по размаху DDoS-атак. Злоумышленникам удалось «положить» сайты сразу нескольких независимых изданий, в том числе «Коммерсант», «Слон» и «Эхо Москвы». Кроме того, в очередной раз был недоступен Живой Журнал [8].

17 марта 2012 г. сайт крупнейшей российской телекомпании НТВ подвергся DDoS-атаке и был недоступен в течение нескольких дней [9].

Лаборатория Касперского сообщает, что в 2013 г. количество DDoS-атак в Российской Федерации увеличилось в 20 раз по сравнению с 2012 г. [10].

По данным компании Prolexic Technologies, специализирующейся на защите от DDoS, в апреле–июне общее количество атак на ее клиентов увеличилось на 20%. Средняя мощность DDoS-атак составила 49,24 Гбит/с, что на 9,25% больше, чем год назад. Второй не менее важный показатель по паразитному трафику – скорость передачи пакетов (pps) за год повысился на 16,55% – до 47,4 млн пакетов в секунду. Средняя продолжительность DDoS-атак за квартал возросла на 10%, за год – на 123% [11].

Если несколько лет назад таким атакам были, как правило, подвержены крупные сайты с преимущественно международным трафиком, то сегодня в сети наметилось смещение атак в сторону региональных ресурсов средней величины [12].

На основании отчета компании Prolexic Technologies можно выделить две доминанты мощности атак. Множество атак низкой мощности (от менее 1 до 5 Гб/с) – это целевые, узконаправленные атаки, по большей части уровня приложений (HTTP Flood и т.д.) или SYN Flood. На диаграмме (рисунок 1) видно еще один пик, соответствующий атакам мощностью более 60 Гб/с [11]. Причем атаки малой мощности выходят на первый уровень. Это означает, что увеличивается количество атак, направленных на малые и средние ресурсы. Среди которых преобладающее количество – это региональные ресурсы. Растет сложность самих атак. Так, например, в результате атак типа HTTP-flood зомби-компьютеры уже не пытаются бездумно запрашивать одну и ту же страницу, а эмулируют действия реальных пользователей.

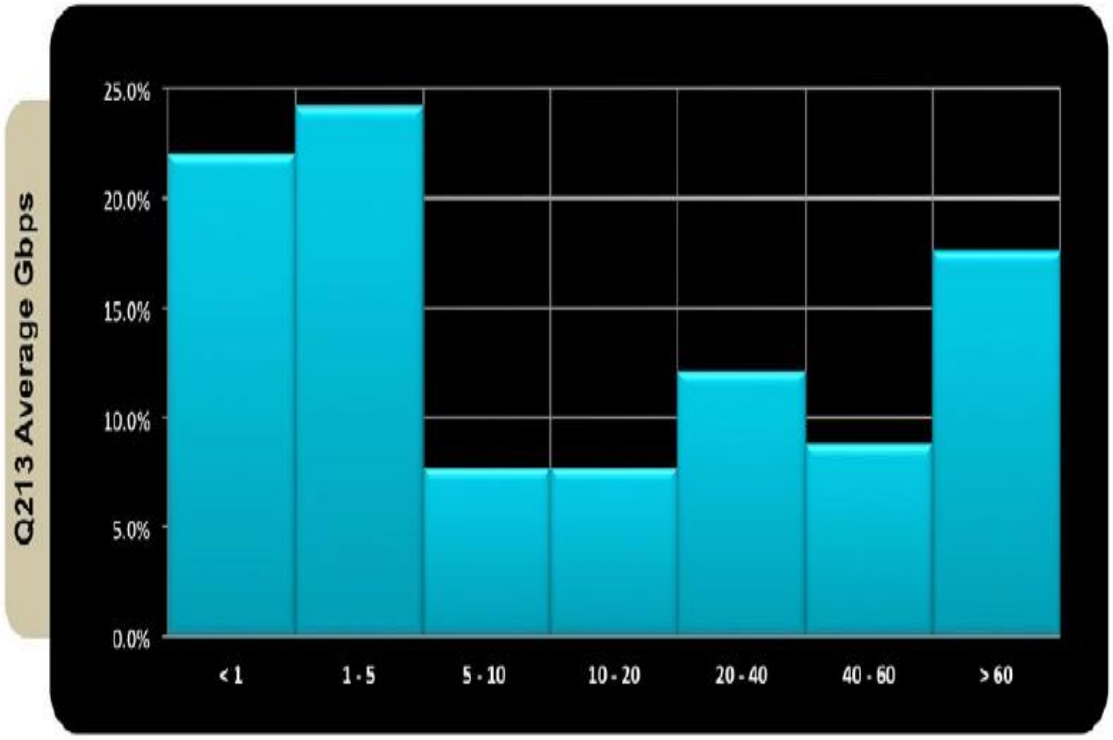


Рисунок 1. Диаграмма распределения мощности DDoS-атак [13]

О необходимости создания единой системы обнаружения, предупреждения и отражения компьютерных атак на информационные ресурсы России говорит Президент Российской Федерации Владимир Владимирович Путин [14].

Примечательно, что уже 15 января 2013 г. Президент подписал Указ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [15].

Кроме того, до конца 2013 года в структуре российских Вооруженных сил должен появится род войск, который будет отвечать за информационную безопасность [16].

Нельзя сказать, что DDoS-атакам подвержены только ресурсы мирового или государственного уровня. Так, например, подобные атаки фиксируются и на региональном уровне. Если рассматривать Алтайский край, то за последние годы была совершена серия атак на сайты региональных СМИ и органов государственной власти:

15 апреля 2013 г., официальный сайт Алтайского Законодательного собрания подвергся распределенной атаке, направленной на отказ в обслуживании, и периодически был недоступен в течение нескольких дней [17].

13 июня 2012 г. сразу несколько сайтов, принадлежащих Информационным агентствам Алтайского края, подверглись массированной DDoS-атаки. Среди них сайты ИА «ПолитСибРу», ИА «Банкфакс», ИА «Амител» [12].

При этом нельзя сказать, что это разовые атаки. Спустя несколько месяцев сайт Информационного агентства «Амител» вновь подвергся атаке и был недоступен в течение нескольких часов [18].

Все приведенные факты информационных атак показывают, что на сегодняшний день DDoS-атаки активно используются абсолютно на всех уровнях для достижения самых различных целей, начиная от банального шантажа и заканчивая задачами военно-политического характера [16].

При этом успешность этих атак говорит о недостаточной эффективности методов защиты информационной безопасности в области обнаружения и противодействия DDoS-атакам.

1.3. Виды DDoS-атак

Общепринятым подходом в классификации DDoS-атак является их разделение на виды, по протоколам, используемым в процессе атаки. Данная классификация приведена в работах Човдури, Зоу, Ксианга [19]. В отчете компании «Лаборатория Касперского», по DDoS-атакам за 2013 г., атаки также группируются по типам протоколов (рисунок 2) [10]. Аналогично атаки классифицируются в отчетах компании Prolexic Technologies [11].

Рисунок 2. Распределение DDoS-атак по типам [10]

Также существуют другие способы классификации атак. Например, в отчете Миттала атаки классифицируются по типам ресурсов, на которые они направлены [20].

Наиболее полный подход в классификации видов DDoS-атак предложен в статье Миркович, Мартина, Райера [21]. В рамках этого подхода классификация осуществляется не только по типу атаки, но и по степени автоматизации, частоте атаки, виду воздействия и т.д. Аналогичный подход предлагается в статье Ковалева [92].

Как видно из отчета компании «Лаборатория Касперского» (рисунок 2), наиболее популярным типом атак на сегодняшний день являются атаки типа HTTP или HTTP-flood. Суть данной атаки заключается в отправке большого количества HTTP-пакетов к атакуемому серверу. Атака данного типа может быть рассчитана как на отказ самого сервера, так и на переполнение полосы пропускания канала связи. Ранее атаки подобного типа являлись самыми примитивными, однако, сегодня с ростом популярности атак такого типа происходит и их усложнение. Так, например, злоумышленники производят атаку на потенциально уязвимые страницы сайта, т.е. скрипты, расходующие большое количество ресурсов и предоставляемые большие по размеру ответы. Или же пытаются имитировать действия легитимного пользователя. Как правило, таким атакам предшествует предварительное исследование сайта-жертвы.

Вторыми по популярности являются атаки типа SYN-flood. Данные атаки эксплуатируют особенности «тройственного рукопожатия» в результате установки соединения. Посылая SYN-запросы на подключения, зомби-компьютеры игнорируют ответные запросы, создавая на сервере очередь из «полуоткрытых» соединений. Популярность этого метода связана с отсутствием эффективных методик по выявлению вредоносных запросов. Методы, основанные на фильтрации трафика, замедляют работу сети в нормальном режиме, кроме того, могут спровоцировать блокировку шлюза или прокси сервера, от которых приходят запросы [65].

Атаки типа UDP и TCP-flood заключаются в отправке большого количества UDP и TCP-пакетов к атакуемому серверу.

DNS Amplification – описание атак такого типа встречается еще в 2006 г. [22], однако, активно атаки такого типа стали использоваться в последнее

время. Так, например, одна из самых крупных атак, зафиксированная в последнее время, использовала DNS усиление [6].

Суть данной атаки заключается в отправки к уязвимому DNS серверу запросов, в которых в качестве исходного адреса посредством подмены указан адрес компьютера жертвы. Отвечая на данные запросы, уязвимые DNS-сервера могут вызвать отказ в работе компьютера-жертвы.

1.4. Методы защиты от DDoS-атак. Обзор современных требований и решений.

Методы защиты от DDoS-атак можно разделить на две группы: это методы, предшествующие началу атаки, которые направлены на предотвращение самого факта атаки и методы, которые применяются уже после начала атаки, это методы активного противодействия и смягчения результатов атаки.

К методам по предотвращению атаки можно отнести организационно-правовые мероприятия. Например, недопустимость вовлечения в конфликтные ситуации, или меры, направленные на ликвидацию результатов, которых хочет добиться злоумышленник, например, разграничение и маскировка критичных ресурсов.

Также на этом этапе реализуется устранение уязвимостей и поддержка задействованного аппаратно-программного комплекса в актуальном состоянии. Некоторые виды сетевых атак направлены именно на эксплуатирование различного рода уязвимостей. Это могут быть уязвимости в программном обеспечении сервера. Или уязвимости, связанные с использованием не оптимизированных программных скриптов, которые могут чрезмерно расходовать ресурсы сервера. В данном случае для достижения преследуемого эффекта злоумышленнику потребуется организовать менее мощную атаку.

После начала атаки используются активные меры, направленные на противодействия атаки [2]. Основными из этих мер являются наращивание ресурсов и фильтрация трафика.

Наращиванию ресурсов предшествует подробный анализ загруженности сервера и сетевого сегмента с целью обеспечения узких мест. Так, например, если в нормальном рабочем режиме сервер расходует значительную часть канала связи, можно предположить, что в случае начала атаки, злоумышленник может добиться полного заполнения канала вредоносными запросами. В этом случае целесообразно заблаговременно увеличить пропускную способность канала связи.

Выделенные в результате анализа «узкие места» наделяются дополнительными ресурсами. Если основным потребителем ресурсов на физическом сервере является сервер баз данных, возможно, целесообразно разместить его на отдельно выделенном сервере или же даже создать распределенный кластер серверов баз данных. Аналогично можно поступить и с другими сервисами. Если продолжить рассмотрение в качестве атакуемого субъекта web-сервер, то, помимо баз данных, повышенную нагрузку может генерировать сам web-сервер или же размещенные на нем скрипты. В этом случае необходимо увеличить ресурсы самого сервера: дополнительная память, более мощный процессор и т.д. Или же посредством специальных инструментов выделить веб-сервера в отдельный кластер. Например, это можно сделать посредством использования связки web-серверов Apache и Nginx.

Такой подход к увеличению ресурсов не является панацеей от сетевых атак, кроме того, имеет ряд минусов:

- наращивание ресурсов связано с изменением аппаратного комплекса и не может быть оперативно проведено в момент начала атаки;
- поддержание избыточных ресурсов экономически нецелесообразно в период ожидания атаки.

Для преодоления этих минусов оптимальным является использование облачных технологий, которые позволяют наращивать ресурсы по мере надобности. Так, например, на сегодняшний момент на рынке представлены предложения от хостинг–провайдеров по предоставлению услуг облачного хостинга [23]. В результате предоставления услуги клиентам предоставляется необходимое в данный момент количество ресурсов. В случае увеличения нагрузки, это может быть, как увеличение числа легитимных пользователей, так и увеличение вредоносных запросов, происходит предоставление дополнительных мощностей, позволяющих обработать каждый запрос. В результате не происходит отказа сервера. Единственным минусом данного подхода является его экономическая составляющая. Так как клиенту облачного хостинга потребуется оплачивать дополнительные мощности, т.е. по сути, платить за обработку вредоносных запросов.

Другой подход увеличения ресурсов позволяет наращивать ресурсы в рамках сети доставки контента (CDN – аббревиатура от английского, Content Delivery Network) [24]. В результате реализации такого подхода происходит кэширование содержимого web-сервера и его доставка через распределенную сеть узлов. При выборе оптимального маршрута учитывается, как правило, географическое расположение клиента сети по отношению к ближайшему узлу. В результате сетевых атак вредоносный трафик делится между различными узлами сети и теряет свою мощность, также возможен вариант, когда вредоносный трафик просто не попадет на узел, в большинстве своем используемый легитимными пользователями. Например, в случае атаки из зомби-сети, находящейся за рубежом, вредоносные запросы будут концентрироваться на ближайшем к ним узле CDN-сети.

В любом случае использование этих подходов напрямую нецелесообразно, так как подразумевает обработку всех запросов без исключения, в том числе и злонамеренных.

Поэтому следующей группой методов, направленных на предотвращение атаки, являются методы, связанные с фильтрацией трафика. Блокировка

заведомо вредоносных запросов и обработка благонадежных и подозрительных позволяют существенно сэкономить средства, выделяемые на увеличение ресурсов.

Для фильтрации вредоносного трафика применяются различные программные и аппаратные средства, которые базируются на количественном и качественном анализе трафика. В основе методов анализа, данных средств, лежат методы кластерного анализа и математической статистики, теории вероятности, поведенческие методы и т.д.

Для эффективных мер противодействия и фильтрации трафика необходимо решение двух тесно связанных задач. Первая задача связана с обнаружением факта начала атаки, вторая – с определением источника атаки, т.е. источника вредоносного трафика. Чем точнее будут решены эти задачи, тем эффективнее будут меры противодействия. На сегодняшний день существуют два подхода, связанные с определением начала атаки. Это подход, основанный на анализе злоупотреблений, и подход, основанный на анализе аномалий. В первом подходе обнаружение атаки происходит путем сравнения данных, характеризующих текущие состояние системы, с данными, характерными для типичных атак. Второй подход оценивает текущее состояние системы с ее нормальным состоянием. Оба эти подхода имеют свои минусы, так, например, первый подход может быть не эффективным при обнаружении принципиально новых типов атак. Это особенно актуально в контексте именно DDoS–атак, так как злоумышленники стараются перейти от аномального поведения и симулировать действия реальных пользователей. Для успешной эксплуатации второго подхода необходимо накопление статистических данных, свидетельствующих о нормальном функционировании системы. Таким образом, для построения эффективной системы обнаружения целесообразно использовать оба эти подхода.

В результате работы такой системы происходит постоянный сбор данных, характеризующих состояние системы, затем их обработка и анализ

на предмет отличия от модельных данных. В случае начала атаки задействуются механизмы обнаружения источника трафика. Проводить сравнение с модельными данными можно различными методами.

К наиболее простым методам, относятся методы, реализованные на *основе правил*. Суть этих методов заключается в установке определенных правил, характеризующих нормальное и аномальное поведение системы. Правила могут описывать как поведение системы в целом, так и поведение её отдельных частей, например, частоту запросов, определенный набор полей запроса и т.д. При достаточной простоте и легкости использования, данные методы, тем не менее, весьма эффективны.

К наиболее популярным методам, можно отнести группу методов, основанных на количественном анализе. Методы данной группы пытаются обнаружить атаку по возрастающей нагрузке. Среди этой группы методов можно выделит, следующие:

Метод *MULTOPS* [25] анализирует соотношение принятых и отправленных пакетов.

Метод *MIB variables* [25] учитывает количество пакетов, их тип и количество запросов.

Методы *ACC* [26, 27] учитывают количество пакетов из различных подсетей.

В *Network-Aware Clustering* [28, 29] происходит группировка входящих запросов по подсетям и их сравнение.

В *Hop-Count Filtering* [30] ведется учет расстояний в хопах (скачках) до подсетей для фильтрации пакетов с ложным адресом отправителя.

Метод Gateway based [31], разделяет проходящий трафик на потоки на основе величины «поражающего воздействия».

D-Ward [32,33] проверяет лигитимность трафика по следующим протоколам

- по протоколу TCP - количество пакетов TCP-ACK,
- по протоколу ICMP - количество пакетов ICMP,
- по протоколу UDP - количество соединений и пакетов в соединении.

Также к перспективным методам можно отнести методы, основанные на *выявлении отклонений по изменениям вероятностных параметров данных*. Их суть заключается в следующем. Берется временной ряд определенного параметра состояний защищаемой системы (набор величин, посчитанных за определенное количество интервалов времени подряд). Значения этого параметра рассматриваются как случайные величины, полученные по некоему закону распределения. Делается предположение, что в момент атаки вид этого распределения меняется, т.е. меняются вероятностные параметры набора данных. Существует ряд методов для выявления таких «точек перехода» (change-point detection) [32, 34, 35].

Данный метод используется в Active Distributed Defense System [36], Improved D–Ward [32], Source IP address monitoring [35] и SYN flooding CUSUM detection [37]. В первом методе анализируется изменение количества новых IP-адресов от входящих соединений. Последние три метода основаны на *методе CUSUM* [32, 35], который позволяет итеративно отслеживать изменение заданного параметра, выявляя «точки перехода». Суть метода заключается в следующем. Если определенный параметр в течение нескольких интервалов времени был выше нормы, то задействуются защитные меры. В Improved D–Ward этим параметром является соотношение потока TCP-пакетов от источника к потоку подтверждений от получателя, в Source IP address monitoring - количество новых IP–адресов, а в SYN flooding CUSUM detection - соотношение пакетов TCP SYN-FIN(RST).

Меньшее распространение получили методы обнаружения атак с помощью извлечения данных (*Data Mining*). К таким методам можно отнести, например, методы, использующие иерархической системы различных обучающихся классификаторов [38].

Среди российских исследований можно выделить метод, предложенный в статье «Разработка системы обнаружения распределенных сетевых атак типа «Отказ в обслуживании»» [39]. Суть метода заключается в вероятностной оценке потерь заявок в сети.

В статье «Обнаружение распределенных атак на информационную систему предприятия» [40] предлагается подход, основанный на многоагентном моделировании.

В статье «Активные методы обнаружения SYN-flood атак» предложена модификация метода активного зондирования DARB, которая оценивает полуоткрытые соединения на основании общей сетевой загрузки [41].

Большинство описанных систем, использующих модельные данные, имеют два режима функционирования: режим обучения (построение модели или настройки пороговых параметров) и режим обнаружения.

На сегодняшний день существуют различные варианты практической реализации и использования указанных методов и систем. Так, например, учет и анализ данных может происходить с помощью программного модуля, установленного непосредственно на защищаемом сервере, или же это могут быть физические средства для анализа и сбора данных, вынесенные за пределы защищаемого сервера. Например, Cisco Guard представляет собой программно-аппаратный комплекс, взаимодействующий с анализаторами трафика установленными в различных сегментах сети.

По месту размещения средств противодействия их можно выделить в три группы:

1. Размещенные в сети источника вредоносного трафика.
2. Между сетями источника и сетью назначения.
3. Размещенные в сети назначения.

Эффективность средств противодействия и защиты увеличивается при их приближении, т.е. в более близком расположении к сети источника трафика. В этом отношении наиболее перспективными методами противодействия сетевым атакам становятся методы, предусматривающие блокировку трафика непосредственно в сети источника вредоносного трафика. Однако, эти методы недостаточно развиты в связи с организационными сложностями их внедрения.

Размещение средств защиты в сети назначения является менее популярным. Так как для организации полноценной защиты требуются сложные и экономически затратные меры:

- подключение к нескольким провайдерам первого уровня;
- наличие в штате компании специалистов, готовых к применению мер по отражению атаки в режиме 24 на 7;
- наличие в сети специализированного оборудования для защиты от сетевых атак.

Говоря о специализированном оборудовании для предотвращения атак и фильтрации трафика, можно выделить систему предотвращения атак Proventia Network IPS от компании IBM [42]. Данный аппаратно–программный комплекс имеет следующие возможности:

- Обработка более 200 протоколов различных типов и уровней.
- Контроль утечек информации
- Различные способы реагирования
- Около 3000 различных алгоритмов для анализа
- Обеспечивает защиту взаимодействующих в корпоративной сети компьютерных систем с помощью агента IBM Proventia Desktop
- Поддержка пользовательских сигнатур
- Всевозможные варианты реагирования на вторжения
- Помещение подозрительного трафика в карантин
- Производительность IPS для скоростей до 40 Гбит/сек и поддержка IPS для Crossbeam
- Поддержка 10 Гбит интерфейсов при помощи Network Security Controller и Crossbeam

Компания Cisco предлагает свое решение для предотвращения сетевых атак на базе Cisco Guard [43]. Этот аппаратно-программный комплекс, взаимодействуя с детекторами аномалий трафика в режиме реального

времени, перенаправляет трафик, предназначенный для целевого устройства, осуществляет его анализ и фильтрацию.

Как правило, такие средства предполагают защиту всей сети в целом и обычно нецелесообразны для построения защиты единичного конечного ресурса.

В связи с этим в настоящий момент большое распространение получили средства защиты и противодействия, устанавливаемые в промежуточных сетях.

Эффективность данных средств напрямую связана с количеством узлов, из которых они состоят. Таким образом, эффективные распределенные системы имеют высокую экономическую стоимость. Владение такими системами доступно или крупным компаниям, или специализированным сервисам по противодействию сетевым атакам. Например, подобную услугу по фильтрации трафика от вредоносных запросов предлагает компания «Лаборатория Касперского» в рамках предоставление услуги Kaspersky DDoS Prevention [44]. В рамках распределенной сети доставки контента Cloud Flare также реализована подобная возможность [45]. Использование таких сервисов по противодействию атакам достаточно эффективно. Экономически более выгодно, по сравнению с личным внедрением средств противодействия. Однако, предполагает включение промежуточного звена, собственно, самого сервиса противодействия между клиентом и сервисом.

Возвращаясь к группе методов и средств, организующих защиту непосредственно внутри атакуемой сети, необходимо выделить подгруппу средств, которые, в отличие от указанных выше дорогостоящих средств, располагаются не на границе сети, а непосредственно на атакуемой системе. Из-за особенности расположения данные средства не являются эффективными для отражения крупных атак. Так, например, они не могут противостоять крупным атакам и атакам, направленным на переполнения полосы пропускания канала связи. Именно поэтому в свое время данные средства защиты не получили должного развития. Однако, в связи с

наметившейся тенденцией к развитию атак низкой и средней мощности, они могут быть эффективны и экономически выгодны.

Среди этих систем можно выделить две группы программных средств:

- средства, действующие на уровне операционной системы атакуемого сервера;
- средства, действующие на уровне приложения.

К первой группе средств можно отнести программные файерволы и специализированные средства.

Conlimit [46]. Модуль для iptables, в *nix системах, позволяет настроить различные лимиты для подключений. Например, не более одного одномоментного подключения с одного адреса.

Ddos deflate [47]. Аналог Colimit. В случае превышения выбранных лимитов блокирует доступ на заданное время.

К другой группе можно отнести средства, которые работают на уровне атакуемых приложений. Это могут быть различные плагины или дополнительные модули, например, для web-серверов, баз данных, других сетевых сервисов.

mod_evasive [48] для web-сервера Apache позволяет проводить блокировку на основании различных правил: ограничение по адресу, количеству запросов, возможность выбрать продолжительность блокировки и т.д.

ngx_http_limit_zone_module [49] аналогичный модуль, но уже для web-сервера Nginx. Обладает сходным функционалом блокировок.

По сути, данные средства осуществляют только блокировку в соответствии с набором правил, не проводя при этом полноценный анализ трафика. То есть являются примитивными и явно недостаточными для противодействия распределенным сетевым атакам. Как правило, основным критерием для блокировки трафика служит превышение заданного количества запросов с определенного адреса. Но данное решение является грубым определением вредоносного трафика, так как под него попадают

различные частные случаи превышения лимитов и запросы из различных сетей, находящихся за прокси сервером или NAT маршрутизатором.

При этом потребность в средствах противодействия, реализованных на стороне сервера, существует. Об этом свидетельствуют различные самостоятельные решения и рецепты системных администраторов, которые периодически появляются в сети. Эти решения представляют попытки провести некоторый анализ входящего трафика, обычно поверхностный, и на основании этого анализа уже точечно блокировать трафик или же назначать ограничения на подозрительные подключения, например, посредством conlimit для iptables.

При этом сам по себе анализ вредоносного трафика на уровне атакуемого сервера или приложения имеет большие возможности, так как появляются дополнительные данные для выявления злоумышленника. Это могут быть, например, поведенческие данные, анализ маршрута навигации пользователя по сайту или анализ загружаемых данных.

Например, в прошлом был актуален метод обнаружения вредоносного трафика по типу загружаемых файлов. Его суть заключается в следующем. Легитимные пользователи проводят загрузку не только целевой страницы, но и сопутствующих данных: картинки, внешние скрипты, иконки и т.д. Зомби-компьютеры обращались только к целевой странице. В настоящее время данный метод потерял актуальность, так как современные зомби-компьютеры пытаются эмулировать действия легитимных пользователей.

1.5. Выводы по первой главе

В первой главе рассмотрен механизм распределенных сетевых атак, направленных на отказ в обслуживании. Проведен мониторинг различных DDoS-атак, осуществлявшихся в последнее время. Изучены отчеты по данному вопросу различных компаний, занимающихся обеспечением информационной безопасности и противодействию сетевым атакам.

В результате такого анализа замечено, что в настоящее время значительно увеличилось число DDoS-атака средней и малой интенсивности, направленных, как правило, на региональные ресурсы. Это увеличение вполне прогнозируемо – с развитием сети увеличивается потенциальное количество возможных жертв. Кроме того, совершенствуется сам механизм проведения атак. Для злоумышленника проведение атаки уже не является столь сложным. А зомби-компьютеры пытаются эмитировать действия самих пользователей. Все это ведет к общему увеличению числа атак.

Анализ средств противодействия показал, что в настоящее время большее развитие получила группа средств противодействия, предназначенная для отражения мощных атак. В эту группу входят, как правило, дорогостоящие средства, предназначенные для крупных провайдеров или компаний. Средства противодействия небольшим и средним атакам, базирующиеся на атакуемом сервере, представлены крайне скудно. Это связано с незначительным количеством таких атак в прошлом. При этом анализ входящего трафика на уровне приложений может быть более эффективным. С одной стороны, проведение такого анализа экономически не затратно, с другой – может быть вполне достаточным для отражения малых и средних атак, тенденция преобладания которых уже наметилась.

Глава 2. Методика защиты от DDoS-атак

2.1. Постановка задачи

Оптимальным решением для обнаружения начала атаки и последующего выявления вредоносного трафика будет являться решение, основанное на анализе аномалий, в результате которого происходит сравнение текущего состояния системы с ее нормальным состоянием. Сравнение состояний системы в контексте DDoS-атак можно проводить 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 [50].

В прошлом было популярно средство противодействия DDoS-атакам типа HTTP-flood, работающее на стороне атакуемого сервера и выявляющее вредоносный трафик с помощью анализа такого свойства сетевой активности, как тип загружаемых данных [51]. Дело в том, что браузер благонадежного клиента при загрузке содержимого web-страницы автоматически загружает дополнительные файлы, необходимые для нормального построения и отображения страницы. К этим файлам могут

относиться: изображения, находящиеся на странице, иконки, каскадные страницы стилей, фрагменты скриптов JavaScript, вынесенные в отдельные файлы. Для злоумышленника эти файлы являются бесполезными, его главная задача – заставить отработать скрипт, генерирующий страницу, и, тем самым, вызвать дополнительную нагрузку на ресурсы сервера. Таким образом, компьютеры зомби-сети могли быть идентифицированы с высокой долей вероятности по анализу только одного этого свойства. Естественно, что злоумышленники в ответ на создание данного метода усложнили алгоритм атаки, и на сегодняшний день зомби-компьютеры пытаются загружать и все сопутствующие данные.

В предыдущей главе было установлено, что на сегодняшний день DDoS-атаки усложняются, и злоумышленники пытаются полностью имитировать поведение благонадежных клиентов. В этой ситуации предпочтение при анализе свойств сетевой активности необходимо отдать тем свойствам, которые не могут быть подделаны злоумышленниками. При недостатке таких свойств необходимо вводить искусственные свойства, например, прохождение модификации тест Тьюринга – ввод данных с картинки.

Таким образом, задача по определению и выявлению вредоносных запросов в контексте данной работы сводится к их классификации на основании свойств сетевой активности.

Оптимальным решением для обнаружения вредоносного трафика является использование различных классификаторов и нейронных сетей. Сложностью в реализации данного решения является тот факт, что для нормального функционирования классификатора требуется иметь две актуальные обучающие выборки, соответствующие вредоносному и благонадежному трафику. Однако до момента начала атаки получить эти выборки не представляется возможным. Это вполне очевидно для выборки, соответствующей вредоносному трафику, так как до начала атаки вредоносные запросы отсутствуют. Но это также справедливо и для выборки,

характеризующей благонадежный трафик. Так как сетевая картина постоянно меняется, будет меняться и содержимое выборки соответствующей благонадежному трафику. Таким образом, выборка по благонадежному трафику, например, месячной давности, может быть не актуальна для текущей сетевой ситуации. Кроме того, есть риск, что в этой выборке могут оказаться данные, соответствующие вредоносным запросам, что в дальнейшем вызовет ошибки в работе классификатора. Эта проблема весьма актуальна, так как злоумышленник может специально начать подмешивать к благонадежному трафику незначительное число вредоносных запросов, которые не смогут быть идентифицированы в качестве начала атаки, но смогут негативно «обучить» выборку характеризующую благонадежный трафик.

Для преодоления этой проблемы необходимо точно определить точку начала атаки. Это даст возможность весь предшествующий трафик отнести к благонадежному и откроет дополнительные возможности по разделению смешанного трафика, который приходит после начала атаки, на благонадежный и вредоносный. В этом случае методика обнаружения вредоносного трафика, в первом приближении, будет сводиться к следующим шагам:

1. Определяем актуальные сезонные периоды.
2. С учетом сезонности определяем точку начала атаки.
3. Относим весь предшествующий началу атаки трафик к благонадежному.
4. Классифицируем смешанный трафик на благонадежный и вредоносный.
5. Сравниваем благонадежный трафик выделенный из смешанного с трафиком поступающим до начала атаки.
6. На основании результатов, полученных в предыдущем шаге и выработанных критериев успешности, корректируем выборки.
7. Весь поступающий трафик анализируем с учетом полученных данных.

2.2. Математическая модель обнаружения начала атаки и вредоносного трафика

2.2.1. Раннее обнаружение начала атаки статистическими методами с учетом сезонности

Начало DDoS-атаки связано с увеличением числа запросов к атакуемому серверу. Таким образом, для фиксации факта атаки необходимо установить границу по количеству запросов к серверу, при нарушении которой однозначно будет фиксироваться нештатная ситуация. Такой границей может выступать максимальное количество запросов к серверу, плюс некоторый запас возможных запросов. Возможность установки предельной границы, после которой будет происходить оповещение администраторов, активация необходимых модулей и т.д., реализована в различных сетевых средствах как программного, так и аппаратного уровня [43, 49]. При этом такой подход имеет ряд минусов:

1. Для предотвращения случайных срабатываний, устанавливаемая граница должна быть существенно выше максимального уровня количества запросов. Что, в свою очередь, приводить к возникновению погрешности при обнаружении атаки.
2. Сетевой ресурс может испытывать различную нагрузку в зависимости от времени суток и дней недели. В этом случае атака, начавшаяся в период затишья, например, в выходной день или ночью, будет зафиксирована с опозданием. Если в системе предотвращения вторжений предусмотрено использование классификаторов и обучение фильтров на основании входящего трафика, есть вероятность в их негативном обучении.

Для решения указанных проблем необходимо использовать скользящую оценку, характеризующую текущую сетевую активность. На основании этой оценки устанавливать динамическую границу, актуальную для периода

возможного начала атаки. В качестве скользящей оценки возможно использовать среднеквадратичное отклонение [50]:

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

где σ – среднеквадратическое отклонение;

n – количество рассматриваемых временных периодов;

x_i – количество запросов за i -период;

$\bar{x}$ – среднее арифметическое запросов по всем периодам.

В результате экспериментов по апробации методики, подробнее о которых будет рассказано в главе четыре, было установлено, что для разных сайтов оптимальное значение верхней границы может отличаться и находиться, как правило, в диапазоне от 2.2σ до 2.9σ. По этой причине, для более гибкой настройки создаваемого, в рамках апробации методики, программного обеспечения по обнаружению начала DDoS-атаки, этот параметр задан не жестко. У оператора программного комплекса есть возможность варьировать значение данного параметра.

Однако такой подход также имеет потенциальную уязвимость, связанную с тем, что злоумышленник может постепенно наращивать мощность атаки, сдвигая при этом границу среднеквадратичного отклонения. Устранить данную уязвимость может учет сезонных колебаний [52].

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 можно выписать 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 может проводиться двумя способами.

- 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.

- С учетом сезонности – расчет проводится по столбцам.

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

Если наблюдатель находится в i-периоде, можно рассчитать границу для i+1 периода, используя значение i+1 столбца. Если сетевой ресурс испытывает нагрузку, связанную с недельными или суточными циклами, то необходимо исключить строки, которые соответствуют праздничным и выходным дням. Или даже использовать только каждую седьмую строку, т.е. сравнивать, например, только период с 13:00 до 14:00 для каждого вторника.

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 (рисунок 3).

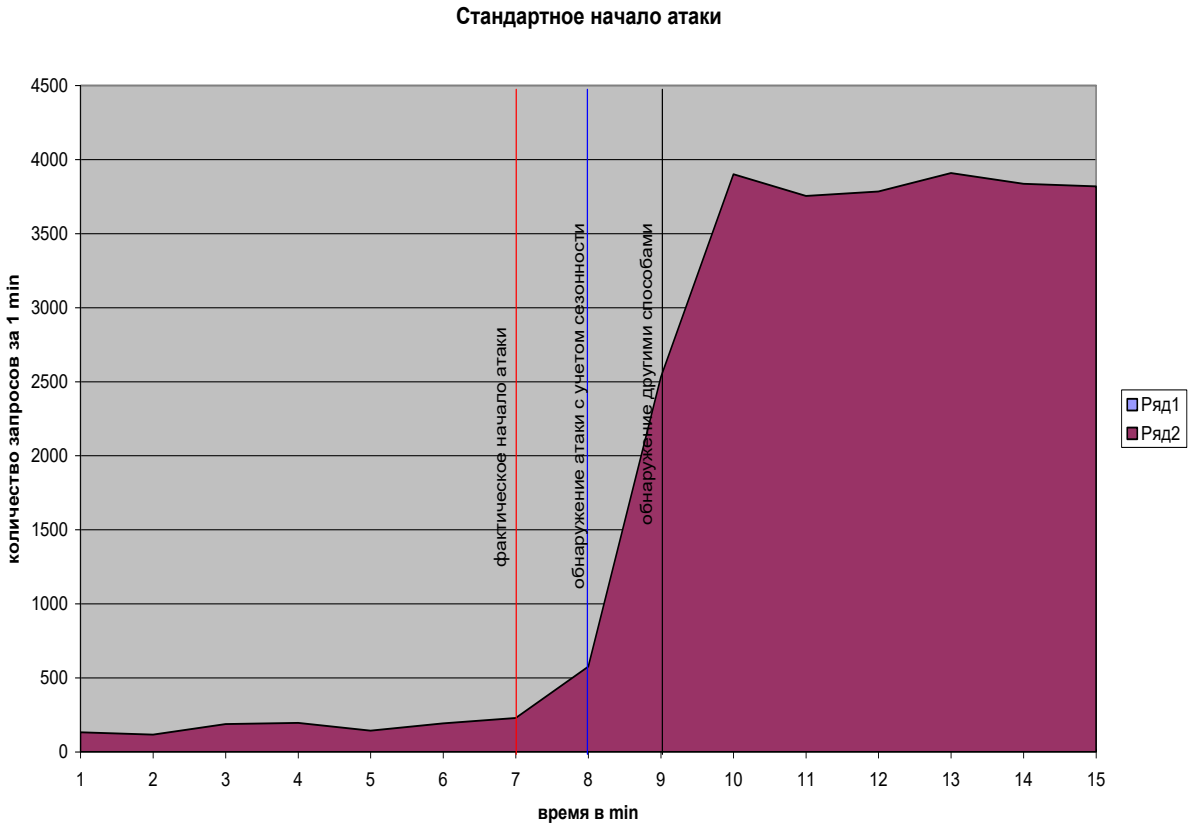


Рисунок 3. Стандартное начало атаки [53]

Кроме того, в рамках такого подхода исключаются возможности негативного обучения фильтров и срабатывания системы обнаружения с запозданием путем постепенного наращивания мощности атаки (рисунок 4). 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 с количеством запросов актуальных сезонных периодов за прошлые сутки.

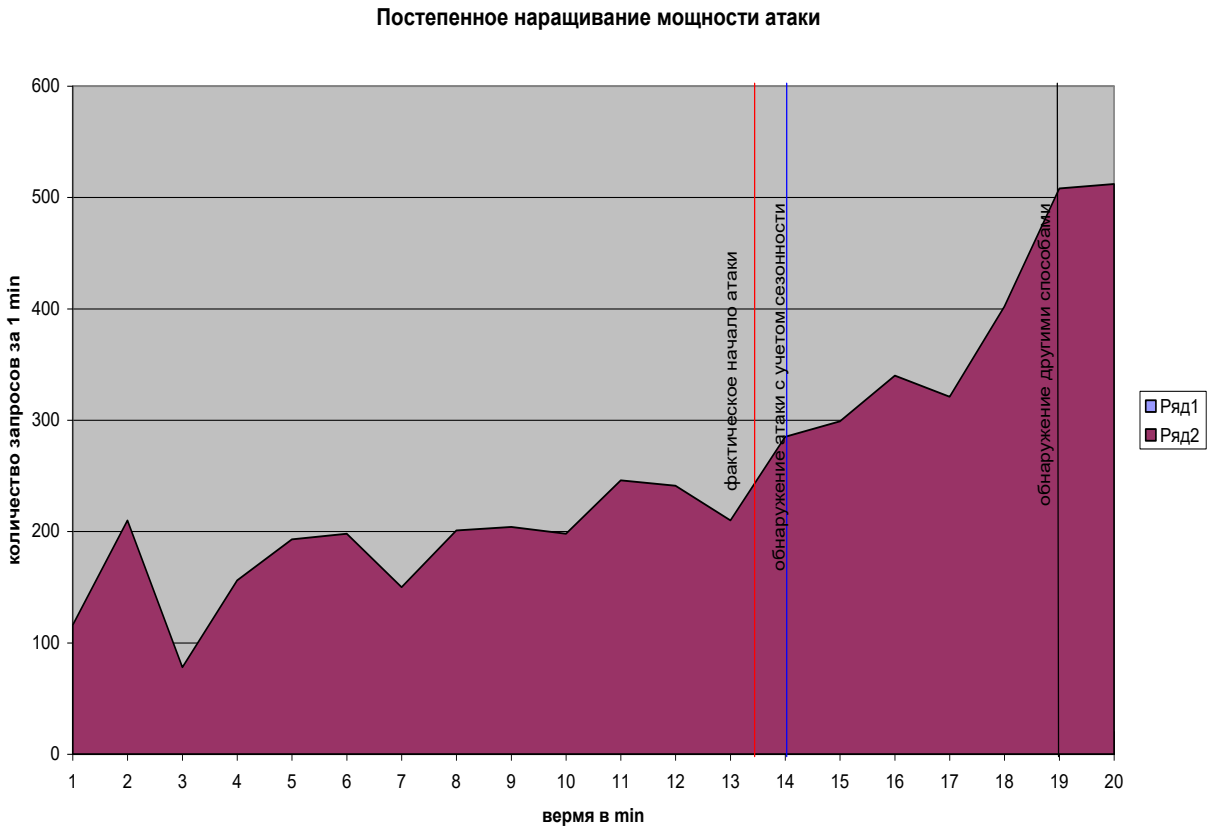


Рисунок 4. Постепенное наращивание мощности атаки [53]

2.2.2. Выявление и исследование сезонности

В рамках создания методики раннего обнаружения начала атаки, и ввиду перспективности подхода учитывающего сезонные колебания, было проведено дополнительное исследование, изучающее сезонные колебания количества запросов к сетевым Internet ресурсам. Основной задачей исследования было доказательство существования сезонных периодов в работе web-сайтов. А также решение вопроса, может ли случайный всплеск в посещаемости Internet ресурса, вызванный, например, публикацией на него ссылки с высоко посещаемого ресурса, вызвать нарушение сезонности, и, как следствие, ложное срабатывание.

Источником статистических данных для проведения исследования стал один из крупнейших сервисов статистики liveinternet.ru [54]. Этот сервис обслуживает более полутора миллионов сайтов, регистрирует ежедневно

около 10 миллиардов просмотров. Сервис собирает и обрабатывает разнообразные статистические данные, характеризующие: посещаемость сайта, источники переходов, посещаемость по времени суток, страны и регионы пользователей, их операционные системы и браузеры, а также много другой информации. Сбор данных происходит путем размещения на всех страницах сайта, чью статистику необходимо отслеживать, специального кода, который отправляет данные о посетителях, загружающих страницу сайта, в сервис статистики. Просмотр статистических отчётов, сгенерированных сервисом liveinternet.ru, доступен непосредственно владельцу сайта, а также может быть, по решению владельца, предоставлен и другим пользователям. Сайтов, которые в рамках данного сервиса по сбору и обработке статистики предоставляют открытый доступ к своим отчетам, достаточно большое количество. Именно эти сайты, с публичным доступом к статистике, и стали источником данных для анализа.

Всего в рамках исследования была проанализирована статистика 60 различных сайтов. В результате анализа было объективно установлено наличие сезонных периодов в работе web-сайтов.

Например, если рассматривать месячную посещаемость одного из крупнейших новостных порталов Алтайского края – Информационное агентство «Амител» (сайт http://amic.ru), то в его работе отчетливо видны недельные сезонные периоды (рисунок 5). Наблюдается всплеск просмотра страниц в начале рабочей недели, спад просмотров в течение всей недели и низкая активность пользователей на выходных.

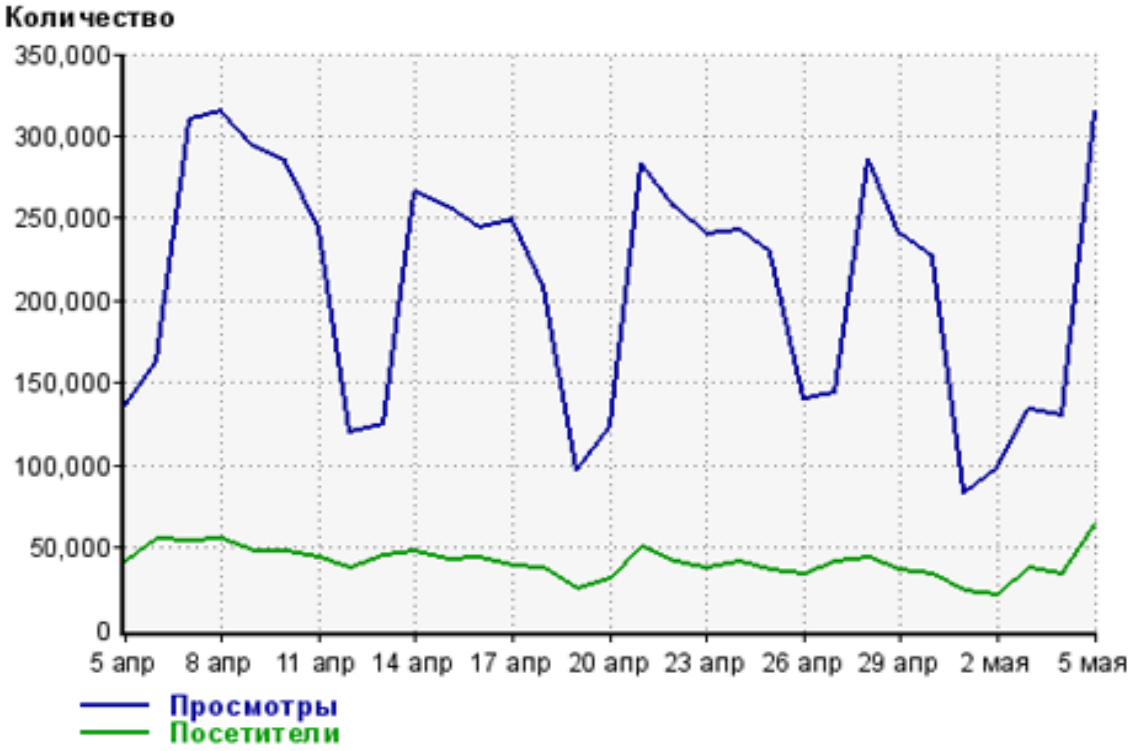


Рисунок 5. Месячный график посещаемости и просмотра страниц, сайта ИА «Амител» [55]

Если рассмотреть внутри суточное количество просмотров, то так же видно наличие сезонных периодов (рисунок 6). Количество просмотров минимально ночью, возрастает с началом рабочего дня (на графике указанно московское время, таким образом, начало активности в 5 часов утра, соответствует началу рабочего дня в Алтайском крае в 8 часов утра), и уменьшается к вечеру.

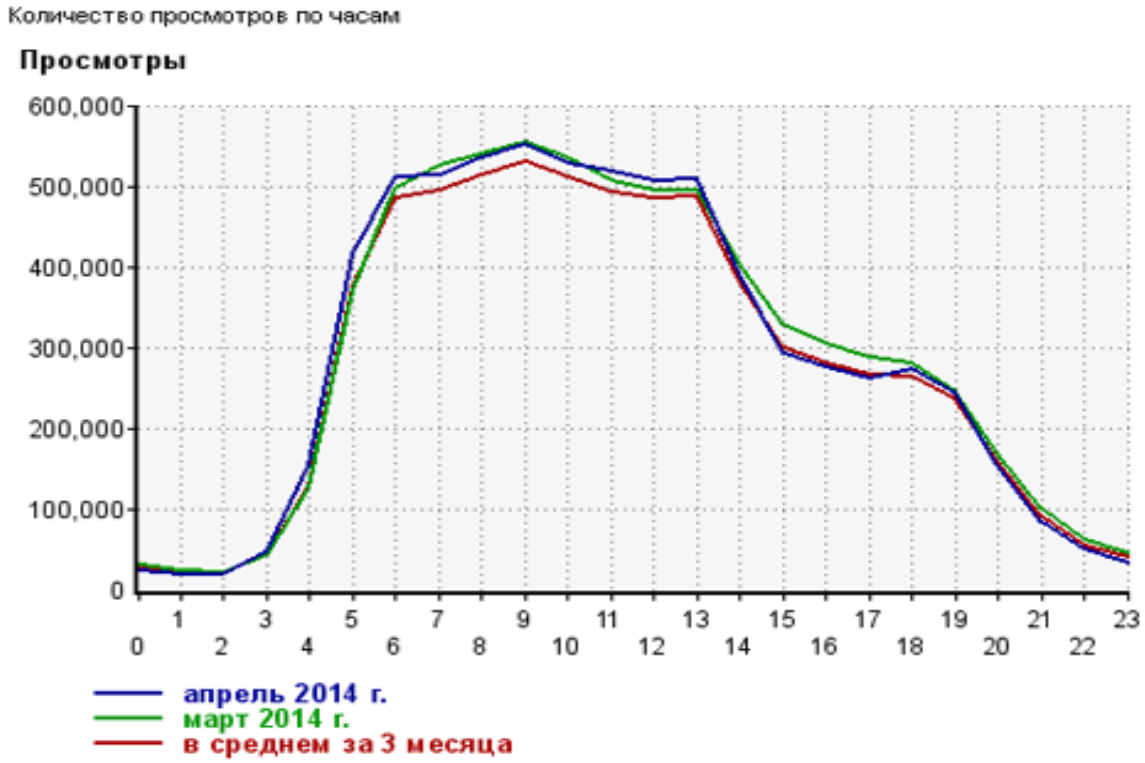


Рисунок 6. Количество просмотров страниц сайта ИА «Амител» по часам [55]

Аналогичная картина видна и на графике, характеризующем суточную активность пользователей за последние два месяца и в среднем за три месяца. Можно предположить, что наличие выраженных внутри суточных сезонных периодов связано с тем, что основной группой пользователей сайта, являются пользователи, проживающие в одном регионе и, соответственно, в одном часовом поясе. Действительно, на следующих изображениях (рисунки 7,8) видно, что основными пользователями сайта являются посетители Российской федерации. Среди которых, преобладают посетители из Барнаула и Новосибирска, проживающие в одном часовом поясе.

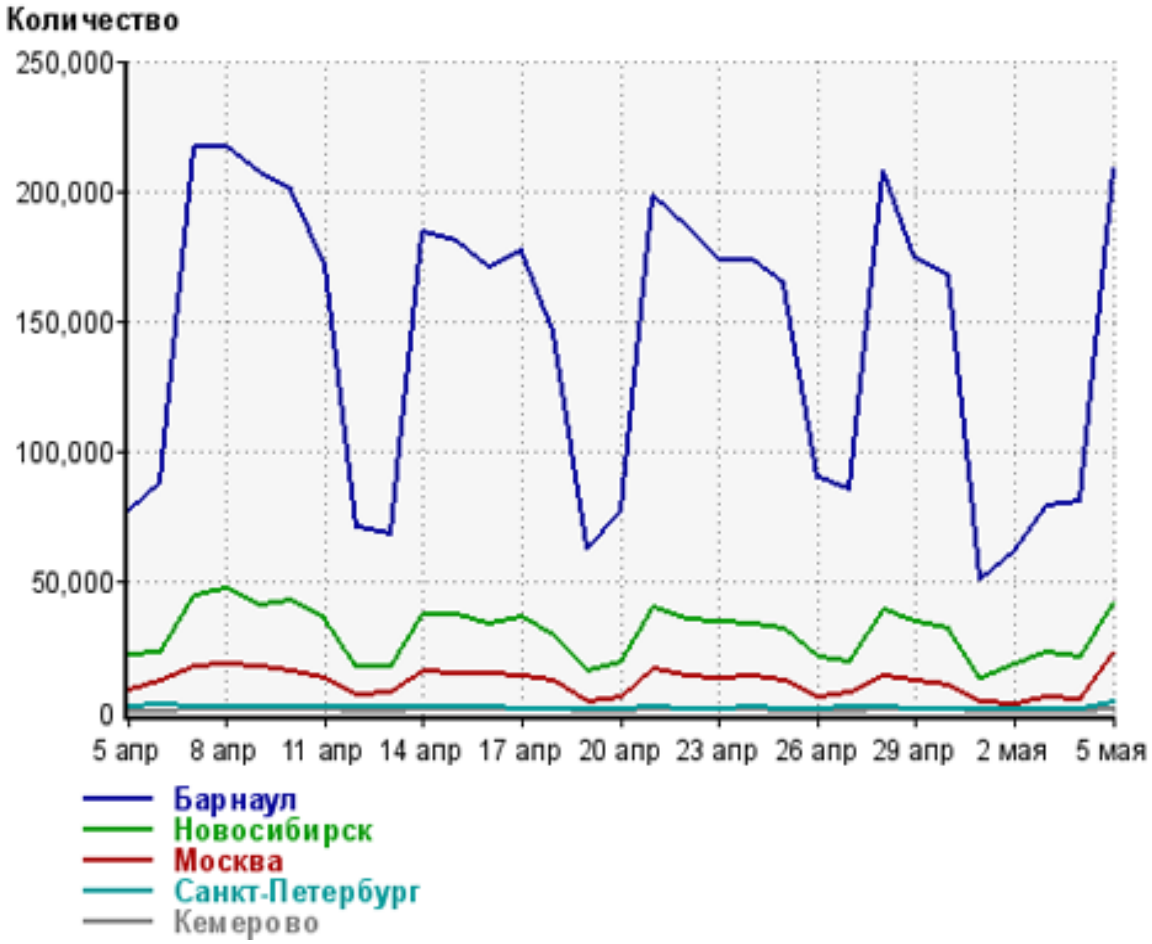


Рисунок 7. Количество просмотров страниц сайта ИА «Амител» по городам и регионам России [52]

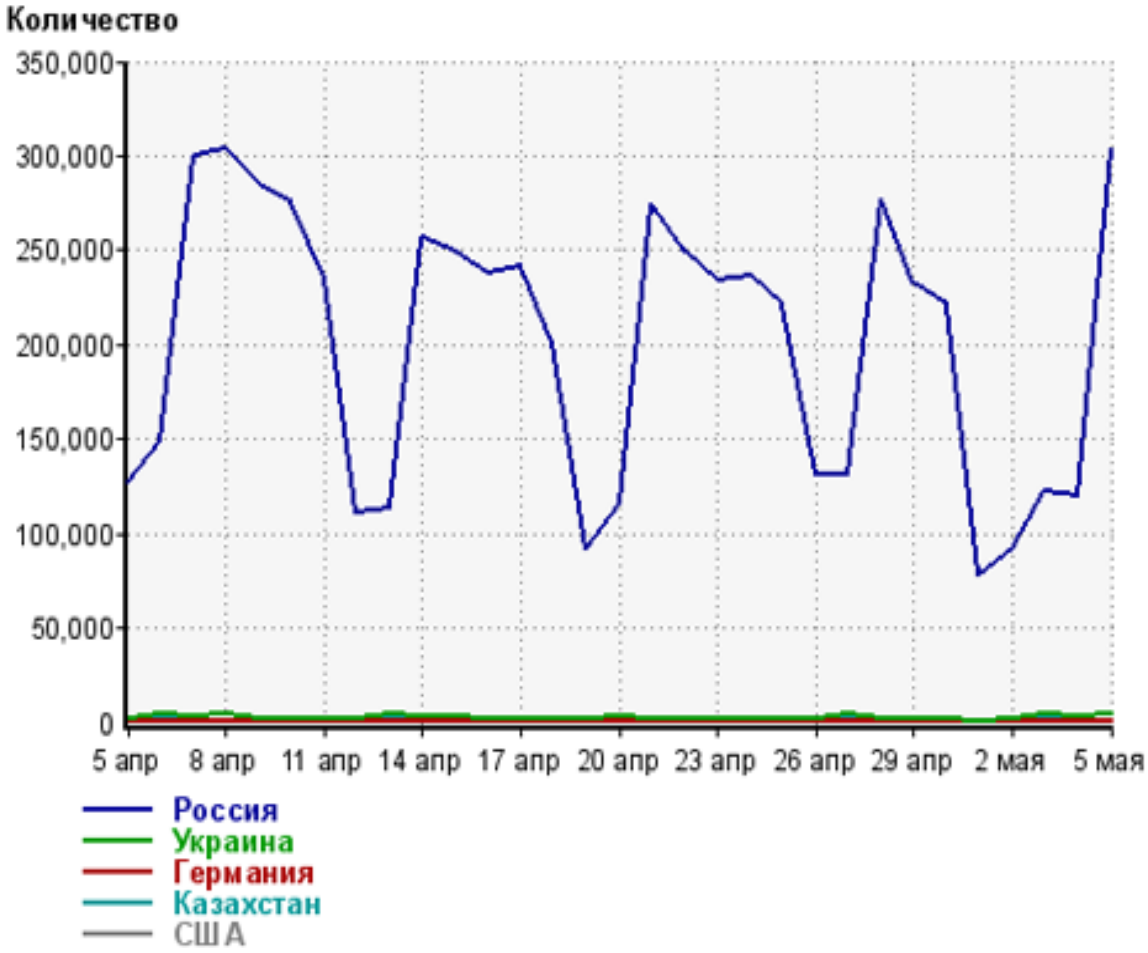


Рисунок 8. Количество просмотров страниц сайта ИА «Амител» по странам [55]

Так же можно предположить, что сайт, основные пользователи которого проживают в разных часовых поясах, например, в разных регионах или даже странах, может не имеет выраженных суточных периодов в работе.

Ярким примером такого высоко популярного сайта может быть развлекательный портал «Я плакалъ» (сайт http://www.yaplakal.com/), имеющий достаточно большую популярность на пост советском пространстве. На графиках, характеризующих его посещаемость, видно, что основными посетителями являются пользователи не только Российской федерации, но и пользователи из Украины, Беларуси, Казахстана (рисунок 9, 10). Если же рассматривать только Российскую федерацию, то среди её посетителей так же присутствуют пользователи из различных её регионов.

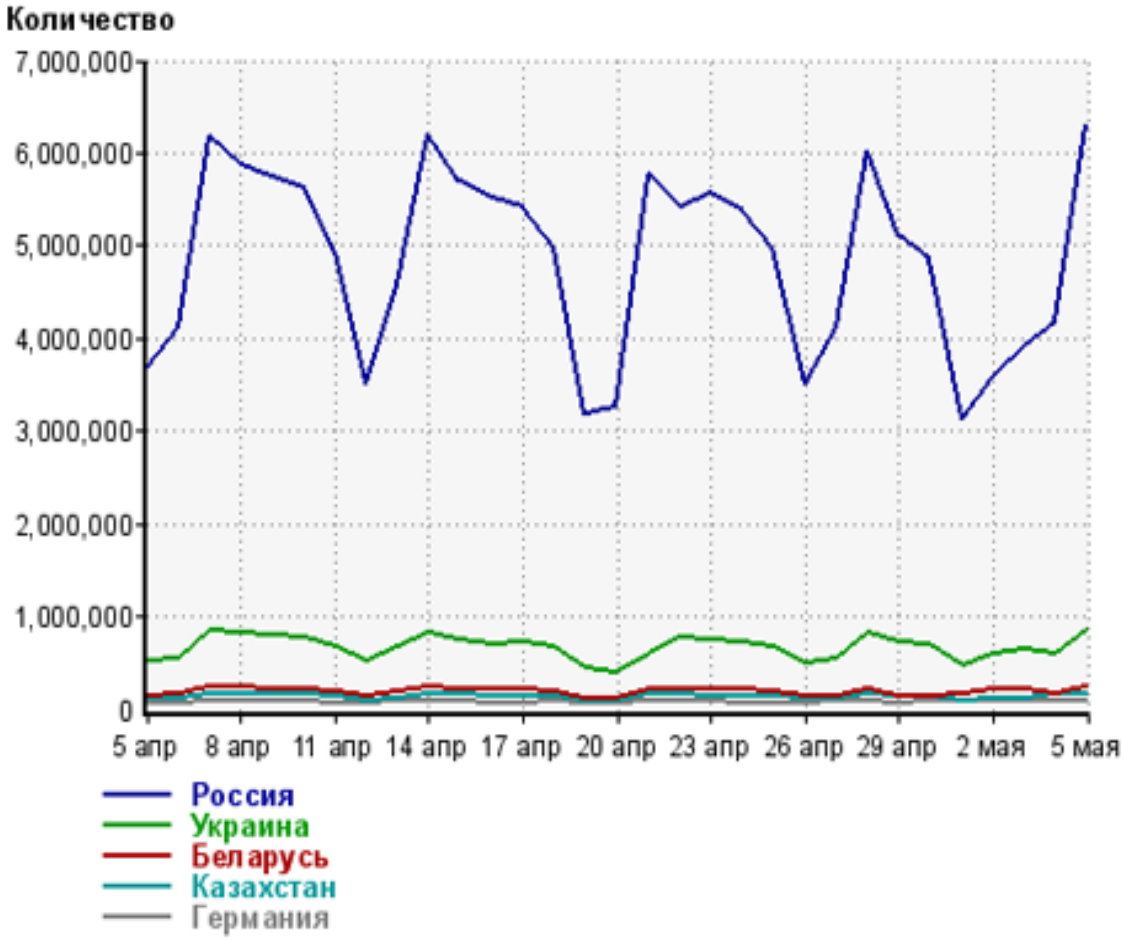


Рисунок 9. Месячный график просмотра страниц сайта «Я плакалъ» по странам мира [56]

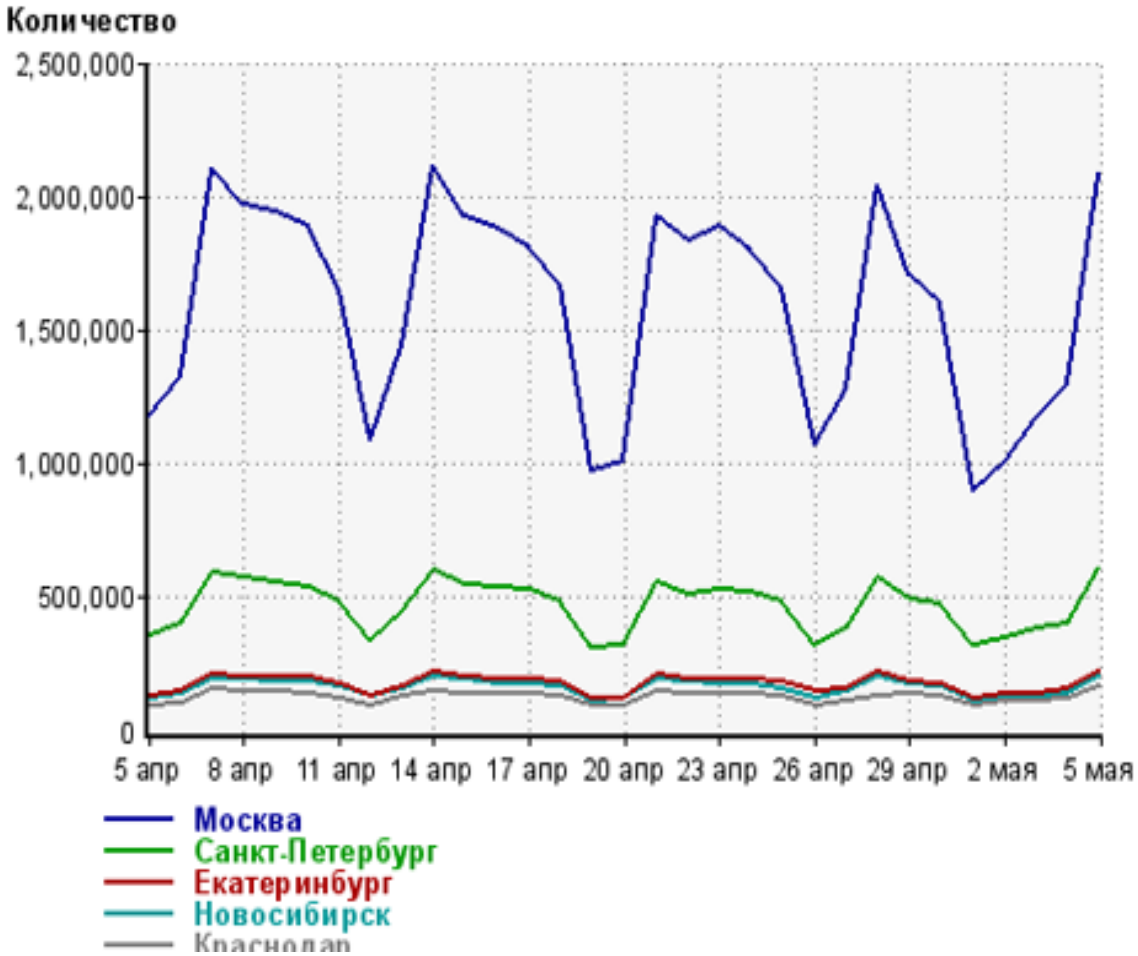


Рисунок 10. Месячный график просмотра страниц сайта «Я плакалъ» по городам и регионам России[56]

На этих графиках отчетливо видно недельную сезонности, которая присуща всем посетителям не зависимо от их региона. Действительно, если обратиться к общему графику посетителей и просмотров, так же видно наличие недельной сезонности (рисунок 11).

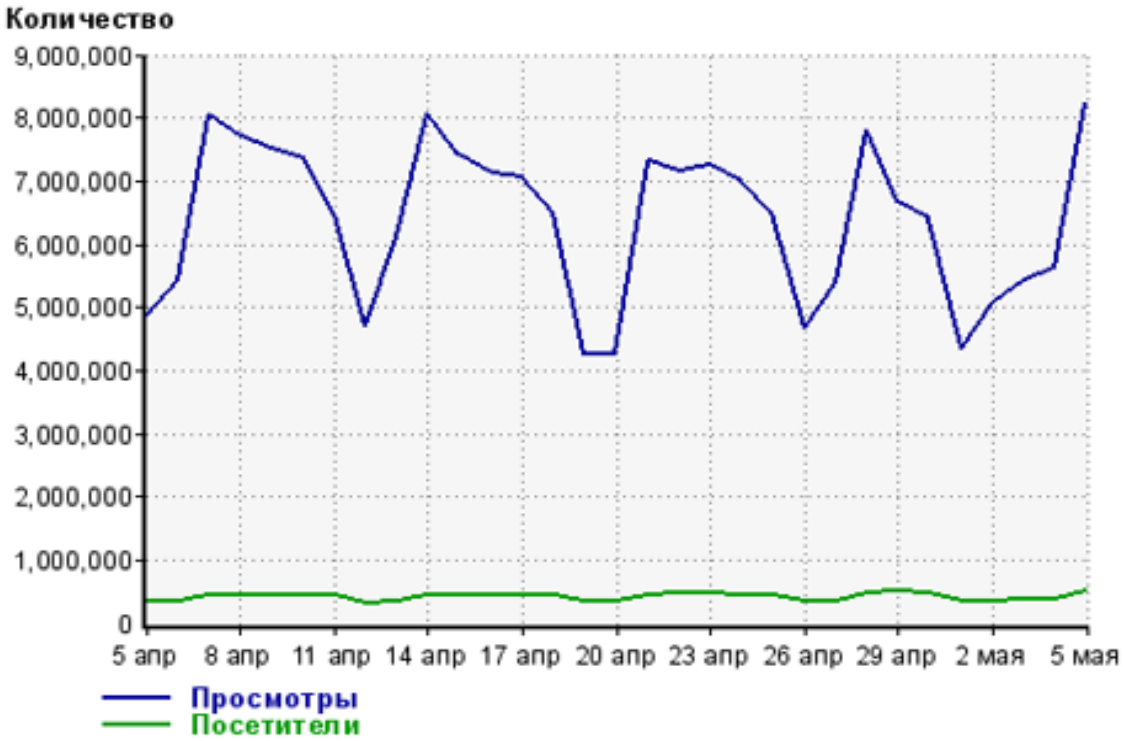


Рисунок 11. Месячный график количества посетителей и просмотра страниц сайта «Я плакалъ» [56]

При этом разброс пользователей по различным часовым поясам не повлиял на наличие внутри суточной сезонности. На следующих графиках отчетливо видно внутри суточные сезонные периоды (рисунки 12, 13). Которые являются сложными сезонными периодами, складывающимися из более простых сезонных периодов. Например, из времени рабочего дня определенного региона пользователей. Об этом свидетельствуют, например, небольшой спад количества просмотров в 18 часов и их рост к 21 часу.

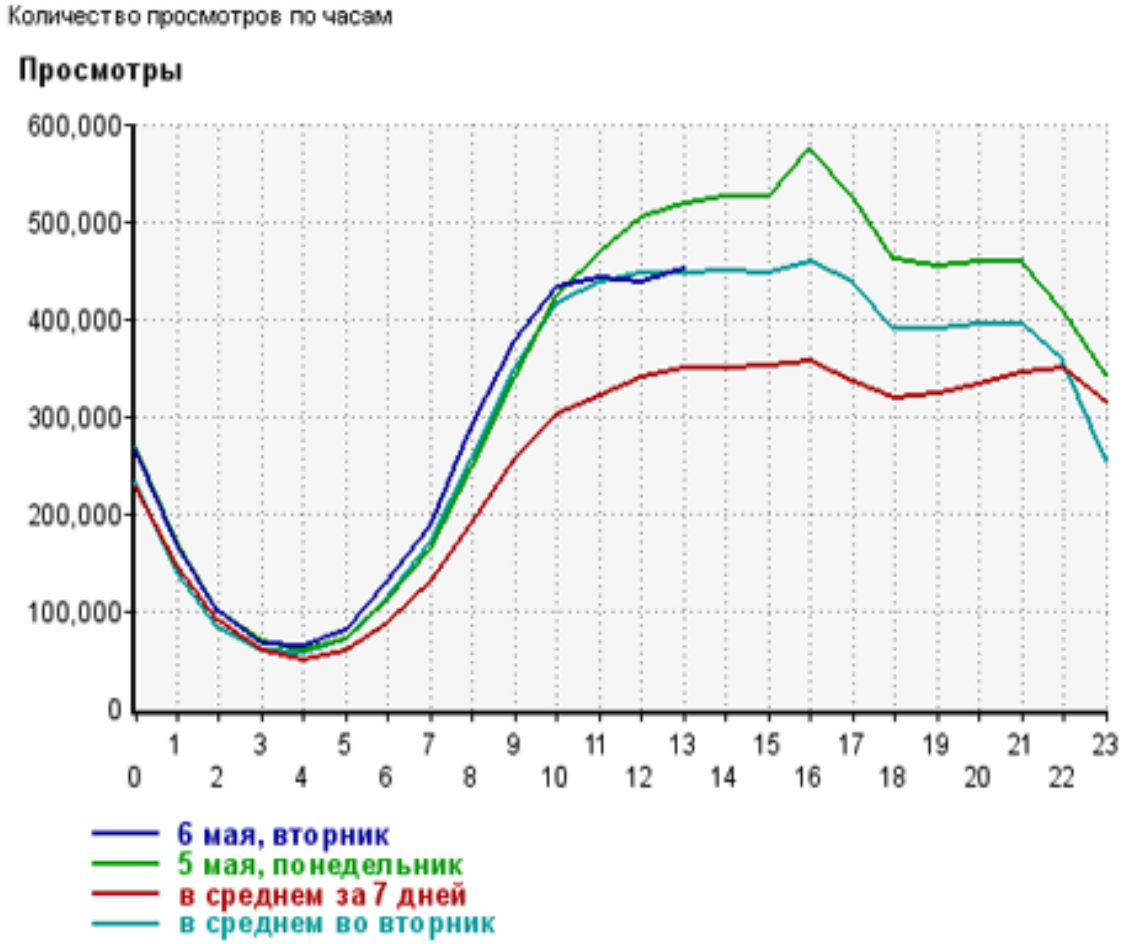


Рисунок 12. Количество просмотров страниц сайта «Я плакалъ» по часам [56]

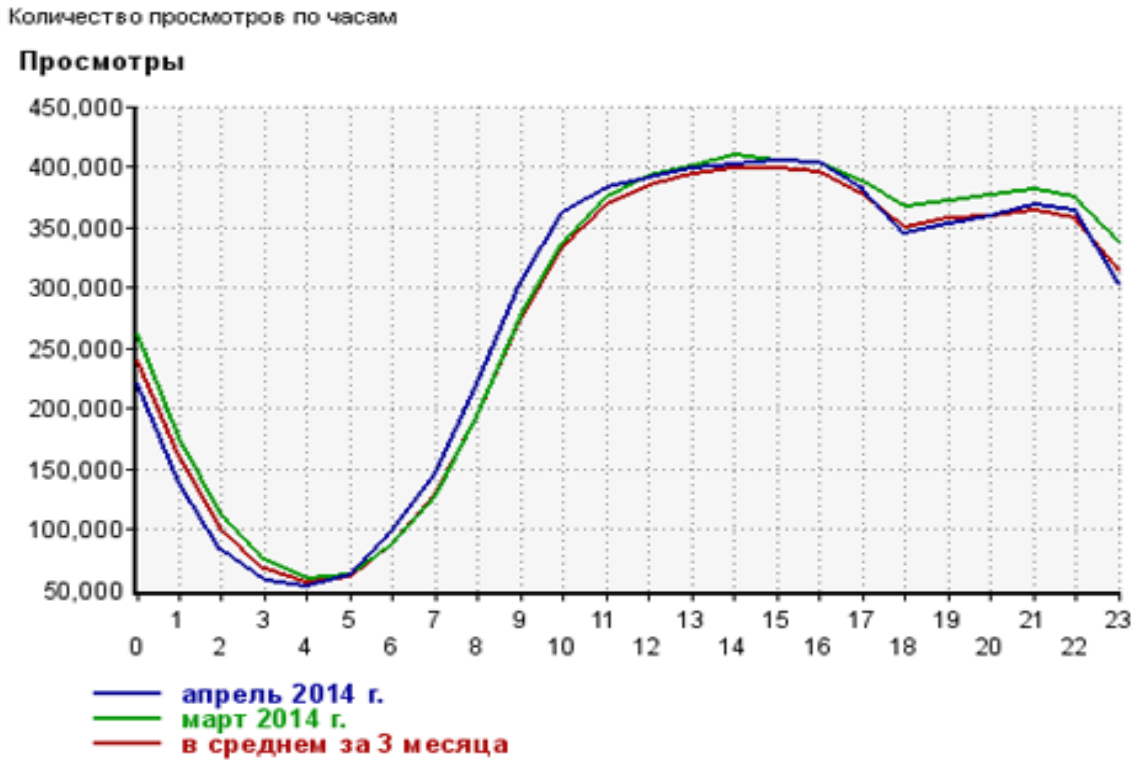


Рисунок 13. Количество просмотров страниц сайта «Я плакалъ» по часам [56]

Очевидно, что сезонные периоды образуются благодаря спросу, который проявляют пользователи того или иного ресурса. Если ресурс предоставляет новую информацию для пользователей только во время рабочей недели, периодическое снижение просмотров на выходных будет вполне очевидным. Аналогичная ситуация будет возникать и в том случае, если в какой-то из дней у пользователей ограничен доступ к ресурсам. Например, в результате исследования были обнаружены сайты, публикующие новую информацию круглосуточно семь дней в неделю, но при этом так же имеющие сезонные периоды, соответствующие неделям. При подробном рассмотрении данной ситуации было установлено, что основными посетителями таких сайтов являются сотрудники офисов, получающие к ним доступ с рабочих мест. При этом могут существовать сайты, пользователи которых проявляют активность всю неделю, не зависимо от будних и выходных дней. Это могут быть сайты социальных сетей или сервисы обмена сообщениями. Так, например, самый популярный ресурс, по версии сервиса статистики liveinternet.ru [57], – социальная сеть «В контакте» - не имеет ярко выраженных недельных периодов (рисунок 14). Но при этом совершенно четко прослеживается внутри суточная сезонность в работе данного ресурса (рисунок 15). Природу возникновения данных периодов можно объяснить временем сна и бодрствования пользователей.

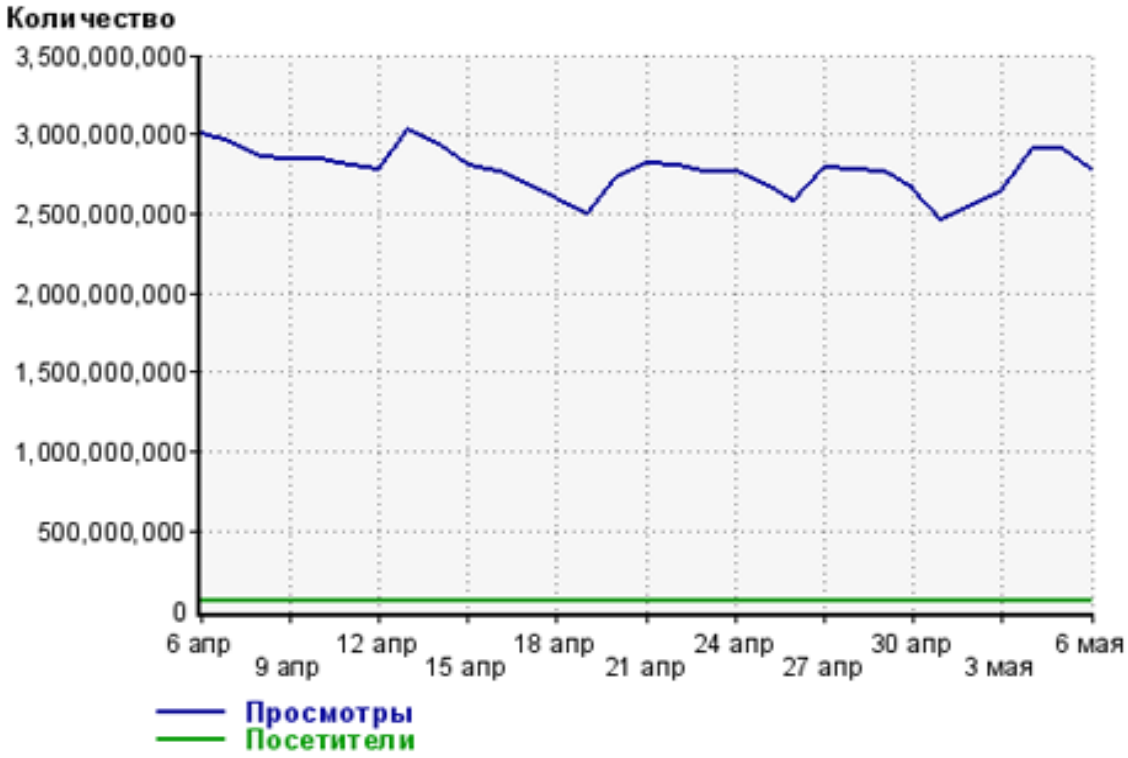


Рисунок 14. Количество посетителей и просмотров страниц социальной сети «ВКонтакте» за месяц [58]

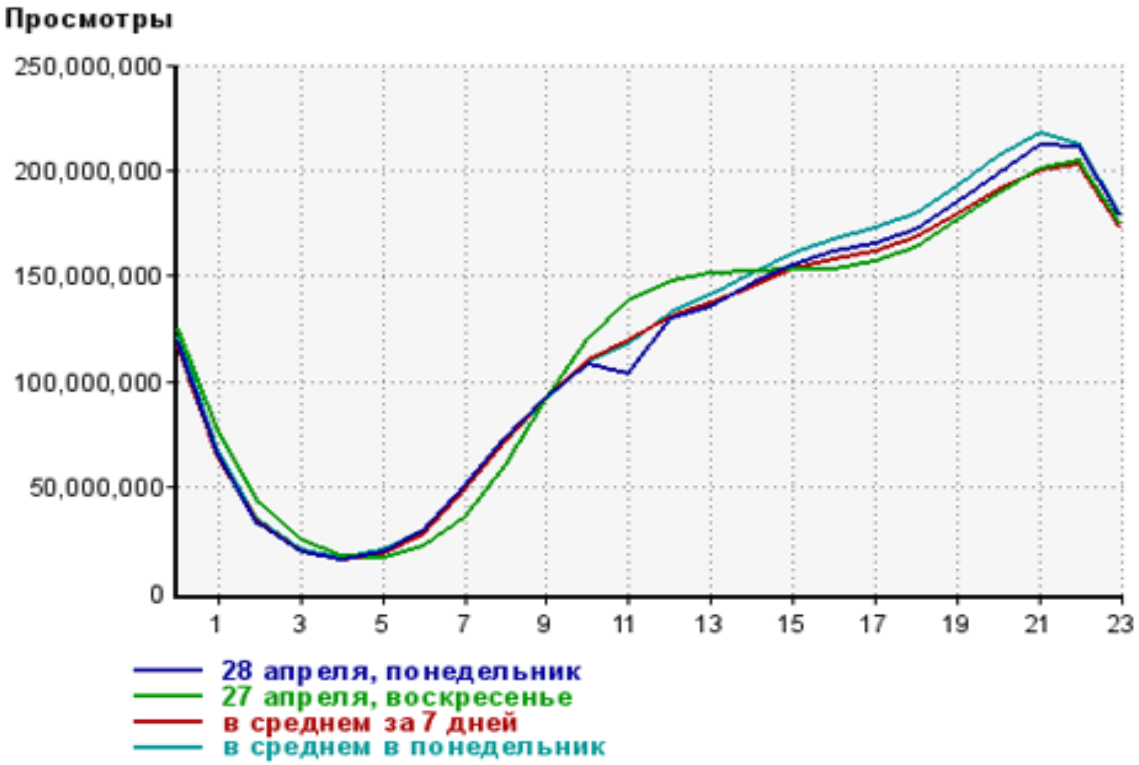


Рисунок 15. Количество просмотров страниц социальной сети «ВКонтакте» по часам [58]

Таким образом, на основании проведенных исследований можно с высокой степенью достоверности говорить о существовании сезонности в работе web-сайтов различных уровней. Так же в результате исследований не было обнаружено всплесков обращений к сайтам, которые бы могли нарушить существующие сезонные периоды. Например, если вернуться к рассматриваемому выше сайту amic.ru и проанализировать график перехода посетителей с других сайтов (рисунок 16), можно увидеть, что 5 мая с сайта news.yandex.ru на целевой сайт перешло около 15 тыс. посетителей.

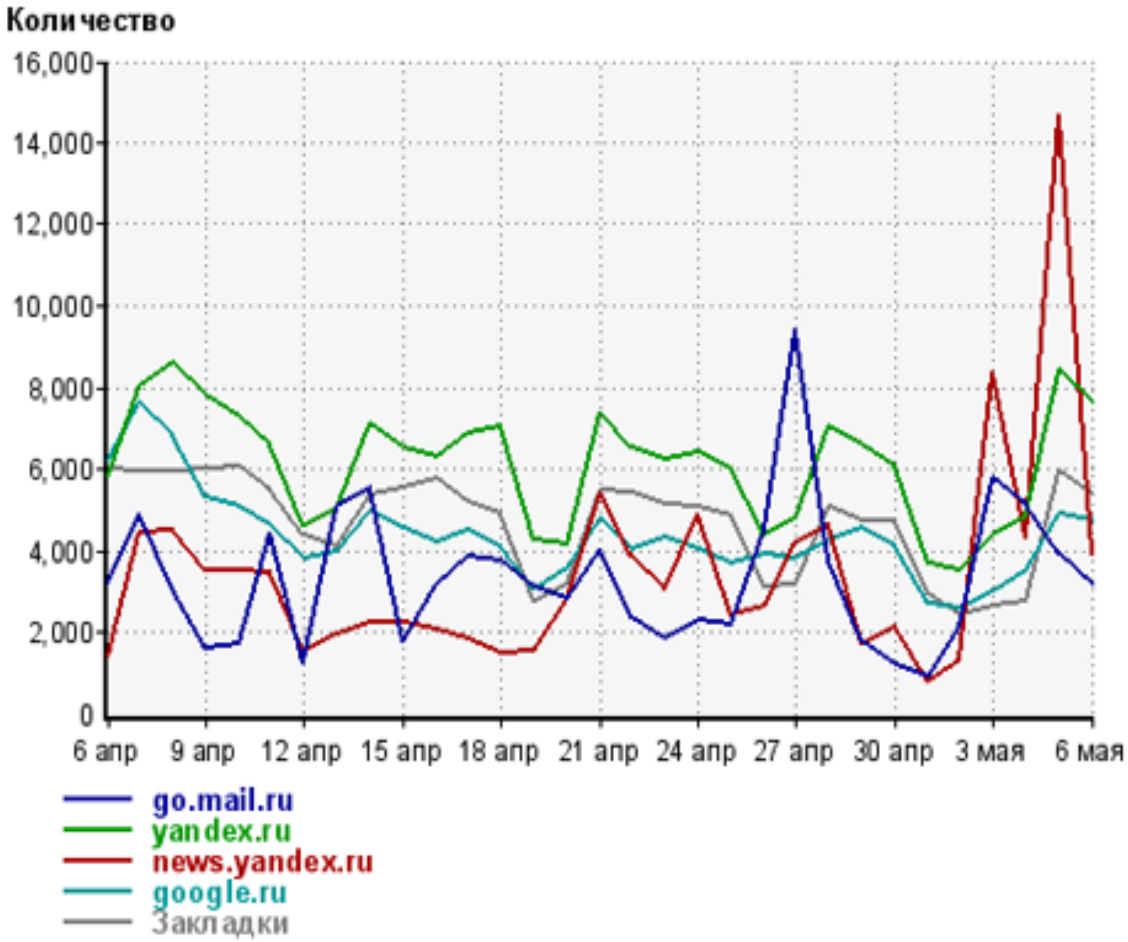


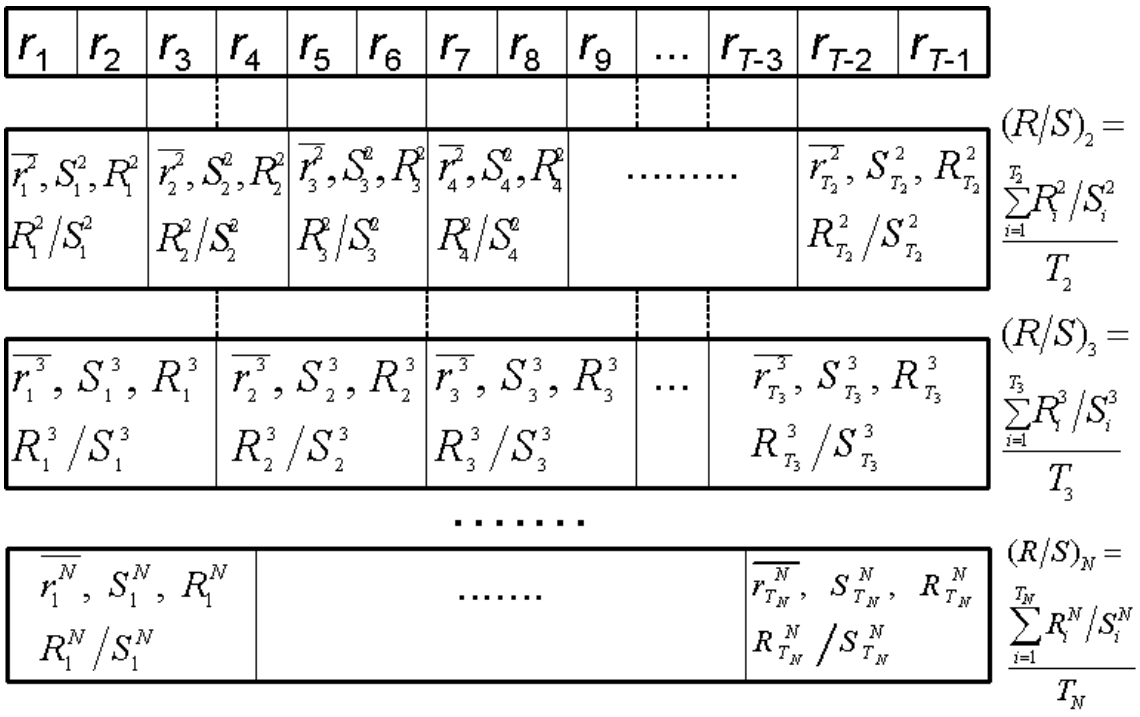
Рисунок 16. Количество переходов на сайт ИА «Амител» с сайтов, основных источников трафика [55]

Данный всплеск, по-видимому, вызвала публикации ссылки на целевой сайт с сайта news.yandex.ru. Потенциально данная ситуация может быть расценена как начавшаяся DDoS-атака. Однако, как видно на приведенных выше графиках месячной и суточной посещаемости и просмотров, в целом

по сайту даже такой мощный всплеск не нарушает верхнюю границу актуального сезонного периода. Данная ситуация является вполне понятной. Существует зависимость между авторитетом и посещаемостью сайта донора и целевого сайта. Крупные сайты доноры в большинстве случаев не будут рекомендовать просмотреть небольшие менее популярные сайты. Те же сайты, которые они рекомендуют, имеют, как правило, такое количество посещений, при котором вновь поступивший трафик не будет являться значительным. Хотя потенциально ситуация, когда на web-сайт может поступить трафик из других источников, сопоставимый с его посещаемостью, возможна. В этом случае предложенная методика зафиксирует начавшуюся DDoS-атаку. Однако, как было установлено в процессе исследований, такая ситуация маловероятна и может быть обработана системным администраторам или операторам, отвечающим за безопасность, в ручном режиме.

2.2.3. Формальное описание сезонности

Для формального описания и математического обоснования выбора актуальных сезонных периодов был применен метод Херста [95]. Впервые метод был применен Херстом при проектировании плотины, для определения сезонных периодов разлива Нила. Метод отличается минимальными требованиями к вычислительным ресурсам.



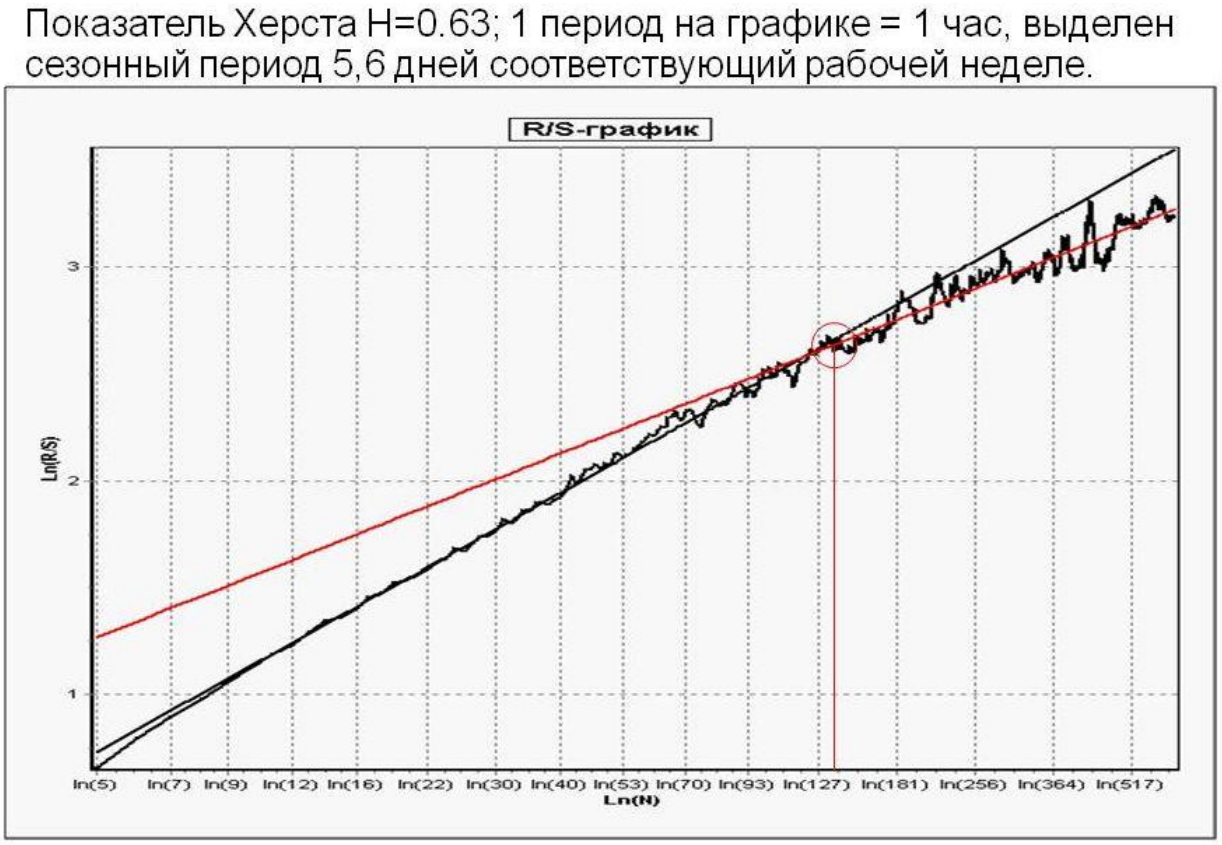
(2)

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 $Ln(n)$.График линейно аппроксимируется.

Коэффициент наклона кривой даёт оценку показателя Херста(H).



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

2.2.4. Выбор и обоснование метода кластеризации

Пусть множество T – это множество клиентских запросов, поступивших до начала атаки. Множество клиентских запросов, поступающих после начала атаки, – это объединение множеств H – вредоносных клиентских запросов и множества T^* – благонадежных клиентских запросов. Таким образом, для получения выборки, характеризующей вредоносный трафик необходимо будет разделить трафик, получаемый после начала атаки, на две группы.

Так как число кластеров заранее известно, в качестве гипотезы можно предположить, что оптимальным будет использование алгоритма k-means [59]. Однако, использование данного алгоритма будет затруднительно при обработке больших данных и потребует дополнительных ресурсов. Если учитывать, что данный метод будет использоваться в рамках атакуемого

сервера, который уже испытывает недостаток в вычислительных ресурсах, то процесс кластеризации данным методом может быть невыполним. Также особенностью данного алгоритма являются чувствительность к выбросам, которые могут искажать среднее. И хотя при исследовании сезонности было установлено крайне редкое появление крупных выбросов, их потенциальное наличие может отрицательно сказаться на результатах как кластеризации, так и работы алгоритма в целом.

Для решения проблемы, связанной с выбросами, лучшие результаты может дать модификация алгоритма k-средних, алгоритмом k-медианы (k-medoids). Алгоритм менее чувствителен к шумам и выбросам данных, чем алгоритм k-means, поскольку медиана меньше подвержена влияниям выбросов. Но при этом алгоритм не эффективен при обработке больших данных [59].

Преодолеть все указанные выше трудности может алгоритм CLARA (Clustering LARge Applications), который был разработан Kaufmann и Rousseeuw в 1990 году для кластеризации данных в больших базах данных. Алгоритм CLARA извлекает множество образцов из базы данных. Кластеризация применяется к каждому из образцов, на выходе алгоритма предлагается лучшая кластеризация. Для больших баз данных этот алгоритм эффективнее, чем алгоритм PAM. Однако, эффективность алгоритма зависит от выбранного в качестве образца набора данных, оптимальный выбор которого в ситуации постоянно меняющейся сетевой картины может быть затруднен.

С целью выбора оптимального алгоритма кластеризации, также были рассмотрены новые, перспективные методы кластеризации. Это методы Clarans, CURE, DBScan и метод WaveCluster [60].

Метод WaveClaster показывает хорошую эффективность при анализе небольших данных, алгоритм не чувствителен к шумам и может строить кластеры произвольной формы. Но при увеличении размерности данных его эффективность резко снижается.

Методы Clarans, CURE, DBScan хотя и предназначены для обработки сверхбольших данных, для решения текущей задачи оказались неэффективны. Так как суть этих методов – начальная установка определенной плотности точек, для оптимизации работы с большими данными не может быть эффективно выполнена в контексте текущей задачи.

По итогам рассмотрения представленных выше методов кластеризации, был выбран метод k-means. Данный методы был исследован на предмет эффективности для решения текущей задачи кластеризации. Исследование проходило с помощью статистического пакета IBM SPSS Statistics версия 21 [61]. В качестве данных для анализа использовались 12-мерный массив данных, полученный из log-файла web-сервера Apache, соответствующих реальным DDoS-атакам. Подробнее о структуре данного файла будет рассказано в главе, посвященной апробации методики и разработанного программного средства. Предварительно, для подтверждения гипотезы о существовании двух кластеров была создана визуализация имеющихся данных. Визуализация представляет собой двухмерную диаграмму рассеивания. Снижение размерности было проведено с помощью метода главных компонент. Диаграмма подтверждает гипотезу о существовании двух кластеров.

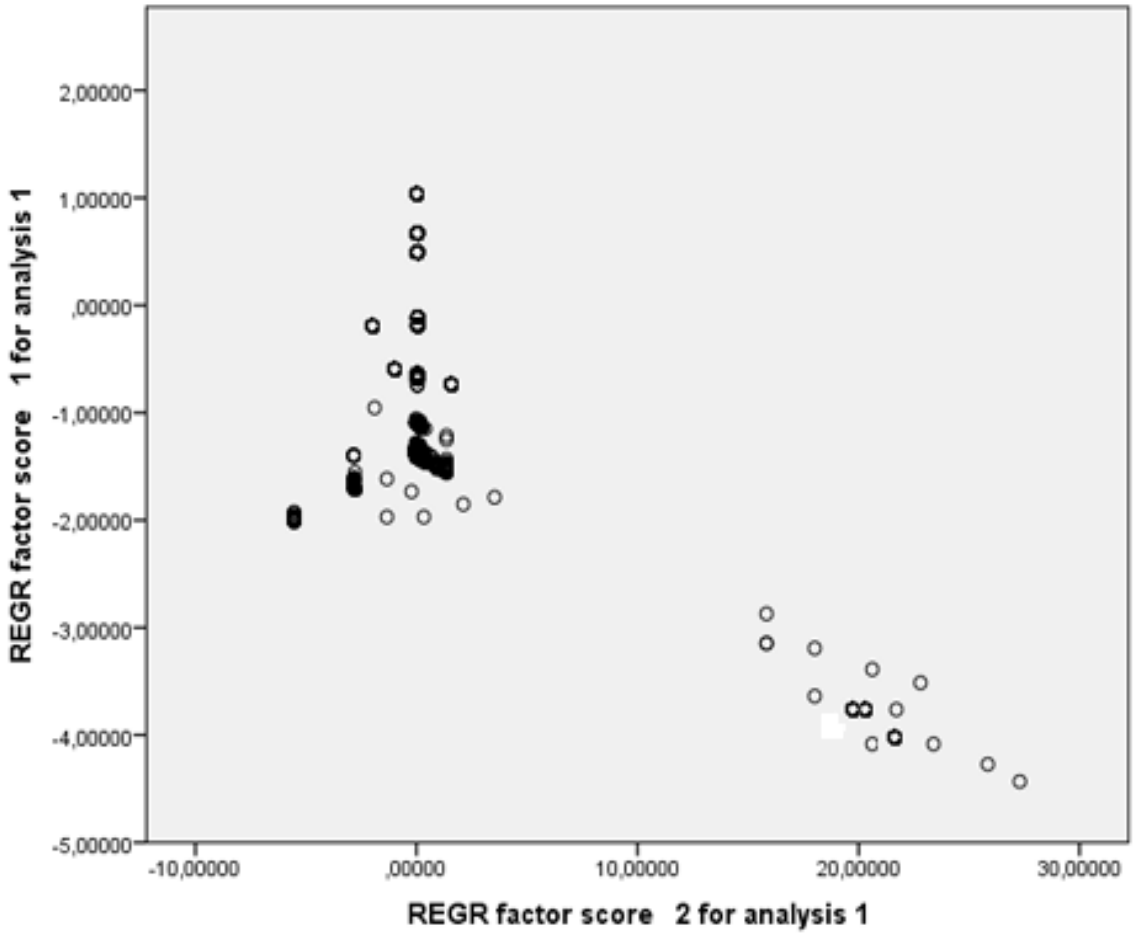


Рисунок 17. Визуализация данных по двум компонентам

Следующим шагом исследования стал выбор оптимальных признаков для проведения кластеризации. Для выбора оптимальных параметров использовалась модель эксперимента, предложенная в статье «Оценка информативного признакового пространства для системы обнаружения вторжений» [62]. В результате экспериментов было установлено, что наибольшую эффективность при кластеризации обеспечивает учет следующих признаков:

- Источник запросов
- Скорость поступления запросов
- Страница назначения запроса
- Загружаемые данные
- Браузер клиента
- Операционная система клиента

- Объем переданных данных
- Объем полученных данных

В целом, выбранные признаки, а также их количество соответствуют результатам, полученным в аналогичных исследования [62-64].

Сокращение размерности исходного массива данных, позволило увеличить скорость кластеризации. Следующим вопросом стал выбор оптимального количества данных для анализа. Ввиду того, что данные для анализа извлекаются из лог-файла, и одному клиентскому запросу может соответствовать несколько записей из этого файла, (при обращении к одной странице могу загружаться различные изображения, файлы каскадных таблиц стилей скриптов и т.д.), указать точный размер данных (в количестве строк), оптимальных для анализа, не представляется возможным. В связи с этим оптимальный размер данных указывается в количестве периодов. Оптимальное количество периодов для расчета среднеквадратичного отклонения равно 22. При уменьшении этого значения возможны ложные срабатывания, при увеличении может происходить незначительный рост точности, который при дальнейшем увеличении количества периодов, как правило, сменяется спадом, вследствие уменьшения чувствительности.

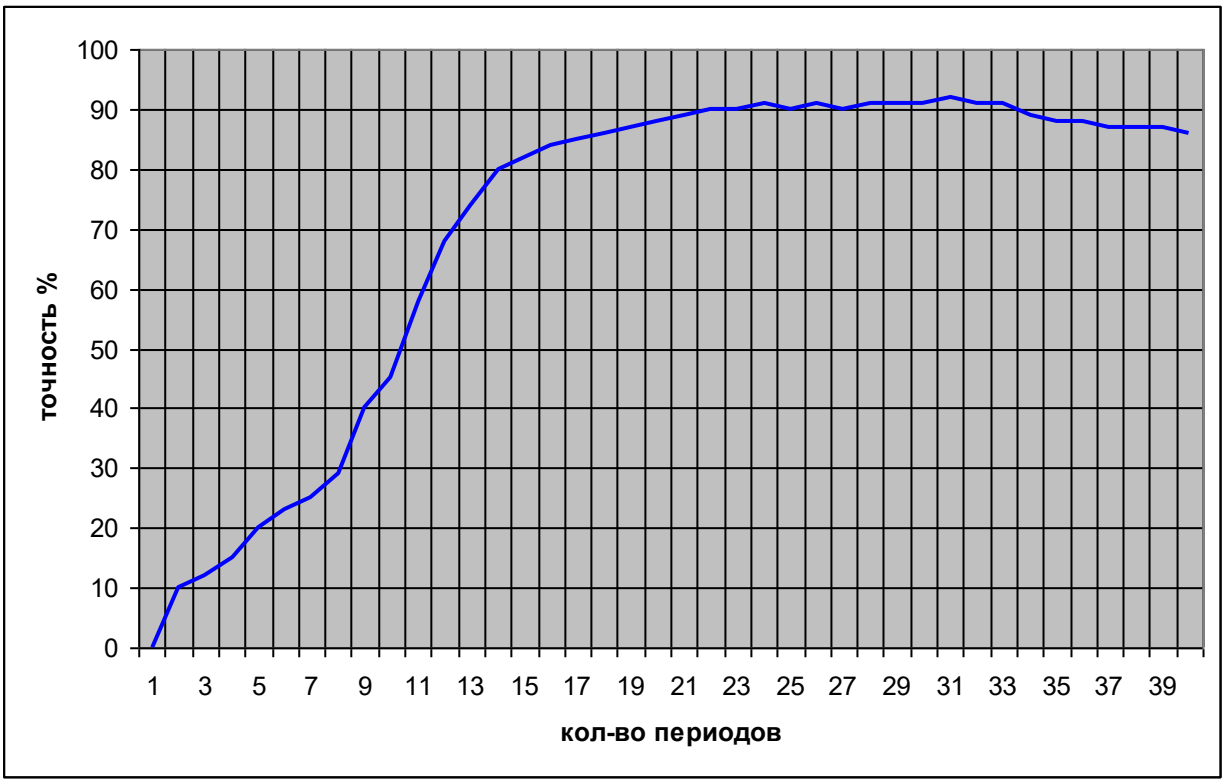


Рисунок 18. График зависимости точности определения начала атаки от количества рассматриваемых периодов

В результате исследования выбранный метод показал свою высокую эффективность. Метод обеспечивает приемлемую точность, минимальную нагрузку и оптимальную скорость работы.

2.2.5. Первичная кластеризация на основе алгоритма k-means

Для первичного разделения смешанного трафика на благонадежный и вредоносный оптимально воспользоваться алгоритмом кластеризации k-means [65]. Обоснование выбора данного алгоритма приведено выше. Данный алгоритм позволяет провести кластеризацию при заранее известном числе кластеров. Алгоритм обладает приемлемой точностью, необходимой для первичного разделения, и более высокой скоростью работы, по сравнению с другими алгоритмами. Суть алгоритма заключается в выделение двух кластеров и вычислении их центров масс, на последующих итерациях происходит коррекция кластеров (перенос элементов в

соответствии с рассчитанными центрами масс) и перевычисление центров масс.

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

где k — число кластеров; S_i — полученные кластеры; $i = 1, 2, \ldots, k$и μ_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. Соответствующая, благонадежному трафику, предшествующему началу атаки – T.
2. Соответствующая, благонадежному трафику, выделенная из смешенной – T^*.
3. Соответствующая вредоносному трафику, выделенная из смешенной – H.

2.2.6. Критерии успешности, коррекция полученных кластеров

Для оценки эффективности кластеризации рассмотрим уравнение стационарных вероятностей [96]:

$$\begin{aligned}
&p_0\lambda = p_1\mu, \\
&(\lambda + i\mu)p_i = \lambda p_{i-1} + (i+1)\mu p_{i+1}, i = 1 \ldots K-2, \\
&(\lambda + (K-1)\mu)p_{K-1} = \lambda p_{K-2} + K\tilde{N}\mu p_K, \\
&(\lambda^* + K\tilde{N}\mu)p_K = \lambda p_{K-1} + K\tilde{N}\mu p_{K+1}, \\
&(\lambda^* + i\mu^*)p_i = \lambda^* p_{i-1} + (i+1)\mu^* p_{i+1}, i = K+1 \ldots N-1.
\end{aligned} \tag{4}$$

где,

λ – интенсивность нагрузки;

λ_L – интенсивность нагрузки, создаваемая легальными пользователями;

S – интенсивность вредоносного трафика;

μ – интенсивность освобождения очереди запросов;

μ^* – интенсивность освобождения очереди запросов при активированном фильтре;

E_1, E_2 – ошибки первого и второго рода;

K – граница активации фильтра;

N – объем очереди запросов;

$\lambda = \lambda_L + S$ – нагрузка в момент атаки;

$\lambda^* = \lambda_L + S(1-E_2)$ – нагрузка при активированном фильтре;

Так как проверка запроса снижает производительность сервера, в некоторых случаях интенсивность освобождения очереди запросов, можно оценить как $Z\mu$, где,

Z – коэффициент замедления;

При нормировании $\sum_{i=1}^{N} p_i = 1,$ получим вероятность блокировки запроса

$$p_{BLK} = \frac{\frac{1}{N!}\left(\frac{\lambda}{\mu}\right)^{K-1}\frac{\lambda}{\mu^*}\left(\frac{\lambda^*}{\mu^*}\right)^{N-K}}{\sum_{i=0}^{K-1}\frac{\left(\frac{\lambda}{\mu}\right)^{i}}{i!} + \sum_{i=K}^{N}\frac{1}{i!}\left(\frac{\lambda}{\mu}\right)^{K-1}\frac{\lambda}{\mu^*}\left(\frac{\lambda^*}{\mu^*}\right)^{i-K}}. \quad (5)$$

Таким образом, эффективность разделения вредоносного и благонадежного трафика можно оценить, как $R = (1-E_1)(1-p_B).$ [96].

На основании полученной оценки, были выработаны критерии успешности.

На следующем шаге алгоритма проводится коррекция полученных выборок с учетом этих критериев:

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. Иными словами, расстояние между этими центрами масс должно стремиться к нулю.

Для дальнейшего уточнения можно рассчитать вероятность принадлежности каждого элемента своему классу. Элементы с наименьшей вероятностью переносятся в противоположные группы с учетом критерия размерности групп.

Для расчета схожести благонадежных кластеров и в дальнейшем для классификации вновь приходящих запросов можно воспользоваться «наивным Байесовким классификатором» [66]. В качестве вероятностной модели для классификатора используем условную вероятность $p(C|F_1,\ldots,F_n)$ над зависимой переменной класса C с малым количеством результатов или *классов*, зависящая от нескольких переменных $F_1\ldots F_n$. Используя теорему Байеса, запишем:

$$p(C|F_1,\ldots,F_n) = \frac{p(C)\ p(F_1,\ldots,F_n|C)}{p(F_1,\ldots,F_n)}.$$

Условное распределение по классовой переменной C может быть выражено так:

$$p(C|F_1,\ldots,F_n) = \frac{1}{Z}p(C)\prod_{i=1}^{n} p(F_i|C)$$

Таким образом, для классификации трафика по двум классам имеем:

$P(T \mid D) = \frac{P(T)}{P(D)} \prod_{i=1}^{n} P(w_i \mid T)$ – для класса благонадежных пользователей;

$P(H \mid D) = \frac{P(H)}{P(D)} \prod_{i=1}^{n} P(w_i \mid H)$ – для класса неблагонадежных пользователей.

В качестве обучающих выборок используются множество T и множество H. По завершении этого шага элементы из множества T*, отнесенные к группе вредоносного трафика, меняются местами с элементами множества H с учетом указанных выше критериев.

Этот шаг повторяется до тех пор, пока все элементы множества T не будут помечены как благонадежные, либо пока алгоритм не достигнет порогового значения итераций.

Полученные выборки, соответствующие благонадежному и вредоносному трафику, а также механизм их поддержания в актуальном состоянии позволяют использовать их с различными классификаторами.

2.3. Блок-схема алгоритмов

Ниже показаны принципиальные схемы алгоритмов (Схема 1.) по определению начала атаки и выделению вредоносного трафика. Первая схема, поясняет алгоритм выделения вредоносного трафика, вторая и третья алгоритм определения начала атаки.

На первом шаге происходит вызов подпрограмм по выявлению сезонных периодов, расчету для них допустимой границы количества запросов, и определения начала атаки. В случае начала атаки, алгоритм проводит разделение смешанного трафика на два кластера, один содержащий вредоносные запросы, другой благонадежные запросы. Эти кластеры уточняются. Новые запросы анализируются на принадлежность тому или иному кластеру и по результату добавляются к соответствующему кластеру.

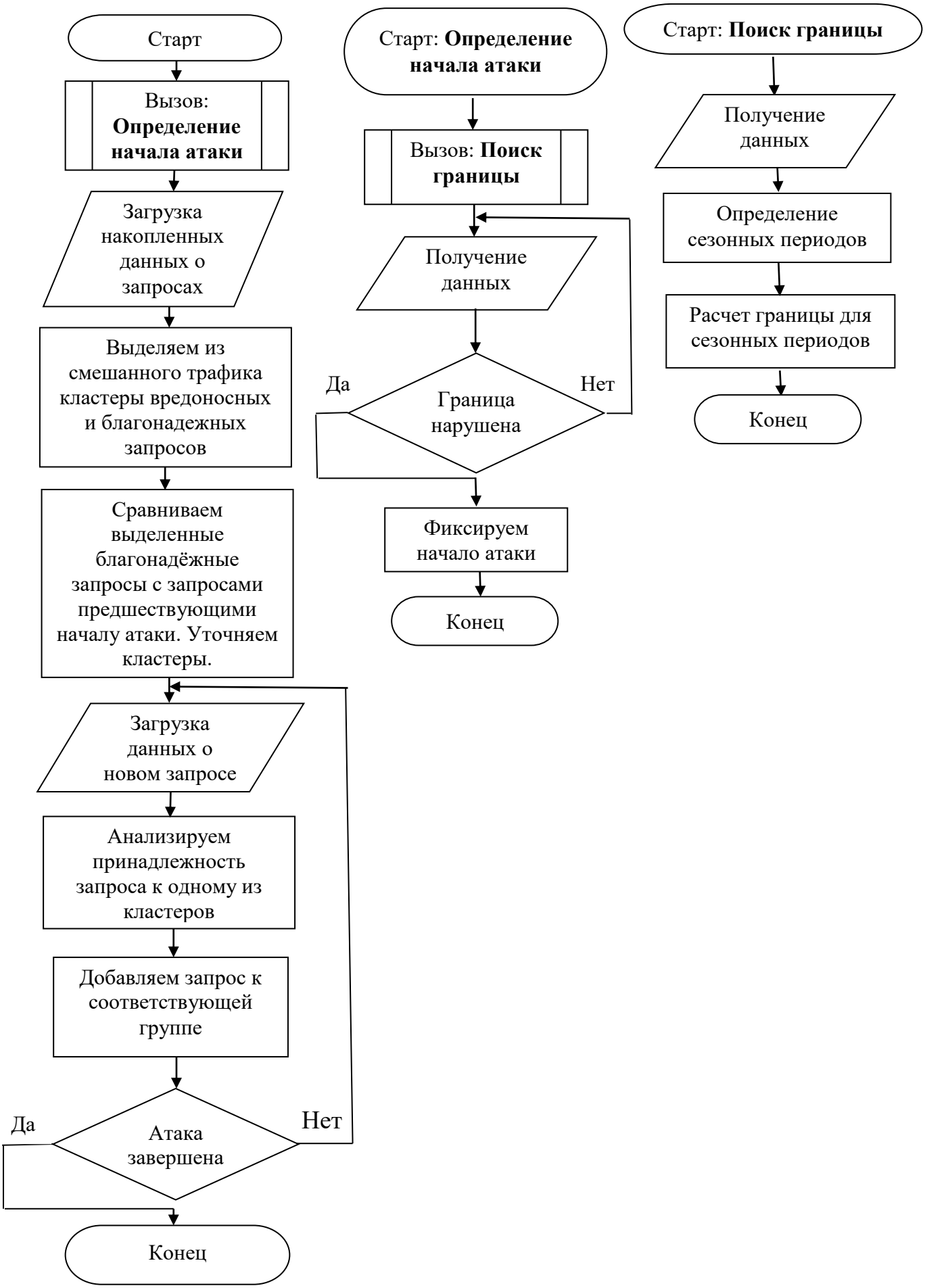


Схема 1. Принципиальная блок-схема алгоритма

2.4. Выводы по второй главе

Во второй главе в рамках разработки методики обнаружения DDoS-атак и вредоносного трафика разработан оригинальный алгоритм обнаружения на ранних стадиях точки начала распределенной атаки, направленной на отказ в обслуживании. Алгоритм учитывает сезонные отклонения в нагрузке, что дает возможность выявлять точку начала атаки на ранних стадиях и с большей точностью. Дополнительно проведено исследование, направленное на подтверждение существования сезонности и выявления типичных сезонных периодов. В результате этого исследования выявлены недельная, суточная и неопределенная сезонность и причины её возникновения.

Разработана методика получения обучающих выборок и классификации поступающего трафика на группы вредоносных и благонадежных запросов. Для разделения смешанного трафика используется алгоритм кластеризации k-means. Выбор данного алгоритма обоснован, проведено доказательство его эффективности. Для алгоритма подобранны оптимальные характеристики и размерность данных, выработаны критерии успешности.

Разработанные алгоритмы составляют основу обобщенной методики обнаружения DDoS-атак и вредоносного трафика, которая в общем виде может быть записана так:

1. С помощью накопленных статистических данных, определяем существующие сезонные периоды.
2. Для каждого сезонного периода определяем допустимую верхнюю границу количества запросов.
3. В случае нарушения границы, фиксируем точку начала атаки.
4. Относим весь, предшествующий началу атаки, трафик к кластеру, соответствующему благонадежному трафику.
5. С помощью алгоритма k-means классифицируем смешанный трафик на благонадежный и вредоносный.

6. Сравниваем трафик, предшествующий началу атаки, с кластером, благонадежного трафика, выделенного из смешанного трафика.
7. На основании результатов, полученных в предыдущем шаге, и с учетом выработанных критериев успешности, корректируем кластеры.
8. Весь поступающий трафик анализируем с учетом полученных в предыдущем пункте результатов.

Полученная методика протестирована на данных из набора KDD99. Для легитимных запросов полнота обнаружения составили 0,9991 при точности 0,9811, для вредоносных запросов, полнота 0,9975, точность 0,9924.

Глава 3. Разработка программного комплекса фильтрации трафика

3.1. Постановка задачи

Необходимо разработать программное средство для противодействия распределенным атакам, направленным на отказ в обслуживании. В основе разрабатываемого средства должны лежать алгоритм и методика, предложенные во второй главе.

В связи со значительным преобладанием среди DDoS-атак атак типа HTTP-flood, специализация разрабатываемого средства должна быть ориентирована на противодействия атакам этого типа.

На основании данных мониторинга, описанного в первой главе и свидетельствующего о наметившемся росте DDoS-атак средней и малой интенсивности, направленных на региональные ресурсы, и отсутствии средств противодействия, эффективных и актуальных для данных атак, целесообразно создаваемое средство адаптировать для решения указанных задач в контексте безопасности региональных ресурсов.

На сегодняшний день региональный web-ресурс – это:

1. Ресурс, расположенный на собственном выделенном сервере средней конфигурации или у одного из хостинг-провайдеров на тарифном плане среднего уровня.
2. Ресурс, использующий в качестве системы управления содержанием (CMS, content managment system) собственную CMS или свободно распростроняемую CMS с открытым исходным кодом.
3. Ресурс, ограниченный в материальных средствах.

На основании этих свойств можно выделить следующие трудности, возникающие при противодействии DDoS-атакам на уровне регионального web-ресурса.

1. В связи с отсутствием собственной сети, нет технической возможности использовать физические средства для противодействия DDoS-атакам. Кроме того, использование таких средств для обеспечения безопасности регионального web-ресурса экономически невыгодно.
2. В связи с обособленностью, нет возможности использовать для анализа данные, полученные на вышестоящих узлах.
3. Также нет возможности заблокировать трафик на вышестоящих узлах.
4. Существует ограничение в физических ресурсах сервера. Привлечение новых ресурсов и увеличение мощности, представляется затруднительным.
5. Ограничение материальных средств не позволяет использовать сторонние средства для фильтрации трафика и сети доставки контента.
6. Использование собственной CMS или адаптированной свободно распространяемой CMS опасно наличием потенциальных уязвимостей и повышенным расходом ресурсов. Что дает возможность злоумышленнику достичь цели при использовании атаки меньшей мощности.

На основании указанных проблем и потребностей можно выделить следующие требования, предъявляемые к разрабатываемой системе фильтрации трафика:

1. Разрабатываемое средство должно быть 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 рамка работы физического или виртуального хостинга.
4. Для блокировки вредоносного трафика используются средства и инструменты, доступные в рамках физического или виртуального хостинга.

5. Средство должно отвечать требованиям кроссплатформенности. Использоваться на разных операционных системах, с различными web-серверами и сетевыми сервисами.
6. В процессе работы средство должно генерировать минимальную нагрузку на ресурсы сервера, так как в результате DDoS-атаки сетевой ресурс может испытывать недостаток в свободных ресурсах.

3.2. Выбор средств реализации

В качестве среды программирования выбран PHP (от англ. PHP: Hypertext Preprocesor). Выбор PHP позволяет выполнить требование кроссплатформенности, применяемое к разрабатываемому средству. Данная среда программирования представляет собой скриптовый язык программирования, интерпретатор компилирующего типа [67]. По состоянию на ноябрь 2013 г., PHP является одним из самых популярных языков для разработки web-приложений [68]. Данный интерпретатор поддерживается различными web-серверами, расположенными на различных платформах. Интерпретатор доступен у большинства хостинг провайдеров на самых различных тарифных планах. Таким образом, средство, разработанное с помощью PHP, будет отвечать требованиям кроссплатформенности и функционировать не зависимо от операционной системы и web-сервера.

В качестве системы управления базами данных был выбран mySQL. Данное программное обеспечение также отвечает требованиям кроссплатформенности [69]. Является свободно распространяемым и доступно у большинства хостинг-провайдеров. Использование в качестве СУБД mySQL в рамках данной разработки не является критичным, при необходимости и минимальных доработках разрабатываемое средство может использовать различные реляционные СУБД.

3.3. Выбор данных для анализа

Разрабатываемое программное средство предназначено для выполнения на защищаемом ресурсе, таким образом, данные для анализа ограничены рамками конечного сервера. В качестве таких данных могут выступать различные log-файлы, например, log-файлы web-сервера, сервера баз данных и т.д., или системные log-файлы. А также данные, полученные непосредственно с сетевого интерфейса. Если сетевой ресурс функционирует в узких рамках виртуального хостинга, то единственными данными, доступными для анализа, будут выступать данные, хранящиеся в log-файлах сервера.

На сегодняшний день одним из самых популярных web-серверов является web-сервер Apache [70]. Реализация программного средства будет происходит на примере анализа данных, полученных из log-файлов этого сервера. Данные обращений к web-серверу Apache сохраняются в log-файле access. log, имеющем следующую структуру –

%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" ,

в котором:

- **%h** – хост/IP-адрес, с которого произведен запрос к серверу;
- **%t** – время запроса к серверу и часовой пояс сервера;
- **%r** – тип запроса, его содержимое и версия;
- **%s** – код состояния HTTP;
- **%b** — количество отданных сервером байт;
- **%{Referer}** – URL-источник запроса;
- **%{User-Agent}** – HTTP-заголовок, содержащий информацию о запросе (клиентское приложение, язык и т.д.);
- **%{Host}** – имя Virtual Host, к которому идет обращение.

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /style.css HTTP/1.0" 200 3214

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /index.php HTTP/1.0" 200 1406

Листинг 1. Пример записи из файла access. log [71]

Подобную структуру файла access.log используют и другие web-сервера: Nginx, Lighthttpd и т.д. Кроме того, принципиальная схема файла access. log, аналогична log-файлам других сетевых сервисов.

3.4. Разработка программного комплекса фильтрации трафика

3.4.1. Алгоритм работы программного комплекса фильтрации трафика

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 анализируется 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 полученные кластеры

5. Трафик, помеченный как вредоносный, блокируется.

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

- модуль обработки данных и их загрузки в базу данных
- модуль обнаружения начала атаки
- модуль фильтрации трафика

3.4.2. Средство обработки и загрузки данных

Выделение средства обработки и загрузки данных в отдельный модуль позволяет организовать работу программного комплекса с log-файлами различных типов и различного содержания. Обработка и приведение данных к одному виду на самом первом шаге работы программного средства в дальнейшем позволяет упростить этот процесс и анализировать их без внесения каких-либо изменений в другие модули. Таким образом, разрабатываемое программное средство может быть использовано не только для защиты web-ресурсов от атак типа http-flood, но и для защиты различных сетевых ресурсов и сервисов от DDoS-атак различных типов.

При разработке программного средства экспорта данных из log-файлов в базу данных особое внимание было уделено нагрузке, которую это средство может генерировать. Вопрос нагрузки является весьма актуальным, так как средство предназначено для обработки больших объемов информации. Одному обращению к серверу в log-файле соответствует, как правило,

несколько записей. Если web-сайт, расположенный на сервере, является популярным, его посещает большое количество пользователей, и, если эти пользователи просматривают большое количество страниц, информация в log-файлах сервера накапливается с большей скоростью. Кроме того, возможен вариант, когда в рамках одного физического web-сервера поддерживается несколько виртуальных. В этом случае количество информации для экспорта в базу данных также увеличивается.

Средство обработки и загрузки данных с заданным интервалом времени производит чтение из log-файла, актуальных данных, приводит их к необходимому виду и производит загрузку в базу данных.

Каждая строка в log-файле соответствует отдельному запросу к сетевому ресурсу. При извлечении данных из log-файла происходит построчное считывание данных. В дальнейшем из каждой строки данные извлекаются в массив или в отдельные переменные. Разбор данных из строки происходит с использованием функций для работы с регулярными выражениями, такими как preg_split(), split(). В результате тестирования программного средства было замечено, что в некоторых случаях эти функции генерируют значительную нагрузку. В связи с этим был разработан дополнительный способ извлечения данных из строк log-файла (Листинг 2).

```
$ip=substr($line,0,strpos($line," "));
$line=substr($line,strpos($line," ")+1,strlen($line));

$t1=substr($line,0,strpos($line," "));
$line=substr($line,strpos($line," ")+1,strlen($line));

$t2=substr($line,0,strpos($line," "));
$line=substr($line,strpos($line," ")+1,strlen($line));

$date=substr($line,1,strpos($line,"] ")-1);
```

```
$line=substr($line,strpos($line,"] ")+1,strlen($line));

$get=substr($line,2,strpos($line,'" ')-2);
$line=substr($line,strpos($line,'" ')+2,strlen($line));

$t3=substr($line,0,strpos($line," "));
$line=substr($line,strpos($line," ")+1,strlen($line));

$t4=substr($line,0,strpos($line," "));
$line=substr($line,strpos($line," ")+1,strlen($line));

$url=substr($line,0,strpos($line,'" ')+1);
$line=substr($line,strpos($line,'" ')+1,strlen($line));
```

Листинг 2. Фрагмент кода разбора строки с помощью функции **substr()**

В этом случае извлечение данных из строки происходит последовательно с помощью функции substr(). Первый параметр извлекается из строки до заданного разделителя, при этом происходит усечение строки до того же разделителя. Данный шаг повторяется до тех пор, пока не будет достигнут конец строки.

Данный способ извлечения данных из строки является более громоздким по сравнению с использованием функций для работы с регулярными выражениями. Однако, в некоторых случаях он использует меньше ресурсов и имеет большую скорость работы.

Информация из log-файла хранится в базе данных в отдельной таблице. Каждый столбец таблицы характеризует одну или несколько колонок из файла access.log. При экспорте данные приводятся к удобным форматам обработки. Так, например, дата и время запроса из текстового вида переводится в так называемое UNIX-время (табл. 1.). Количество секунд,

прошедших с полуночи (00:00:00 UTC) 1 января 1970 г. (четверг); время с этого момента называют «эрой UNIX» (англ. Unix Epoch) [72].

Все присутствующие в log-файле данные могут быть использованы для анализа. Также на основании этих данных можно выделить сопутствующие данные, которые также могут быть использованы. Эти данные можно получить с помощью группировки основных данных или на основании внешних данных, характеризующих основные:

- количество запросов за определенный период с определенного адреса, к определенной странице, определенного размера и т.д.;
- скорость поступления запросов;
- данные, сгруппированные по различным срезам, например, на основании модуля GeoIP, можно выделить запросы с определенного региона, города, страны и т.д.

Таблица 2

Пример таблицы в базе данных

id_log	ip	log_time	get	kod	size	url	brows
3	94.125.184.50	1361675477	POST /wp-login.php HTTP/1.1	200	3200	"http://cntdaltai.ru/wp-login.php"	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
4	94.125.184.50	1361677446	POST /wp-login.php HTTP/1.1	200	3200	"http://cntdaltai.ru/wp-login.php"	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
5	46.39.239.151	1361678160	POST /wp-login.php HTTP/1.0	200	3200	"http://cntdaltai.ru/wp-login.php"	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
6	77.66.3.219	1361678195	POST /wp-login.php HTTP/1.1	200	3495	"http://cntdaltai.ru/wp-login.php"	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
7	163.43.132.41	1361678226	POST /wp-login.php HTTP/1.1	200	3495	"http://cntdaltai.ru/wp-login.php"	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0

3.4.3. Средство обнаружения начала атаки

Средство обнаружения начала атаки в режиме реального времени рассчитывает среднеквадратичное отклонение с учетом актуальных сезонных периодов по количеству запросов к сетевому ресурсу в каждом периоде.

Программное средство дает возможность задать размерность рассматриваемых периодов: 1 минута, 15 минут, 1 час и т.д. А также вести мониторинг сразу по нескольким периодам. На основании рассчитанного среднеквадратичного отклонения задается верхняя граница количества запросов к сетевому ресурсу соответствующего периода.

Средство обнаружения начала атаки имеет гибкие настройки, позволяющие задать чувствительность к возможной атаке (Листинг 3). Конфигурационные данные выделены в отдельный php-файл, что дает дополнительные возможности как с точки зрения удобства, так и с точки зрения безопасности. Чувствительность варьируется посредством коррекции границы, а также нарушением границы сразу в нескольких периодах разного размера. Например, при нарушении границы на минутных интервалах средство может только известить заинтересованных лиц о возросшей активности. В случае нарушения границы также на пятиминутном интервале происходит полное включение механизма защиты.

```
//время периода сетевой активности в секундах, 86400 сутки, 604800 неделя
$loop=40400;
//период для исследования в секундах
$user_per=300;
//количество периодов для анализа
$count_user_per=100;
//период, который необходимо отступить от начала атаки для пометки благополучного трафика
$safe_per=600;
//число в процентах, на которое благополучный трафик должен отличаться от вредоносного
$pogresnost=10.
```

Листинг 3. Фрагмент конфигурационного файла

В случае обнаружения начала атаки выполняются следующие действия:

1. Рассылка оповещений. В автоматическом режиме происходит рассылка сообщений электронной почты.
2. Выполнение скриптов. Запускаются скрипты или сторонние программы, подготовленные для выполнения системным администратором. Это могут быть как скрипты, включающие дополнительные уровни кэширования или же отключающие модули web-ресурса, генерирующие повышенную нагрузку, так и системные скрипты и программы.
3. Активация средства фильтрации трафика.

3.4.4. Средство фильтрации трафика

На основании разработанного алгоритма средство фильтрации трафика проводит первичную кластеризацию. В результате первичной кластеризации в базе данных создаются две таблицы, характеризующие вредоносный и благонадежный трафик. Полученные таблицы используются в качестве обучающих выборок при классификации поступающих запросов. В процессе работы таблицы уточняются и дополняются.

Данные, содержащиеся в таблице, характеризующей вредоносный трафик, используются для блокировки трафика. В разрабатываемом программном средстве предусмотрена возможность извлечения из таблицы, соответствующей вредоносному трафику, клиентских IP адресов и создание на их основе запрещающих правил. Кроме этого, на основании данных о вредоносном трафике возможно реализовать дополнительные механизмы защиты. Например, при поступление вредоносных запросов к конкретной странице можно в автоматическом режиме временно заблокировать эту страницу или же подменить ее статичной или кеш-версией. В этом случае вредоносный трафик, который был некорректно классифицирован и не был заблокирован на предыдущем уровне, нанесет меньший вред.

3.4.5. Блокировка вредоносных запросов

Для блокировки вредоносных запросов предусмотрено два варианта. В первом варианте блокировка осуществляется посредством создания соответствующих запрещающих правил для iptables. Второй вариант будет актуален если средство функционирует в узких рамках виртуального хостинга, в этом случае блокировка вредоносного трафика осуществляется посредством запрещающих правил, указанных в файле .htaccess (Листинг 4). В обоих случаях блокировка трафика осуществляется полностью в автоматическом режиме. Также предусмотрен механизм экспорта данных о вредоносном трафике для блокировки его в различных программных файерволах или же на вышестоящих сетевых узлах.

```
order allow,deny
deny from 192.168.0.1
deny from 192.168.0.2
allow from all
```

Листинг 4. Пример блокировки IP-адресов в файле .htaccess

3.4.6. Архитектура программного комплекса

Архитектура программного комплекса представлена на схеме 3. Взаимодействие модулей программного комплекса, друг с другом и с WEB-сервером, происходит по следующей схеме:

В результате обработки запросов приходящих к WEB-серверу из сети интернет, в журнал WEB-сервера добавляются соответствующие события.

Модуль загрузки данных с заданным интервалом времени считывает новые данные из журнала и загружает их в базу данных.

Модуль обнаружения начала атаки, анализирует данные о запросах содержащиеся в базе данных. В случае обнаружения начала атаки, этот модуль создает в базе данных две пустые таблицы. Одну для легитимных запросов, вторую для вредоносных.

Модуль обнаружения вредоносного трафика отслеживает появление и состояние указанных выше таблиц БД. Если таблицы не заполнены, модуль проводит кластеризацию и первичное заполнение таблиц. Если в таблицах уже есть данные, модуль анализирует вновь поступившие запросы на предмет принадлежности к группам благонадежных или вредоносных запросов, и добавляет данные о запросе в соответствующую таблицу.

Модуль блокировки запроса получает список IP-адресов из таблицы содержащей вредоносные запросы и вносит их в «черные списки» файервола или передает для блокировки на вышестоящий сетевой сегмент.

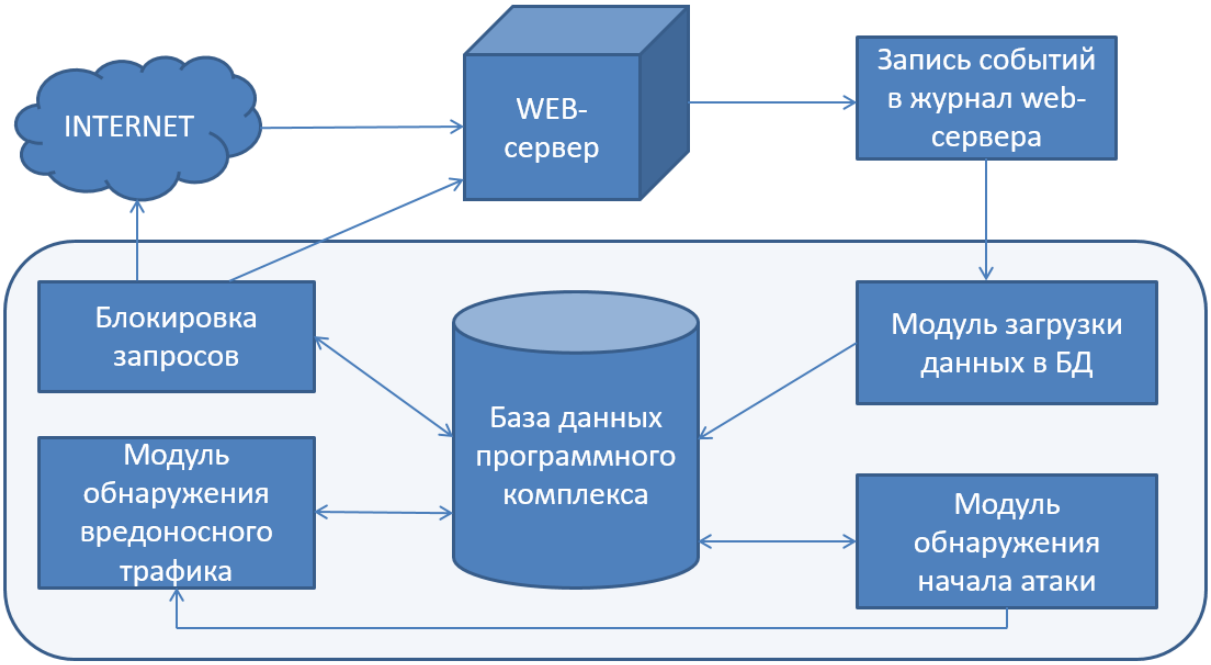


Схема 2. Архитектура работы программного комплекса

3.5. Выводы по третьей главе

Разработанное программное средство полностью отвечает поставленным задачам. Основные черты созданного программного комплекса для обнаружения и противодействия DDoS-атакам это кроссплатформенность, универсальность и масштабируемость. Программный комплекс может применяться в качестве средства обеспечения безопасности так называемой «последней мили». Основной специализацией комплекса является обеспечение безопасности web-серверов от DDoS-атак типа http-flood. Программный комплекс поддерживает различные операционные системы, он может быть использован с большинством современных web-серверов. При этом инсталляция комплекса может осуществляться как в рамках физического сервера, так и в рамках виртуального хостинга.

Универсальность программного комплекса обнаружения и противодействия DDoS-атакам заключается в возможности его использования не только для обнаружения http-flood'a, но и других DDoS-

атак различных типов. При незначительных изменениях, не затрагивающих основной модуль, программное средство может анализировать различные данные, содержащиеся в log-файлах различных сетевых сервисах, или же использовать данные, полученные от сетевых локаторов.

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 сети. 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 одновременно 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.

Глава 4. Апробация разработанного программного комплекса

4.1. Постановка задачи

Практическая апробация разработанного программного комплекса, оценка его эффективности, равно как и исследование DDoS-атак, осложняется их стихийностью. Разработка средств и методик противодействия, как правило, происходит по мотивам прошедших атак. При этом возможность полноценного исследования и апробации созданных средств противодействия имеют только крупные организации, предоставляющие услуги в области защиты от DDoS-атак, и в ходе своей работы, сталкивающиеся с такими атаками ежедневно. Область интересов таких компаний обычно составляют средства противодействия магистрального уровня.

Другая проблема в оценке эффективности разработанного программного комплекса связана с отсутствием «эталонных» средств противодействия, эффективность работы которых можно было бы сравнивать с эффективностью работы разработанного средства обнаружения и противодействия.

Для решения первой проблемы, при отсутствии возможности использовать для апробации и обкатки программного средства реальных условий, целесообразно создать искусственную среду для проведения нагрузочных и стресс тестов, которые бы эмулировали реальные атаки. Оценку эффективности работы в рамках данных стресс тестов можно проводить в сравнении со средствами обнаружения и противодействия вторжениям, которые входят в пакеты различных средств безопасности для рабочих станций. Аналогичный подход был предложен и использован в диссертационной работе «Обнаружение низкоактивных распределенных атак типа «Отказ в обслуживании» в компьютерных сетях», автор М.В. Щерба [73]. Специализация этих средств безопасности напрямую не связана с обнаружением и противодействием DDoS-атакам, но при этом данные

средства могут выступать некоторым, «эталонным» результатом, с которым могут сравниваться результаты работы разработанного средства, а также результаты, полученные в аналогичных, сторонних научных исследованиях.

4.2. Создание нагрузочной сети

В рамках исследования DDoS-атак, а также в рамках апробации методики и разработанного программного комплекса противодействия и обнаружения DDoS-атак, разработана специализированная нагрузочная сеть [74, 75].

Нагрузочная сеть разработана на базе общеуниверситетских компьютерных классов Алтайского государственного университета.

Компьютерные классы Алтайского государственного университета – это около 20 компьютерных аудиторий, включающих в себя более 300 физических компьютеров. Общеуниверситетские компьютерные классы распределены по четырем корпусам университета, находящимся в некотором географическом удалении друг от друга. Объединение компьютерных классов, расположенных в разных корпусах, в локальную сеть и подключение их к сети INTERNET, осуществляется различными способами и различными провайдерами. Данная особенность делает созданную нагрузочную сеть максимально приближенной к реальной зомби-сети. При этом существуют богатые возможности по сбору и анализу данных. Сетевые локаторы-детекторы могут быть установлены в различных узлах сети, при этом имеется возможность получать статистическую информацию с корпусных маршрутизаторов и других сетевых устройств.

В среднем компьютеры, входящие в созданную нагрузочную сеть, имеют следующие технические характеристики и комплектность:

- процессор: Celeron Dual 2600 MHz;
- размер оперативной памяти: 2Gb;
- размер жесткого диска: 250Gb;
- сетевой адаптер: 100 Mb/s;

- операционная система: Windows XP Professional, Service pack 3;
- LCD монитор, 17 дюймов;
- мышь, клавиатура.

Компьютеры нагрузочной сети в силу того, что они располагаются на базе общеуниверситетских компьютерных классов, имеют разнообразный набор установленного программного обеспечения, используемого в учебном процессе:

- **Офисные пакеты** – Microsoft office, Open office и т.д.
- **Средства разработки** – Eclips, Visual Studio, NetBeans, Lazarus, FreePascal и т.д.
- **Графические пакеты** – Adobe Photoshop, Corel Drow, 3D studio MAX, Blender, Gimp и т.д.
- **Интернет браузеры** – Mozilla Firefox, Internet Explorer, Opera, Google Chrome.

Напрямую установленное программное обеспечение не может помешать при проведении нагрузочных тестов. С одной стороны, некоторые программы, использующие сетевые ресурсы или ресурсы компьютера, могут влиять на работу специализированного программного обеспечения, отвечающего за проведение нагрузочных тестов. С другой – наличие данного программного обеспечения и его использование обучающимися, в том числе и в момент проведения нагрузочных тестов, эмулирует компьютеры зомби-сети, которые состоят из компьютеров, принадлежащих обычным пользователям.

В качестве специализированного программного обеспечения для создания нагрузочной сети выступает клиент-серверное приложения для проведения нагрузочных и стресс-тестов – Apache JMetr [76].

Указанное программное обеспечение является свободно распространяемым. Распространяется по лицензии Apache license 2.0. Текущая версия Apache JMetr позволяет проводить нагрузочные тесты для различных соединений: FTP, LDAP, SOAP, JMS, POP3, IMAP, в том числе

HTTP и TCP. Поддерживается проведение распределенных нагрузочных тестов при инсталляции программного средства на несколько компьютеров. Реализована поддержка авторизации виртуальных пользователей. В нагрузочной сети данное программное средство работает в фоновом режиме, не мешая работе основных пользователей общеуниверситетских компьютерных классов. Точно так же, как работает вредоносное программное обеспечение клиентских компьютеров зомби-сетей.

Для гибкого и одновременного управления установленным программным обеспечением был разработан управляющий модуль, позволяющий удаленно запускать и отслеживать состояние серверной части Apache Jmetr.

Важной особенностью используемого программного обеспечения и созданной нагрузочной сети является возможность разработки сценариев нагрузочных тестов на основании реальных данных доступа к серверу. Это дает возможность проводить нагрузочные тесты по мотивам реальных DDoS-атак. При этом нагрузочный тест, по сути, будет являться уменьшенной копией существующей атаки – экспериментом, который можно повторять необходимое количество раз, изменяя входные данные и подбирая оптимальное средство противодействия.

Созданная нагрузочная сеть для проведения стресс-тестов имеет следующие характеристики:

- размер сети – около 300 физических компьютеров;
- распределение нагрузочной сети по разным корпусам;
- наличие различных точек для отслеживания трафика;
- максимальная приближенность к реальным бот-сетям;
- возможность создавать тест на основании данных доступа реальных DDoS-атак.

4.3. Ход экспериментов

4.3.1. Инсталляция и подготовка сервера

В качестве операционной системы для сервера, безопасность которого требуется обеспечивать, была выбрана операционная система DEBIAN [77]. Данная операционная система относится к семейству операционных систем Linux, состоит из свободно распространяемого программного обеспечения с открытым исходным кодом. В настоящее время является одним из самых важных и популярных дистрибутивов этого семейства, оказывающего важное влияние на его развитие [78, 79].

На сервер установлена последняя актуальная версия данной операционной системы – Debian 7.3, полученная из официального репозитария. Сервер имеет следующие технические характеристики:

- процессор: Intel Core i3;
- размер оперативной памяти: 4Gb;
- размер жесткого диска: 500Gb;
- сетевой адаптер: 1 Gb/s;
- операционная система: Debian 7.3;
- LCD монитор, 17 дюймов;
- мышь, клавиатура.

Установка операционной системы происходит со стандартным набором компонентов «СЕРВЕР». Среди прочего программного обеспечения, входящего в этот набор, были установлены WEB-сервер с поддержкой интерпретатора PHP, сервер баз данных. В качестве WEB-сервера и сервера баз данных используются, соответственно, WEB-сервер Apache и СУБД mySQL, обоснованность использования которых была приведена в предыдущей главе.

Конечной целью экспериментальных DDoS-атак, типа http-flood, должны стать web-страницы, генерируемые сервером. В качестве источника

таких страниц выступает CMS Wordpress (CMS аббревиатура от английского Content Management System – система управления содержанием) [80].

Система управления содержанием Wordpress распространяется по лицензии GNU/GPL с открытым исходным кодом. Использование данной системы управления содержанием в экспериментах по обеспечению безопасности WEB-сервера неслучайно. Во-первых, Wordpress является одной из самых популярных систем управления содержанием. Во-вторых, в качестве системных требований для инсталляции данного программного обеспечения требуется наличие PHP интерпретатора и системы управления базами данных mySQL, которые по условиям эксперимента уже доступны на сервере.

На сервер установлена последняя стабильная версия Wordpress, на момент проведения экспериментов – Wordpress 3.4. Дистрибутив CMS получен с официального сайта. Установка проведена в базовом режиме, без подключения сторонних модулей. После инсталляции в CMS Wordpress добавлено содержание – созданы страницы, добавлены записи, загружены фотографии. Всего добавлено около 100 записей различного размера, иллюстрированные изображениями.

На этом этапе состояние сервера было зафиксировано в отдельный образ жесткого диска установленного в сервере. Данная мера применена в связи с необходимостью протестировать отдельно каждое средство обнаружения и противодействия DDoS-атакам. Инсталляция всех средств одновременно нецелесообразна, так как несколько средств противодействия, установленные одновременно в рамках одного сервера, могут мешать работе друг друга и накладывать определенные погрешности на результаты экспериментов. Последовательная установка средств противодействия и их удаление после проведения эксперимента также не желательны, так как средство противодействия при установке может вносить изменения в операционную систему, ее конфигурационные файлы и т.д.

В связи с этим было принято решение зафиксировать чистый образ сервера с установленным всем необходимым программным обеспечением, кроме средства противодействия. Установку средства противодействия проводить отдельно для каждой серии экспериментов, при этом возвращая сервер в исходное состояние.

В качестве средства клонирования образа диска и его дальнейшего восстановления было выбрано специализированное программное обеспечение – Clonezilla.

Clonezilla – свободно распространяемое программное обеспечение с открытым исходным кодом, предназначенное для клонирования жестких дисков и их разделов [81]. Может применяться для создания резервных копий и аварийного восстановления. Актуальная версия Clonezilla получена из официального репозитария.

В связи с тем, что некоторые средства, используемые в рамках данной работы для обнаружения и блокировки вредоносного трафика DDoS-атак, существуют только для операционных систем семейства Windows. Для объективной оценки разрабатываемого программного обеспечения было принято решение, создать ещё один рабочий образ на базе этой операционной системы. В качестве базового набора программного обеспечения использовалось программное обеспечение, указанное выше, – WEB-сервер Apache, СУБД mySQL, PHP. Указанное программное обеспечение является кроссплатформенным или имеет отдельные версии для различных типов операционных систем.

4.3.2. Проведение простых нагрузочных тестов

Успешная работа разработанного программного комплекса подразумевает наличие достаточного объема исторических данных, доступных для анализа. В реальных условиях эти данные могут быть получены из архивов log-файлов, по умолчанию срок хранения которых составляет три месяца. В рамках проводимых внутри нагрузочной сети

экспериментов эти данные отсутствовали. Поэтому для предоставления программному комплексу актуальных данных для анализа были использованы имеющиеся у автора реальные данные из файлов access.log web-сервер Apache, соответствующие запросам к системе управления содержанием Wordpress. Эти данные можно использовать, так как установленные копии Wordpress'a имеют сходную структуру и сходное пространство url-адресов. Незначительные отличия в log-файлах, такие как, например, название картинок, были отредактированы вручную. После этого данные были помещены в log-файлы web-сервера нагрузочной сети и стали доступны для анализа.

Так как в самой простой реализации нагрузочных тестов предполагался только анализ данных из файла access.log и выявление вредоносных и благонадежных запросов без оценки работоспособности самого сервера. Было принято решение эмулирования запросов путем постепенной, последовательной загрузки их в базу данных без использования созданной нагрузочной сети. При этом к существующим данным, характеризующим нормальную сетевую активность, были добавлены данные, характеризующие вредоносные запросы. Всего было разработано три сценария проведения экспериментальных DDoS-атак:

1) благонадежные запросы, плюс флуд-запросы к отдельной странице;
2) благонадежные запросы, плюс флуд-запросы к нескольким страницам;
3) благонадежные запросы, плюс динамические флуд-запросы к различным ресурсам сервера.

В последнем сценарии вредоносные запросы пытались имитировать действия реальных пользователей, обращаясь к разным страницам.

Результаты этих тестов сложно соотнести с реальными данными, однако можно достаточно быстро и без затрат, в первом приближении, подтвердить или опровергнуть разрабатываемые гипотезы. Основным же

минусом таких экспериментов является невозможность оценить работу других средств противодействия.

На следующем шаге все компьютеры, входящие в созданную нагрузочную сеть, были разделены на благонадежные и вредоносные. На основании этого разделения были созданы сценарии проведения экспериментальных DDoS-атак [82]. Благонадежные компьютеры генерировали запросы эмулируя поведение легитимных пользователей, на основании данных о легитимных пользователях из файла access.log web-сервера. Вредоносные компьютеры генерировали запросы на основании разработанных выше сценариев.

Таблица 2

Сводные результаты работы различных средств противодействия и обнаружения по итогам нагрузочных тестов – DDoS-атак типа http-flood, направленных к одной странице.

Система	Ложные срабатывания, %	Не обнаруженные вредоносные запросы, %	Среднее время между началом и обнаружением атаки, мин.
Kaspersky Anti-Haker	0,2	5,4	8
Snort	0,6	5,1	7
Symantec	0,8	7,1	14
DDOS deflate	0,4	5,9	10
Разработанное средство	0.4	2,2	5

Таблица 3

Сводные результаты работы различных средств противодействия и обнаружения DDoS-атак типа http-flood, направленных к разным страницам.

Система	Ложные срабатывания, %	Не обнаруженные вредоносные запросы, %	Среднее время между началом и обнаружением атаки, мин.
Kaspersky Anti-Haker	0,4	5,5	8
Snort	0,8	5,4	9
Symantec	0,8	8,2	14
DDOS deflate	0,8	12	10
Разработанное средство	0,9	3,3	5

Таблица 4

Сводные результаты работы различных средств противодействия и обнаружения, по итогам нагрузочных тестов – динамических DDoS-атак типа http-flood.

Система	Ложные срабатывания, %	Не обнаруженные вредоносные запросы, %	Среднее время между началом и обнаружением атаки, мин.
Kaspersky Anti-Haker	0,7	9,4	10
Snort	0,9	10,9	12
Symantec	0,8	12,8	17
DDOS deflate	0,7	18,1	14
Разработанное средство	1	8,1	6

4.3.3. Проведение нагрузочных тестов – копий реальных DDoS-атак

Следующим этапом в апробации разработанного программного средства стало его тестирование с использованием данных, соответствующих реальным DDoS-атакам. Эти данные были получены из файлов access. log реальных web-серверов и характеризуют период начала атаки.

На основании этих данных были созданы сценарии для проведения нагрузочных тестов, которые в данном случае будут являться уменьшенными копиями реальных DDoS-атак. При разработке сценариев все данные были проанализированы, отдельно для последующей оценки результатов были выделены вредоносные запросы. Результаты этих тестов приведены в таблице 5.

Таблица 5

Сводные результаты работы различных средств противодействия и обнаружения по итогам нагрузочных тестов – копий DDoS-атак типа http-flood.

Система	Ложные срабатывания %	Не обнаруженные вредоносные запросы, %	Среднее время между началом и обнаружением атаки, мин.
Kaspersky Anti-Haker	0,7	11	44
Snort	3,8	10,9	17
Symantec	4,3	8,4	12
DDOS deflate	2,2	18,1	37
Разработанное средство	3,8	8,1	4

4.3.4. Имитация DDoS-атак к существующим web-сайтам

В завершающей стадии экспериментов было принято решение протестировать работу нагрузочной сети на реальных серверах, входящих в

корпоративную компьютерную сеть Алтайского государственного университета.

Корпоративная компьютерная сеть Алтайского государственного университета, помимо серверов и активного сетевого оборудования включает около 3 тыс. физических, пользовательских компьютеров, располагающихся в различных корпусах головного вуза, а также в его подразделениях и филиалах, расположенных в различных городах Алтайского края. Также внутри корпоративной сети существует несколько внутрикорпоративных ресурсов, доступ к которым осуществляется только с компьютеров корпоративной сети. Среди этих ресурсов: Информационно-аналитическая система «Кейс»; внутренний «web-портал»; Информационная система «Университетское расписание» и т.д. Так как работа многих указанных ресурсов является критичной и существует опасение, что проведение нагрузочного тестирования может выйти за рамки эксперимента и парализовать работу указанных сервисов, после согласования с администрацией университета было принято решение провести нагрузочное тестирование, имитирующее реальную DDoS-атаку, к Информационной системе «Университетское расписание». Работа этой системы является менее критичной, кроме того, данные о текущем расписании могут быть получены напрямую в Бюро расписания или с факультетских досок расписания.

Предварительное нагрузочное тестирование было проведено в выходной день, когда количество легитимных обращений к серверу минимально. Его результаты подтвердили работоспособность разработанного программного комплекса, а также «живучесть» тестируемого ресурса.

Основное тестирование было проведено в течение рабочей недели, когда к Информационной системе «Университетское расписание» обращались не только компьютеры, входящие в нагрузочную сеть и имитирующие вредоносные запросы, но и другие, с которых обращение к системе совершали легитимные пользователи. Тестирование средства, в

условиях максимально приближенных к реальным, показало результаты, согласуемые с результатами предыдущих тестов (табл. 6).

Таблица 6

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, %	Не обнаруженные 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

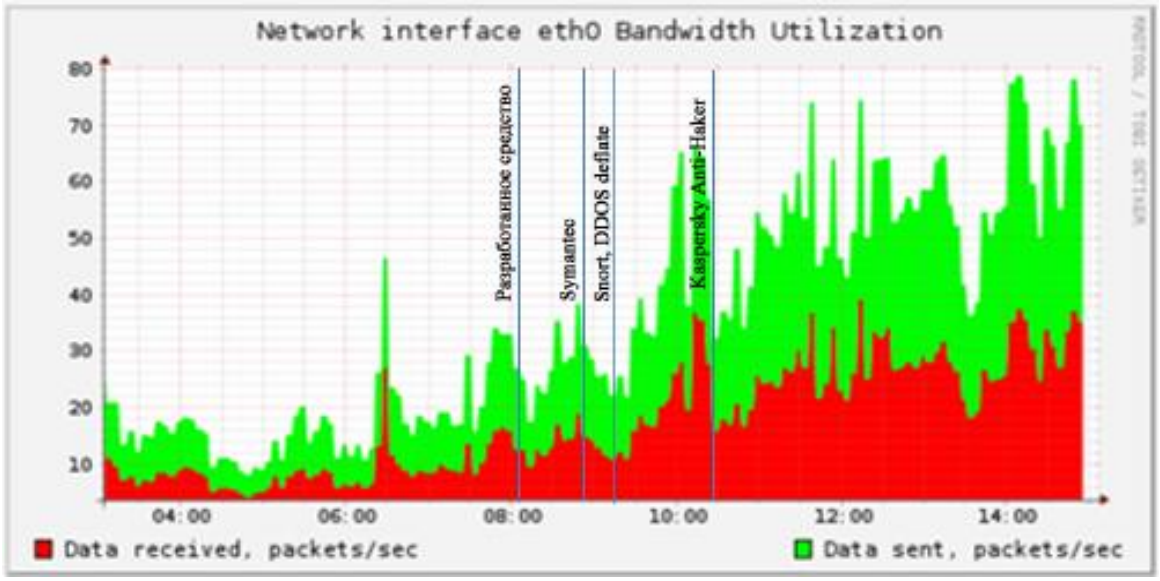


Рисунок 19. Время обнаружения начала атаки тестируемыми средствами противодействия

Данный эксперимент позволил не только подтвердить работоспособность разработанного программного комплекса по обнаружению и противодействию DDoS-атакам, оценить его эффективность по сравнению с другими средствами противодействия, но и оценил работу Информационной системы «Университетское расписание». В рамках эксперимента оценивались: время отклика сервера, его доступность, комфортность работы со стороны пользователя и т.д.

Также в результате данного масштабного эксперимента были даны оценки работы корпоративной компьютерной сети в целом. Нагрузочное тестирование позволило выявить «узкие» места в топологии компьютерной сети и ошибки, допущенные при проектировании. Данные для проведения такого анализа были получены с управляемых коммутаторов различных сегментов корпоративной компьютерной сети.

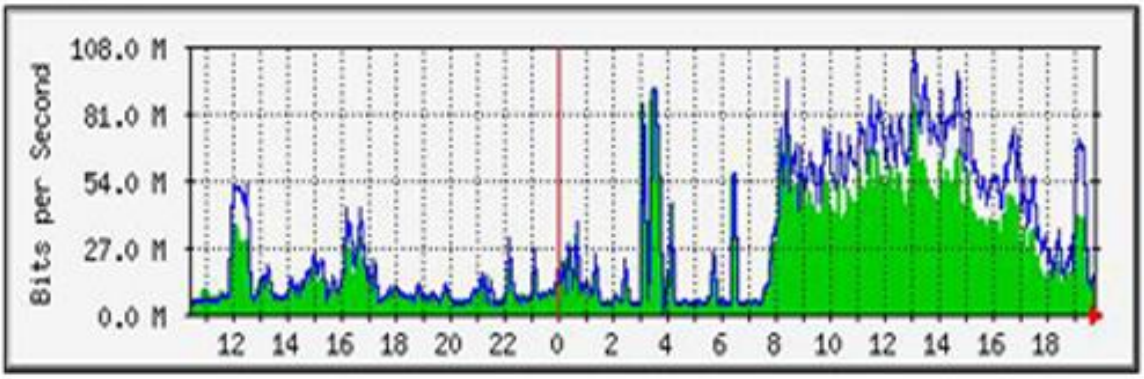


Рисунок 20. Пример загрузки порта коммутатора, отдельного сегмента сети после начала атаки

4.3.5. Обобщение данных. Результаты

Проводимые нагрузочные тесты эмулировали DDoS-атаки средней и малой интенсивности. В результате этих тестов не происходило перенаполнения полосы пропускания (рисунки 20, 21). Таким образом, мощность тестовых атак в среднем соответствовала мощности реальных распределенных атак, направленных на отказ в обслуживании к региональным сайтам.

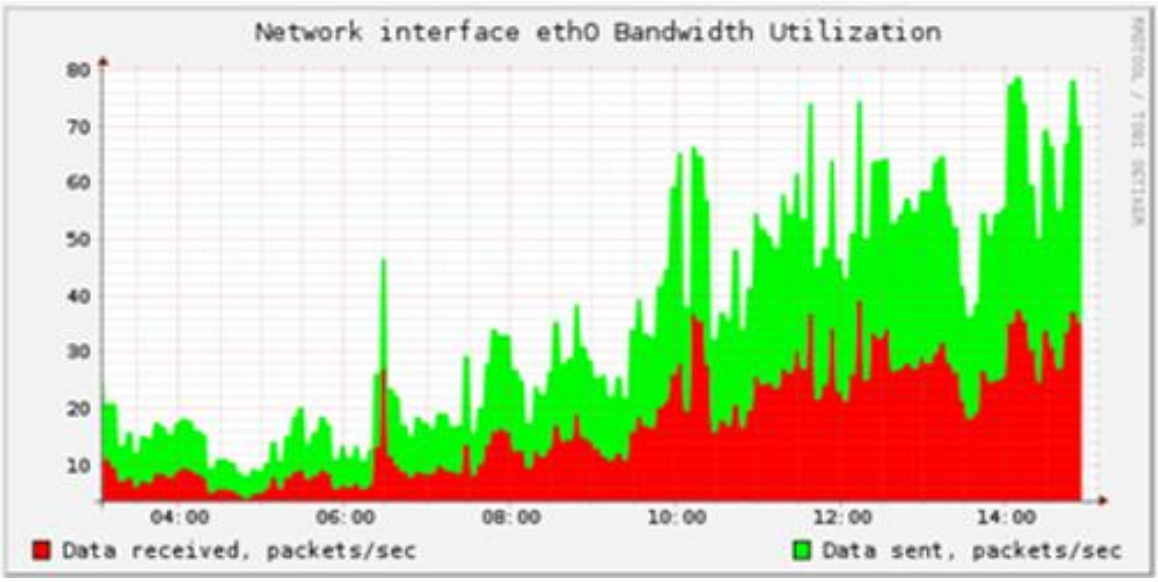


Рисунок 21. Загрузка сетевого интерфейса атакуемого сервера после начала атаки

В среднем после обобщения данных, полученных по итогам всех тестов, были зафиксированы следующие результаты эффективности разработанного программного средства: ошибка первого рода (количество ложных срабатываний) – 2%, ошибка второго рода (количество необнаруженных атак) – 7.4, время, потребовавшееся для обнаружения начала атаки – 12 мин. Таким образом, разработанное программное средство лидирует по скорости обнаружения начала атаки и по выявлению вредоносных запросов, среди рассматриваемых аналогов. Если рассматривать результативность разработанного программного средства с аналогичными средствами, разработанными в рамках других исследований, можно выделить результаты диссертационной работы «Обнаружение низкоактивных распределенных атак типа «Отказ в обслуживании» в компьютерных сетях», автор М.В. Щерба [73]. По итогам этой работы были получены следующие результаты для ошибок первого рода (количество ложных срабатываний – 11,6%) и ошибок второго рода (количество необнаруженных атак – 3,4%). В указанной диссертационной работе также приводится описание эксперимента и полученные результаты. В рамках данной диссертационной работы для объективной оценки результатов была

предпринята попытка провести эксперимент, аналогичный предложенному. В ходе эксперимента были получены следующие данные (табл. 7).

Таблица 7

Результаты проведения эксперимента по сравнению эффективности

Система	Ложные срабатывания, %	Не обнаруженные 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

На основании сравнения этих результатов можно сделать вывод, что разработанное программное средство имеет большую эффективность. Данное сравнение является приемлемым, так как в указанной диссертационной работе результаты приводятся совместно с результатами использования других средств: Snort, Aids, Kaspersky Anti-Haker. И в целом показатели эффективности этих средств коррелируют между собой.

Благодаря использованию разработанного программного средства в целом была снижена нагрузка на использование ресурсов атакуемого сервера за счет блокировки вредоносных запросов до момента их поступления к web-серверу. Так, например, использование ресурсов процессора находилось на приемлемом уровне (рисунки 22–24). В случае отключения средства противодействия процессы web-сервера и сервера баз данных полностью использовали свободные ресурсы процессора.

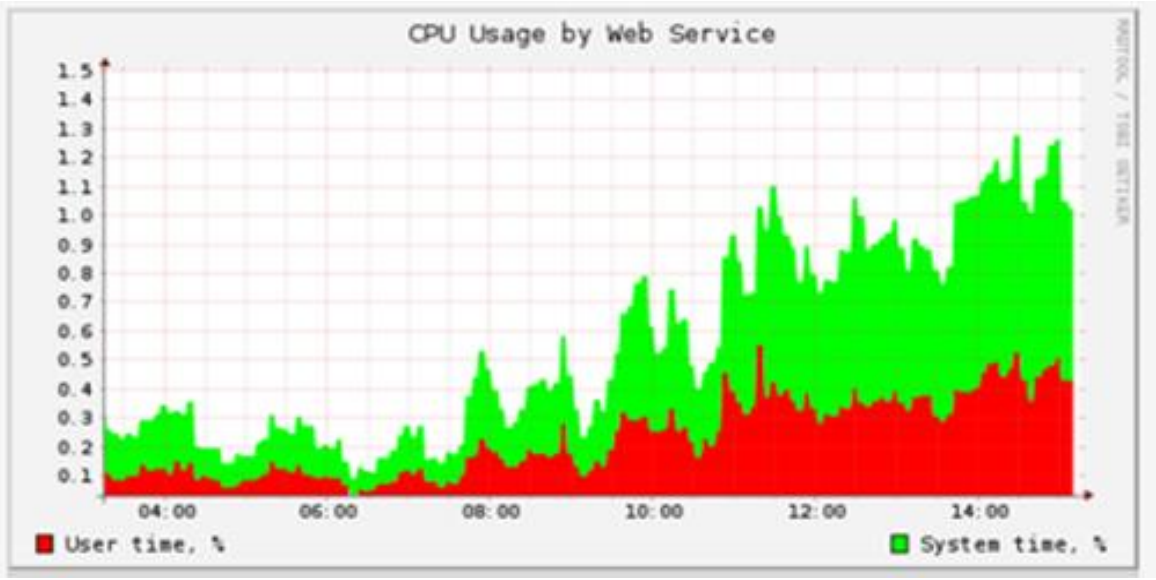


Рисунок 22. Использование ресурсов процессора атакуемого сервера после начала атаки

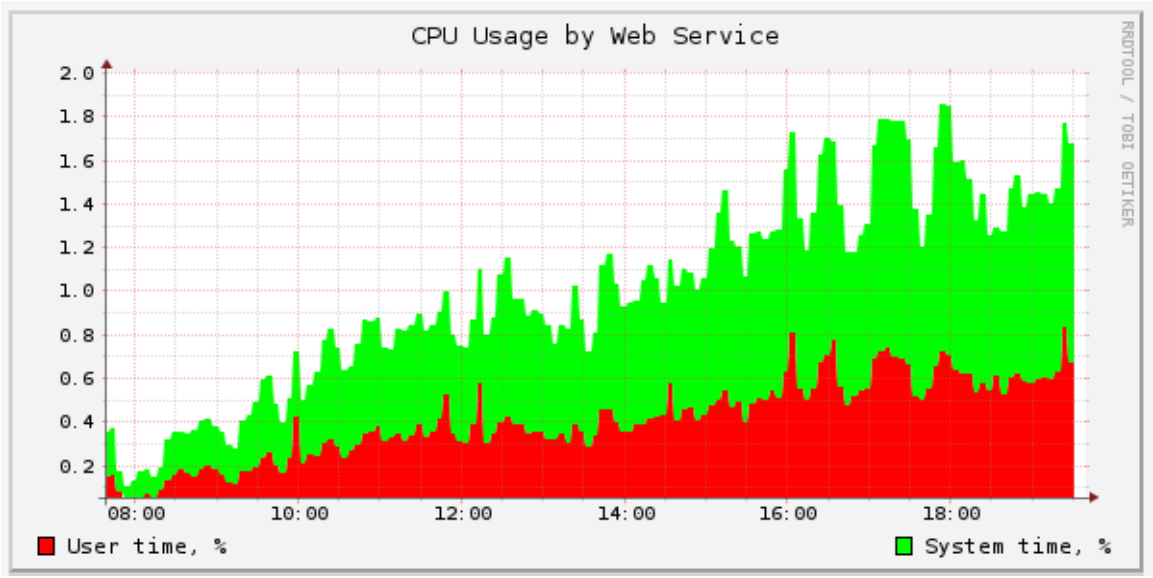


Рис. 23. Нагрузка на процессор со стороны web-сервера после начала атаки

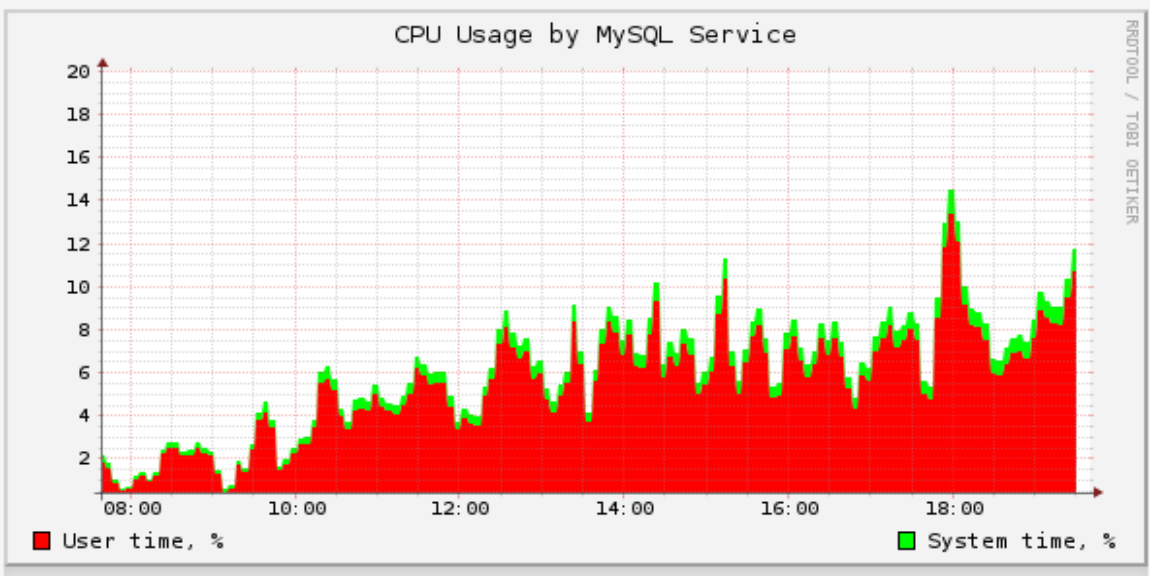


Рис. 24**.** Нагрузка на процессор со стороны сервера баз данных после начала атаки

4.4. Апробация в реальных условиях

После апробации разработанного программного комплекса по обнаружению и противодействию DDoS-атакам была проведена его государственная регистрация в реестре программ для ЭВМ – Свидетельство № 2013617238 от 06 августа 2013 (Приложение 1). С момента получения свидетельства разработанный программный комплекс активно внедряется на ряде площадок регионального и всероссийского уровней. На момент 1 января 2014 г. за неполные полгода, разработанное программное средство успешно внедрено на пяти площадках и размещено на 14 серверах, безопасность которых требуется обеспечивать. Результаты оценки эффективности обнаружения начала атаки и выявление вредоносного трафика в целом соответствуют результатам, полученным при проведении тестов в нагрузочной сети. Отклонение для ошибки первого рода составило не более 3%, отклонение для ошибки второго рода не более 6%. Данные результаты подтверждаются актами внедрения разработанных программных средств на площадках заказчиков.

Также представители заказчиков выделяют следующие показатели эффективности:

Таблица 8

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

4.5. Методика определения уязвимостей к DDoS-атакам систем управления содержанием

При проведении внутри нагрузочной сети различных экспериментов была зафиксирована значительная разница в использовании таких ресурсов, как оперативная память и процессорное время, при обращении к различным скриптам сервера [83]. Эта разница вполне очевидна, так как разные скрипты могут проводить ресурсоемкие вычисления, получать большие выборки данных из базы данных, кроме того, эти скрипты могут быть не оптимизированы с точки зрения правильности и аккуратности написания кода. Известно также, что при проведении http-flood атак средней и малой интенсивности, не нацеленных на заполнение всей полосы пропускания, злоумышленники пытаются найти скрипты, использующие в работе максимальное количество ресурсов. Для отслеживания и последующей оптимизации таких скриптов в распоряжении системных администраторов существует набор системных средств, фиксирующих расходы ресурсов отдельными скриптами. Однако в рамках проведения нагрузочных тестов было замечено, что эти данные не отвечают условию объективности. В

системе управления содержанием потенциально могут быть скрипты, генерирующие приемлемую нагрузку в нормальном режиме работы. Но при поступлении лавинообразного количества запросов могут начать генерировать значительно большую нагрузку, не поддающуюся прогнозу.

Для изучения данной ситуации была проведена серия нагрузочных тестов. При проведении этих тестов не использовалось разработанное средство противодействия. Проводилась только фиксация потребляемых ресурсов. По сути, проводилось исследование по методу «черного ящика», направленное на выявление уязвимостей [84]. По этой же причине для тестов использовался только один образ операционной системы на базе Windows XP, указанный выше.

Основной трудностью при проведении эксперимента стало выявление целей-скриптов, на которые необходимо было проводить атаки. Это связано с тем, что один и тот же скрипт может использовать различные ресурсы в зависимости от передаваемых в него параметров. И его полный url-адрес может быть не отражен в log-файлах. Для создания списка всех возможных целей была использована библиотека mnoGoSearch для языка PHP, которая представляет модуль полнотекстового поиска – реализацию поисковой машины [85]. С помощью этого модуля был создан список всех возможных страниц сайта – список скриптов с определенными параметрами. Затем из списка были удалены однотипные страницы, показывающие различные записи или новости.

Второй задачей, требующей решения в рамках проведения данного эксперимента, стала задача по выбору оптимального значения интенсивности теста. Если к серверу будет поступать слишком большое количество запросов, т.е. интенсивность нагрузочного теста будет высока, единственное, что можно будет установить, это то, что сервер работает некорректно. Так как в этом случае абсолютно любой скрипт будет использовать всю доступную для него память и процессорное время. Необходимо выбрать такое значение интенсивности, при котором можно будет оценить и сравнить

работу всех скриптов. Это должно быть такое значение, при котором найдутся скрипты, не использующие все предложенные ресурсы, т.е. можно будет провести сравнение потребляемых, разными скриптами, ресурсов.

Для выбора оптимального значения была проведена предварительная серия экспериментов, в ходе которой интенсивность нагрузки постепенно наращивалась.

Перед началом экспериментов были зафиксированы значения используемых ресурсов. При нулевой нагрузке, т.е. при отсутствии с сервером активных соединений загрузка процессора составила около 0%, использование памяти – 433 Mb, время отклика – меньше 1 ms. При среднесуточной нагрузке использование ресурсов составило: процессор – 28%, оперативная память – 450 Mb, время отклика – меньше 1 ms.

В ходе проведения экспериментов был зафиксирован размер потребляемых различными скриптами ресурсов (табл. 9). Все скрипты потребляют примерно одинаковое количество ресурсов. Это показывает, что в данном случае не выявлено скриптов, требующих отдельного внимания. Этот результат ожидаем, так как Wordpress является одним из лидеров среди систем управления содержанием.

Анализ промежуточных результатов экспериментов показал, что самым ресурсоемким процессом является процесс web-сервера. Основную нагрузку этот процесс создает при генерации динамических страниц при помощи интерпретатора языка PHP. Были проведены дополнительные тесты со статичными файлами, как и ожидалось, установлено, что работа со статическими файлами использует гораздо меньше ресурсов сервера, даже при максимальной нагрузке при нормально функционирующем и настроенном сервере. Выяснив, что в данном случае основную угрозу несут именно динамические страницы, необходимо в случае обнаружения атаки включить кэширование и тем самым снизить нагрузку. Если бы по результатам экспериментов было установлено, что основную нагрузку генерирует, к примеру, сервер баз данных, можно было бы рекомендовать

перенести его на отдельный физический или виртуальный сервер. Знание уязвимых мест позволяет системному администратору заранее, не дожидаясь начала атаки, оптимизировать работу скриптов и программного обеспечения, включить средства кэширования и т.д. Кроме того, аппаратные и программные средства, которые используются для раннего обнаружения DDoS-атак, могут быть настроены в соответствии с уровнем уязвимости конкретных скриптов. Например, у более уязвимых скриптов можно задать повышенную чувствительность к атаке.

Таблица 9

Потребление скриптами ресурсов сервера при проведении DDoS-атаки

№ п/п	Страница	Использование памяти (Mb)	Загрузка процессора (%)	Время отклика (ms)
1.	index.php *главная страница*	475	50	<1
2.	index.php?p=1 *страница с записью*	479	57	<1
3.	wp-comments-post.php *добавление комментария*	467	52	<1
4.	wp-login.php *авторизация*	482	49	<1
5.	index.php?s=search_text *поиск*	492	53	<1
6.	indx.php?feed=rss2 *RSS лента*	483	51	<1
7.	index.php?m=201205 *архив за месяц*	470	54	<1
8.	readme.html *статичный файл*	450	27	<1
9.	readme.html *тоже при максимальной нагрузке*	459	38	3

Если оптимизировать работу определенных скриптов не представляется возможным, то при обнаружении атаки можно отключить

скрипты, создающие максимальную нагрузку. Например, при обнаружении атаки можно автоматически блокировать работу скрипта регистрации новых пользователей. С одной стороны, новые пользователи не будут иметь возможности зарегистрироваться, но с другой – такая мера позволит сохранить доступность ресурса.

На следующем этапе эксперимента к системе управления содержанием Wordpress было подключено несколько модулей сторонних разработчиков. После чего серия экспериментов была проведена повторно. В результате был зафиксирован значительный рост нагрузки со стороны некоторых скриптов (табл. 10)

Из результатов эксперимента видно, что максимальную нагрузку генерирует скрипт работы с комментариями. При детальном рассмотрении подключенного дополнительного модуля, отвечающего за ранжирование комментариев пользователей, были обнаружены ошибки при проектировке таблиц в базе данных, используемых этим модулем. В таблицах не был указан первичный ключ, кроме того, использовалось значительное количество запросов к базе данных в рамках запуска одной копии скрипта. В результате чего web-сервер и сервер баз данных начали использовать большее количество ресурсов. Ошибки при разработке этого модуля, как видно из таблицы результатов, также наложили отпечаток и на работу других скриптов.

Таблица 10

Потребление скриптами ресурсов сервера при проведении DDoS-атаки

№ п/п	Страница	Использование памяти (Mb)	Загрузка процессора (%)	Время отклика (ms)
1.	index.php *главная страница*	540	51	<1
2.	index.php?p=1 *страница с записью*	530	62	<1
3.	wp-comments-post.php *добавление комментария*	691	78	2
4.	wp-login.php *авторизация*	444	49	<1
5.	index.php?s=search_text *поиск*	492	51	<1
6.	indx.php?feed=rss2 *RSS лента*	483	57	<1
7.	index.php?m=201205 *архив за месяц*	491	50	<1
8.	readme.html *статичный файл*	450	28	<1
9.	readme.html *тоже при максимальной нагрузке*	462	38	3

В рамках исследования уязвимостей системы управления содержанием Wordpress была выработана следующая методика по обнаружению уязвимостей web-ресурсов и систем управления содержанием:

1. Получение списка всех возможных URL-адресов web-ресурса.
2. Обработка полученного списка. Исключение однотипных страниц, генерируемых одним и тем же скриптом при использовании одних и тех же ресурсов.
3. Замер основных параметров сервера: загрузка процессора, использование памяти, время отклика и т.д., соответствующих нормальной работе сервера.

4. Выбор значения интенсивности нагрузочного теста.
5. Проведение тестовых атак на выбранные скрипты. Фиксация результатов.
6. Обработка результатов, выделение уязвимых мест.

После проведения указанного исследования необходимо оптимизировать работу обнаруженных, уязвимых скриптов и повторить исследование, необходимое количество раз. Это позволяет на каждом шаге выявлять новые уязвимости и увеличивать стойкость сервера к будущим атакам. На каждом новом шаге будут определяться другие скрипты, расходующие ресурсов больше остальных. Процесс оптимизации можно считать законченным, когда все скрипты потребляют примерно одинаковое количество ресурсов и сократить это потребление уже не представляется возможным.

4.6. Выводы по четвертой главе

Для практической апробации программного комплекса, равно как и методики, на базе которой он был разработан, создана специализированная сеть для проведения нагрузочных тестов, имитирующих реальные DDoS-атаки. Всего в рамках экспериментов по тестированию и апробации разработанного программного средства в нагрузочной сети проведено около 300 нагрузочных тестов. Данные тестов подтверждают работоспособность и эффективность разработанного программного комплекса для противодействия DDoS-атакам и их обнаружения.

В рамках экспериментов проведено сравнение разработанного программного комплекса с существующими аналогами. Установлено, что разработанное средство является более эффективным. Кроме того, разработанное средство показывает лучшие результаты по обнаружению атак по сравнению с результатами, достигнутыми в аналогичных исследованиях.

При проведении нагрузочных тестов связанных с оценкой работы разработанного программного комплекса, также проводилось исследование самих DDoS-атак. Был выявлен ряд особенностей в поведении аппаратно-

программного комплекса, в отношении которого осуществляется атака. Разработана методика по обнаружению потенциальных уязвимостей в системах управления содержанием к атакам типа http-flood.

По итогам внедрения разработанного программного комплекса проведена апробация работы в реальных условиях на пяти различных площадках и четырнадцати серверах. В целом результаты работы в реальных условиях соответствуют результатам, полученным по итогам тестирования в нагрузочной сети.

Заключение

В данной работе предложена методика раннего обнаружения начала DDoS-атаки и последующего определения вредоносных запросов. В основе разработанных методик лежат методы теории вероятности, кластерного и статистического анализа, принципы машинного обучения.

В качестве основных результатов диссертационной работы можно выделить следующие:

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 различных сетевых ресурсов и их защиты от атак различных типов.
8. Для апробации результатов диссертационной работы и проведению 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.

Результаты диссертационной работы соответствуют целям и задачам, поставленным во введении.

На основании методики, предложенной в диссертационной работе, разработано два программных средства:

1. **Основное – «Система раннего обнаружения DDoS-атак и вредоносного трафика».**

Свидетельство о государственной регистрации в реестре программ для ЭВМ № 2013617238 от 06 августа 2013 (Приложение 1).

2. **«Система управления сжимающим прокси сервером».**

Свидетельство о государственной регистрации в реестре программ для ЭВМ № 2013660609 от 12 ноября 2013 (Приложение 1).

Разработанные программные средства активно внедряются на площадках различных уровней и форм собственности (Приложение 2). Среди уже внедренных можно выделить крупные региональные и всероссийские ресурсы:

- Региональное Информационное агентство «Атмосфера».
- Новостной портал Сибиркого Федерального округа – «Сибинфо».
- Средство массовой информации «Коррупции – нет».

По результатам внедрения разработанных программных средств в среднем достигнут 20-процентный экономический эффект, связанный с экономией средств выделяемых на обеспечение информационной безопасности. Экономия заключается в возможности отказаться от подписки на услуги внешних систем по фильтрации трафика и распределенной доставки контента (CDN-сетей). В четыре раза увеличена доступность защищаемых ресурсов. В пять раз увеличена скорость реакции персонала на начавшуюся атаку.

Разработанная методика и программное средство «Система раннего обнаружения DDoS-атак и вредоносного трафика» были высоко оценены

профессиональным сообществом. В 2013 г. разработанное программное средство было представлено на региональной выставке в Алтайском крае – «IT-форум – 2013», и заняло первое место [93]. По результатам краевого профессионального «Конкурса IT-проектов», в 2013 г., программное средство также было удостоено первого места [94].

В перспективе на основе разработанной методики планируется создание программного средства для обнаружения и противодействия DDoS-атакам на уровне маршрутизатора.

Практическая значимость результатов диссертационной работы заключается в возможности использования не только для обнаружения и противодействия широкому спектру атак, но и применения в других областях. Например, для определения различного спама, попыток подбора паролей и т.д.

Апробация результатов диссертационной работы проводилась на десяти научно-технических конференциях различного уровня, в том числе на международных и специализированных конференциях, посвященных вопросам информационной безопасности. Основные результаты, полученные автором в рамках данной диссертационной работы, отражены в 15 научных публикациях, пять из которых в ведущих рецензируемых журналах, рекомендованных для публикации ВАК.

Результаты, полученные в диссертационной работе, и разработанная методика используются в учебном процессе в ведущих вузов Алтайского края: ФГБОУ ВО «Алтайский государственный технический университет им. Ползунова» и ФГБОУ ВО «Алтайский государственный университет», а также при проведении научно-исследовательских работ (Приложение 2).

Список литературы и электронных ресурсов

1. DDoS-атаки [Электронный ресурс] / URL: http://localname.ru/soft/ataki-tipa-otkaz-v-obsluzhivanii-dos-i-raspredelennyiy-otkaz-v-obsluzhivanii-ddos.html
2. Предотвращение атак с распределенным отказом в обслуживании (DDoS): [Электронный ресурс] / Официальный сайт компании Cisco / URL: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html
3. DDoS-атаки второго полугодия 2011 г. [Электронный ресурс] / URL: http://www.securelist.com/ru/analysis/208050745/DDoS_ataki_vtorogo_polugodiya_2011_goda
4. DDoS-весна в Рунете [Электронный ресурс] / URL: http://www.securelist.com/ru/blog/207768876/DDoS_vesna_v_Runete
5. Хакеры атаковали сайт биржи Nasdaq [Электронный ресурс] / URL: http://lenta.ru/news/2012/02/15/block/
6. Одна из самых больших DDoS-атак в истории [Электронный ресурс] / URL: http://habrahabr.ru/post/174483/
7. Россия — главный источник всех кибер-атак [Электронный ресурс] / URL: http://www.amic.ru/news/211097/
8. В день выборов в Рунете бесчинствовали хакеры [Электронный ресурс] / URL: http://lenta.ru/articles/2011/12/05/upalo/
9. Сайт телекомпании НТВ вновь подвергается DDoS-атаке [Электронный ресурс] / URL: http://www.amic.ru/news/175831/
10. DDoS-атаки первого полугодия 2013 года [Электронный ресурс] / URL: http://www.securelist.com/ru/analysis/208050810/DDoS_ataki_pervogo_polugodiya_2013_goda
11. Prolexic о II квартале: DDoS становятся все более мощными [Электронный ресурс] / URL: http://threatpost.ru/2013/07/23/prolexic_o_ii_kvartale_ddos_stanovjatsa_vse_boleje_moshchnymi/

12. Сразу у нескольких новостных алтайских сайтов возникли технические проблемы [Электронный ресурс] / URL: http://amic.ru/news/183654/
13. Диаграмма мощности DDoS-атак [Электронный ресурс] / URL: http://www.securelist.com/ru/images/vlill/ddos_sept2013_pic08.png
14. Заседание коллегии Федеральной службы безопасности [Электронный ресурс] / URL: http://kremlin.ru/news/17516
15. Путин поручил ФСБ создать систему по борьбе с кибер-атаками [Электронный ресурс] / URL: http://www.amic.ru/news/205917/
16. В России появится новый род войск [Электронный ресурс] / URL: http://news.mail.ru/politics/13789078/?frommail=1
17. Сайт Алтайского Заксобрания подвергается DDoS-атакам [Электронный ресурс] / URL: http://www.bankfax.ru/news/88169/
18. Сайт amic.ru подвергся DDoS-атаке [Электронный ресурс] / URL: http://www.amic.ru/news/192772/
19. Xiang, Y. A Survey of Active and Passive Defence Mechanisms against DDoS Attacks : Technical Report, TR C04/02 *I* Y. Xiang, W. Zhou, M. Chowdhury. – Deakin University, Australia, 2004.
20. MittaI, P. Defense against Distributed Denial of Service Attacks : a seminar report. – Department of Computer Science and Engineering. Indian Institute of Technology, 2005. – 20 p.
21. Mirkovic J. A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms : Technical report #020018 I J. Mirkovic, J. Martin, P. Reiher. – Computer Science Department. University of California, 2002. – 16 p.
22. DNS Amplification Attacks [Электронный ресурс] / URL: http://www.securiteam.com/securityreviews/5GP0L00I0W.html
23. Amazon Elastic Compute Cloud [Электронный ресурс] / URL: http://aws.amazon.com/ec2/
24. Erik Nygren The Akamai Network: A Platform for High-Performance Internet Applications Ramesh K. Sitaraman, and Jennifer Sun. – ACM SIGOPS Operating Systems Review, vol. 44, no. 3, July 2010.

25. Cabrera, J.B.D. Proactive detection of distributed denial of service attacks using mib traffic variables – a feasibility study I J.B.D. Cabrera, L. Lewis, X. Qin et al. II Proc.of International Symposium on Integrated Network Management. Seattle, 14–18 May. 2001. – Piscataway: IEEE, 2001. – P. 609–622.

26. Ioannidis, J. Implementing Pushback: Router-Based Defense Against DDoS Attacks *I* J. loannidis, S.M. Bellovin *II* Proc. of Symposium of Network and Distributed Systems Security (NDSS). San Diego, 6-8 February 2002. - [S. 1. : s. п.], 2002.-P. 57-71.

27. Manajan, R. Controlling High Bandwidth Aggregates in the Network : ICSI Technical Report *I* R. Manajan, S.M. Bellovin, S. Floyd et al. - ICSI, 2001.-16

28. CoIIins, M. An Empirical Analysis of Target-Resident DoS Filters I M. Collins, M.K. Reiter If Proc. of 2004 IEEE Symposium on Security and Privacy (S&P'04). Oakland, May 9 –12, 2004. – Piscataway : IEEE, 2004. – P. 103–114.

29. Krishnamurthy, B. On network-aware clustering of Web clients I B. Krishnamurthy, J. Wang II Proc. of ACM SIGCOMM 2000. Stockholm 28 August – 1 September, 2000. – [USA]: ACM publishing, 2000. – P. 97–110.

30. Jin, C. Hop-count filtering: An effective defense against spoofed DDoS traffic *I* C. Jin, H. Wang, K.G. Shin *II* Proc. of 10th ACM Conference on Computer and Communications Security. Washington, October 27-30, 2003. - [USA] : ACM publishing, 2003. -P. 30-41.

31. Xuan, D. A Gateway-Based Defense System for Distributed DoS Attacks in High Speed Networks *I* D. Xuan, R. Bettati, W. Zhao *II* Proc. of 2nd IEEE SMC Information Assurance Workshop. West Point, NY, June, 2001. - Piscataway : IEEE, 2001.-P. 212-219.

32. Kang, J. Protect E-Commerce against DDoS Attacks with Improved D-WARD Detection System *I* J. Kang, Z. Zhang, J. Ju *II* Proc. of 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service. Hong-Kong, 29 March - 1 April, 2005. - Piscataway : IEEE, 2005. - P. 100-105.

33. Mirkovic, J. A Taxonomy of DDoS Attacks and Defense Mechanisms / J.Mirkovic, P. Reiher *II* ACM SIGCOMM Computer Communications Review. - 2004. - Vol. 34; no. 2. - P. 643-666.

34. Li, M. Decision Analysis of Statistically Detecting Distributed Denial-of-Service Flooding Attacks I M. Li, C Chi, W. Jia et al. II International Journal of Information Technology and Decision Making. - 2003. - Vol. 2; no. 3. - P. 397- 405.

35. Peng, T. Proactively Detecting DDoS Attack Using Source IP Address Monitoring I T. Peng, C. Leckie, R. Kotagiri II Networking 2004. Athens, Greece, May 9-14, 2004. - Berlin : Springer, 2004. - Vol. 3042. - P. 771-782.

36. Xiang, Y. An Active Distributed Defense System to Protect Web Applications from DDOS Attacks I Y. Xiang, W. Zhou // Proc. of Sixth International Conference on Information Integration and Web Based Application & Services (HWAS2004). Jakarta, Indonesia, 27-29 September, 2004. -[S. 1. : s. п.], 2004. -P. 559-568.

37. Wang, H. Detecting SYN flooding attacks I H. Wang, D. Zhang, K.G. Shin// Proc. of IEEE Infocom'2002. New York, 23-27 June, 2002. - Piscataway : IEEE, 2004.-P. 101-112.

38. Gorodetsky, V. Asynchronous alert correlation in multi-agent intrusion detection systems I V. Gorodetsky, O. Karsaev, V. Samoilov, A. Ulanov II Proc. of Autonomous Intelligent Systems: Agents and Data Mining International Workshop, AIS-ADM 2005. St.Petersburg, June 6-8, 2005. - Berlin : Springer, 2005. - Vol. 3685. - P. 366-379.

39. Щерба Е.В. Разработка системы обнаружения распределенных сетевых атак типа «Отказ в обслуживании» / Щерба Е.В., Волков Д.А. // «Прикладная дискретная математика. Приложение». – 2013. №6 – С.68-70.

40. Никишова А.В. Обнаружение распределенных атак на информационную систему предприятия / Никишова А.В., Чурилина А.Е. //

«Известия Южного федерального университета. Технические науки». – 2013. №12(149) – С.135– 143.

41. Корнев Д.А. Активные методы обнаружения SYN-flood атак / Корнев Д.А., Лопин В.Н., Лузгин В.Г. // «Информационная безопасность». – 2012. Т. 15, №2 – С.189– 196.
42. IBM Proventia Network Intrusion Prevention System (IPS) [Электронный ресурс] /URL: http://www.ibm.com/ru/services/iss/proventia_network_intrusion_prevention.html
43. Cisco Guard DDoS Mitigation Appliances [Электронный ресурс] / URL: http://www.cisco.com/web/RU/products/ps5888/index.html
44. Kaspersky DDoS Prevention [Электронный ресурс] / URL: http://www.kaspersky.ru/ddos-prevention
45. CloudFlare [Электронный ресурс] / URL: https://www.cloudflare.com/
46. Iptables Tutorial 1.2.2 [Электронный ресурс] / URL: https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
47. DDOS Deflate [Электронный ресурс] / URL: http://deflate.medialayer.com/
48. mod_evasive – защита от DOS и DDoS-атак [Электронный ресурс] / URL: http://muff.kiev.ua/content/modevasive-zashchita-ot-dos-i-ddos-atak
49. Модуль ngx_http_limit_zone_module [Электронный ресурс] / URL: http://nginx.org/ru/docs/http/ngx_http_limit_zone_module.html
50. Терновой О.С. Использование байесовского классификатора для получения обучающих выборок при определении вредоносного трафика на коротких интервалах / Терновой О.С., Шатохина А.С. // «Известия Алтайского государственного университета». – 2013. №1/2(74) – С.104–108.
51. Простой способ защиты от классического HTTP DDoS [Электронный ресурс] / URL: http://habrahabr.ru/post/151420/

52. Терновой О.С. Ранее обнаружение DDoS-атак статистическими методами при учете сезонности [Текст] /О.С. Терновой, А.С. Шатохин // Доклады Томского государственного университета. – 2012. – №1/2 (25) – С.104–108.

53. Терновой О.С. Снижение ошибки обнаружения DDoS-атак статистическими методами при учете сезонности [Текст] /О.С. Терновой, А.С. Шатохин // Ползуновский вестник. – 2012. – №3/2.

54. Сервис статистики LiveInternet [Электронный ресурс] / URL: http://www.liveinternet.ru/corp/about.html

55. Статистика сайта amic.ru [Электронный ресурс] / URL: http://www.liveinternet.ru/stat/amicru/

56. Статистика сайта yaplakal.com [Электронный ресурс] / URL: http://www.liveinternet.ru/stat/yaplakal.com/index.html

57. Рейтинг сайтов, все категории, Россия [Электронный ресурс] / URL: http://www.liveinternet.ru/rating/ru/

58. Статистика социальной сети «ВКонтакте» [Электронный ресурс] / URL: http://www.liveinternet.ru/stat/vkontakte.ru/index.html?date=2014-04-28

59. Алгоритмы кластерного анализа [Электронный ресурс] / URL: http://www.dea-analysis.ru/clustering-5.htm

60. Методы кластерного анализа. Итеративные методы. [Электронный ресурс] / URL: http://www.intuit.ru/studies/courses/6/6/lecture/184?page=5

61. Программное обеспечение SPSS [Электронный ресурс] / URL: http://www-01.ibm.com/software/ru/analytics/spss/

62. Мещеряков Р.В. Оценка информативного признакового пространства для системы обнаружения вторжений Мещеряков Р.В., И.А. Ходашинский, Е.Н. Гусакова // «Известия Южного федерального университета. Технические науки.» – 2013. №12(149) – С. 57–63.

63. Singh S., Silakari S. An ensemble approach for feature selection of Cyber Attack Dataset // International Journal of Computer Science and Information Security. - 2009. - Vol. 6, № 2. - P. 297-302.

64. Tavallaee M., Bagheri E., Lu W., Ghorbani A.A. A detailed analysis of the KDD CUP 99 data set // Proceedings IEEE international conference on computational intelligence for security. - Ottawa, 2009. - P. 53-58.

65. Dan Pelleg Accelerating Exact k-means Algorithms with Geometric Reasoning / Dan Pelleg, Andrew Moore // Carnegie Mellon University, Pittsburgh. – 2010.

66. Harry Zhang The Optimality of Naive Bayes / Harry Zhang // University of New Brunswick Fredericton, New Brunswick, Canada – 2004.

67. Бенкен Е.С. PHP, MySQL, XML. Программирование для Интернета [Текст] – СПб.: БХВ-Петербург, 2011.

68. TIOBE Programming Community Index for November 2013 [Электронный ресурс] / URL: http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html

69. What is MySQL? [Электронный ресурс] / URL: http://dev.mysql.com/doc/refman/5.6/en/what-is-mysql.html

70. January 2011 Web Server Survey [Электронный ресурс] / URL: http://news.netcraft.com/archives/2011/01/12/january-2011-web-server-survey-4.html

71. Log files [Электронный ресурс] / URL: http://httpd.apache.org/docs/2.2/logs.html

72. UNIX TIMESTAMP [Электронный ресурс] / URL: http://www.unixtimestamp.com/index.php

73. Щерба М.А. Обнаружение низкоактивных распределенных атак типа «Отказ в обслуживании» в компьютерных сетях: дис. … работа канд. тех. наук Омский гос. университет, Омск, 2012.

74. Терновой О.С. Имитация и исследование DDOS-атак в лабораторных условиях. Терновой О.С., Шатохин А.С. XIX Всероссийская научно-методическая конференция Телематика , Санкт-Петербург, 2012.

75. Терновой О.С. Обнаружение источников вредоносного трафика DDoS-атак методами статистического анализа. В кн.: Материалы XV Региональной конференции по математике, Барнаул, июнь, 2012. С. 80
76. Apache JMetr [Электронный ресурс] / URL: http://jmeter.apache.org/
77. Debian [Электронный ресурс] / URL: http://www.debian.org/index.ru.html
78. DistroWatch Page Hit Ranking [Электронный ресурс] / URL: http://distrowatch.com/dwres.php?resource=popularity
79. Дистрибутивы GNU/Linux, основанные на Debian [Электронный ресурс] / URL: http://www.debian.org/misc/children-distros
80. About WordPress [Электронный ресурс] / URL: http://wordpress.org/about/
81. About Clonezilla [Электронный ресурс] / URL: http://clonezilla.org/
82. 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). – С. 123–126.
83. Терновой О.С. Методика обнаружения уязвимостей к DDoS-атакам систем управления контентом на примере системы Wordpress/ Терновой О.С., Шатохина А.С. // «Известия Алтайского государственного университета». – 2012. №1/2(71). – С. 104–108.
84. Мещеряков Р.В. Концепция защиты образовательного портала отрасли Мещеряков Р.В., Шелупанов А.А., Давыдова Е.М. // «Информационное противодействие угрозам терроризма». – 2005. №4. – С. 232–239.
85. Поисковая система mnoGoSearch для Windows – русская версия [Электронный ресурс] / URL: http://www.mnogosearch.org/winrus.html
86. О.С. Терновой, А.С. Шатохин Методики и средства выявления и противодействия угрозам информационной безопасности в контексте региональных web-ресурсов // Региональные аспекты технической и правовой защиты информации. – Барнаул: Издательство АлтГУ, 2013.

87. Родионов А.С. Анализ средств противодействия одному виду атак типа «отказ в обслуживании» // Родионов А.С., Шахов В.В. // «Вестник Новосибирского государственного университета. Серия: Информационные технологии». – 2008. Т. 6. №2. – С. 80–87.

88. Karagiannis K. DDOS: are you next? // PC Magazine, Ziff Davis Media Inc. – 2003. Т. 22. №1. – С. 79.

89. Sigmond S. DDOS attacks: precursor to digital terrorism // SIGMOND S., KAURA V. // SILICONINDIA – 2001. Т. 5. №11. – С. 60–62.

90. Соколов А.В. DDoS-атаки как форма политической активности // Соколов А.В., Кирилова Е.В. // Российский политический процесс в региональном измерении: история, теория, практика. – 2013. – С. 122–125.

91. Афанасьев А. DDOS: противостояние. Как происходят атаки и как их отражать // Системный администратор. Синдикат 13. М. – 2001. №1. – 2(122–123). – С. 59–61.

92. Ковалев Д.А. Классификация методов проведения DDoS-атак // Мир транспорт. – 2013. №1(45). – С. 130–134.

93. Состоялся VI Алтайский региональный ИТ-форум [Электронный ресурс] / URL: http://altapress.ru/story/117694

94. Названы имена победителей конкурса «Лучшие проекты информатизации–2013» [Электронный ресурс] / URL: http://www.it-alttpp.ru/news/forumnews/2013/10/07/782/

95. Эдгар Э. Петерс Хаос и порядок // Э.Э. Петерс – Москва:Мир, 2000 – 85с.

96. Родионов А.С. Анализ средств противодействия одному виду атак, типа «отказ в обслуживании» // Родионов А.С., Шахов В.В. // Вестник НГУ. Серия информационные технологии. – 2008. Т. 6. №2 – С. 80–87.

Приложение 1. Свидетельства о регистрации

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2013617238

«Система раннего обнаружения DDOS атак и вредоносного трафика»

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Алтайский государственный университет» (RU)***

Авторы: ***Терновой Олег Степанович (RU),***
Шатохин Александр Семенович (RU)

Заявка № **2013613076**
Дата поступления **17 апреля 2013 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***06 августа 2013 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2013660609

«Система управления сжимающим прокси-сервером»

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Алтайский государственный университет» (RU)***

Автор: ***Терновой Олег Степанович (RU)***

Заявка № **2013618593**
Дата поступления **23 сентября 2013 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***12 ноября 2013 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов

Приложение 2. Акты, подтверждающие внедрение

УТВЕРЖДАЮ
Ректор ФГБОУ ВПО «Алтайский государственный технический университет им. И.И. Ползунова»

_____ А.А. Ситников
«__» _____ 2013 г.

АКТ
о внедрении в учебный процесс ФГБОУ ВПО АлтГТУ результатов кандидатской диссертационной работы Тернового О.С. «МЕТОДИКА И СРЕДСТВА РАННЕГО ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЗУЛЬТАТЕ DDOS АТАК»

Комиссия в составе:

председатель: декан ФИТ Зрюмов Евгений Александрович,
члены комиссии: заведующий кафедрой ВСИБ Якунин Алексей Григорьевич,
доцент кафедры ВСИБ Шарлаев Евгений Владимирович,
доцент кафедры ВСИБ Загинайлов Юрий Николаевич

составила настоящий Акт о том, что результаты диссертационной работы Тернового О.С. используются в учебном процессе ФГБОУ ВПО АлтГТУ, в учебном курсе «Безопасность вычислительных сетей и их администрирование», читаемого для студентов, обучающихся по направлению Информационная безопасность. При проведении лабораторных работ, студенты исследуют и тестируют разработанные средства, алгоритмы и методики противодействия атакам направленным на отказ в обслуживании. Результаты диссертационной работы используются в научной исследовательской работе студентов кафедры ВСИБ ФГБОУ ВПО АлтГТУ.

председатель: декан ФИТ Зрюмов Е.А.
члены комиссии:
заведующий кафедрой ВСИБ Якунин А.Г.

доцент кафедры ВСИБ Шарлаев Е.В.

доцент кафедры ВСИБ Загинайлов Ю.Н.

УТВЕРЖДАЮ
Генеральный директор
ООО «Медиа группа «Сфера влияния»

_____ Кречетова О.П.
«07» февраля 2013 г.

АКТ
об использовании результатов кандидатской диссертационной работы Тернового О.С. «МЕТОДИКА И СРЕДСТВА РАННЕГО ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЗУЛЬТАТЕ DDOS АТАК»

Комиссия в составе: председатель О.П. Кречетова, члены комиссии ведущий инженер Билле А.А. составили настоящий акт о том, что в ООО «Медиа группа «Сфера влияния» внедрена методика обнаружения и противодействия DDOS атакам, с целью увеличения защищенности web-ресурсов компании.

ООО «Медиа группа «Сфера влияния» является учредителем ряда средств массовой информации, регионального и всероссийского уровней. Среди них: информационное агентство «Атмосфера», информационно-политический портал «Сибинфо», средство массовой информации «Коррупции.нет».В связи с высокой популярностью данных ресурсов их публичностью и спецификой, они периодически подвергаются атакам различных уровней.

Внедрение результатов кандидатской диссертационной работы О.С. Тернового, позволило:

- на ранних стадиях диагностировать начало атаки;
- увеличить скорость реакции на начавшуюся атаку в 4 раза;
- увеличить защищенность web-ресурсов компании;
- повысить доступность web-ресурсов, в течение атаки на 40%;

Как следствие, компанией были снижены затраты на обеспечение информационной безопасности и отказоустойчивости на 19%.

Ген. директор _____ Кречетова О.П.

Вед. инженер _____ Билле А.А.

УТВЕРЖДАЮ
Директор КАУ «Алтайский государственный Дом народного творчества»

_____Казанцева В.П.
«10» октября 2013 г.

АКТ
об использовании результатов кандидатской диссертационной работы Тернового О.С. «МЕТОДИКА И СРЕДСТВА РАННЕГО ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЗУЛЬТАТЕ DDOS АТАК»

Настоящим актом подтверждается, внедрение результатов кандидатской диссертационной работы Тернового О.С. на официальном сайте КАУ «Алтайский государственный Дом народного творчества».
Использование разработанных О.С. Терновым алгоритмов, позволило увеличить сопротивляемость сайта к различным сетевым атакам. А так же противостоять попыткам направленным на фальсификацию результатов онлайн голосований и опросов.
После внедрения разработанных алгоритмов, время доступности web-сервера, во время атак, увеличилось в 5 раз.

Ведущий методист Солдатова Ю.Н.

УТВЕРЖДАЮ
Ректор Алтайского
государственного университета
С.В. Землюков

19.09.13

АКТ
ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММЫ В РАБОТЕ
ТЕЛЕКОМУНИКАЦИОННЫХ СЛУЖБ

Настоящим актом подтверждается, что программа для ЭВМ **«Система раннего обнаружения DDOS атак и вредоносного трафика»** (свидетельство о государственной регистрации РФ **№2013617238 от 06.08.13** по заявке 2013613076 от 17.04.2013, авторы Терновой О.С., Шатохин А.С.) используется в работе отделов телекоммуникации и защиты информации. Программа производит мониторинг трафика сервисов узла связи Алтайского государственного университета.

Начальник управления Рязанов М.А.

Начальник отдела
защиты информации Широков И.М.

УТВЕРЖДАЮ
директор ООО «МЕМ»
_____ Потапов М. А.
«19» ноября 2013 г.

АКТ
о внедрении в рабочий процесс результатов кандидатской диссертационной работы Тернового О.С. «МЕТОДИКА И СРЕДСТВА РАННЕГО ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЗУЛЬТАТЕ DDOS АТАК»

Комиссия в составе:

председатель: М.А. Потапов
члены комиссии: Давыдов Е.С., Романова О.А.

Составили настоящий акт о нижеследующем:

Результаты диссертационной работы О.С. Тернового используются в рабочем процессе ООО «МЕМ», для обеспечения информационной безопасности корпоративного web-ресурса компании.

Техническое преимущество используемой работы состоит в автоматизации процесса реагирования на DDOS атаку. Выявление атаки на ранних стадиях и своевременное оповещение администратора, позволило увеличить скорость реакции на атаку в 4 раза. Увеличено время доступности и up-time web-сервера на 6%.

Достигнут положительный экономический эффект:

- сокращены расходы на обеспечения информационной безопасности и доступности сайта на 20%
- ликвидированы потери от упущенной выгоды, в результате невозможности клиентов воспользоваться ресурсом во время атаки

По итогам внедрения результатов диссертационной работы, удалось отказаться от услуг сторонних провайдеров CDN сетей. Что позволило повысить сохранность индивидуальных данных передаваемых клиентами.

председатель комиссии М.А. Потапов

зам. директора Е.С. Давыдов

вед. специалист Романова О.А.