Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Павлов
Никита Александрович

Повышение эффективности работы мультисервисной сети связи

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-45 80 01 «Системы, сети и устройства телекоммуникаций»

_____

Научный руководитель

Хацкевич Олег Александрович
доцент, канд. техн. наук

Минск 2015

Тема диссертации: Повышение эффективности работы мультисервисной сети связи.

Повышение эффективности включает различные факторы: повышение скорости передачи, оптимизация конфигурации сети, повышение защищенности сети. Последний фактор является черезвычайно важным для корпоративных сетей крупных компаний, банков и мультисервисных сетей, госорганов, также сетей всех силовых структур, таможенных органов, налоговых органов и т.д. По этой причине тема данной магистрской работы является актуальной. Данная работа посвящена исследованию способов повышения защиты мультисервисной корпоративной сети от внешнего воздействия. Одной из самых актуальных задач в сфере услуг предоставления информации является борьба с DDoS-атаками (от англ. DistributedDenialofService, распределённая атака типа «отказ в обслуживании»). Суть таких атак сводится к тому, чтобы всеми доступными способами уменьшить количество полезной нагрузки на ресурс, или вовсе сделать его недоступным.

Актуальность данной работы состоит в том что данная проблема возникла вместе с появлением сети интернет и становиться все более актуальной в связи с развитием и расширением корпоративных сетей связи. На рынке существуют открытые программные решения, которые могут справиться только с простыми случаями DoS-атак, но и с другими внешними воздействиями.

Магистерская работа посвящена изучению источников формирования нежелательного трафика их разновидностей и входных параметров на стороне сервера обработки запросов, а также созданию модели корпоративной сети, в которой присутствует веб-сервер, созданию алгоритма для отличия нежелательного трафика генерированного ботнетом.

Целью исследования является повышение качества фильтрации трафика от нежелательной нагрузки путем разработка модели обработки внешних запросов в телекоммуникационной корпоративной сети и усовершенствовании алгоритмов их фильтрации.

Анализ параметров и структуры модели корпоративной сети. Исследование данных, полученных в процессе моделирования, для создания алгоритма защиты информации на сети. Создание алгоритма фильтрации нежелательного трафика. Оценка эффективности разработанных алгоритмов.

Для решения поставленной задачи необходимо:

1) Изучить способы построения и моделирования корпоративных сетей связи в условиях мешающего воздействия;

2) Оценить существующие методы маршрутизации, с точки зрения обеспечения ими надежности;

3) Модернизировать ПО, позволяющее эффективно защитить корпоративные сети связи;

4) Разработать метод оценки алгоритма маршрутизации на сетях связи. Модернизировать ПО, позволяющее производить выбор наиболее защищенные модели;

5) Разработать помехозащищенный алгоритм маршрутизации сетей связи.

Практическая ценность полученных результатов заключается в том, что они позволяют при проектировании новых или модернизации имеющихся корпоративных сетей обосновано осуществить выбор маршрутизаторов с минимальными требуемыми параметрами производительности и безопасностиканалов связи с минимальной требуемой пропускной способностью!

Объектом исследования является:

Корпоративная сеть передачи данных, представленная во всех крупнейших информационных точках.

Предметом исследования станут алгоритмы методов фильтрации нежелательного трафика.

В рамках магистерской работы планируется получение актуальных научных результатов по следующим направлениям:

1. Исследование характера угроз в корпоративных сетях связи. Особенности DoS-Атак и методы борьбы с ними. Разработка алгоритма фильтрации нежелательного трафика.
2. Проведение обзора основного программного обеспечения, направленного на методы защиты корпоративных сетей от внешних воздействий, а также DoS-атак в частности.
3. Исследование вопросов маршрутизации в сетях связи уровня Tier 1 иTier2.
4. Защита автономных систем от DDoS атак.

В заключении будет сделана оценка полученных результатов внешних атак, выводы и некоторые рекомендации по применению программного обеспечения.

В основе организационной стратегии построения защищенной корпоративной сети передачи данных является комплексный подход к обеспечению информационной безопасности компании и вычислительных сетей рисунок 1.1. Надлежащее выполнение требований и предписаний законодательства и стандартов обеспечения информационной безопасности в части построения защищенных вычислительных сетей. Выбор и использование сертифицированных средств и аттестованных информационных систем и технологий построения и администрирования сети.

В условиях современного "технологического бума", увеличения пропускной способности каналов связи, уменьшения их стоимости и стоимости оборудования, сложно ограничить число используемых для построения КСПД технологий и инструментов. Но в любом техническом решении по организации КСПД должны быть

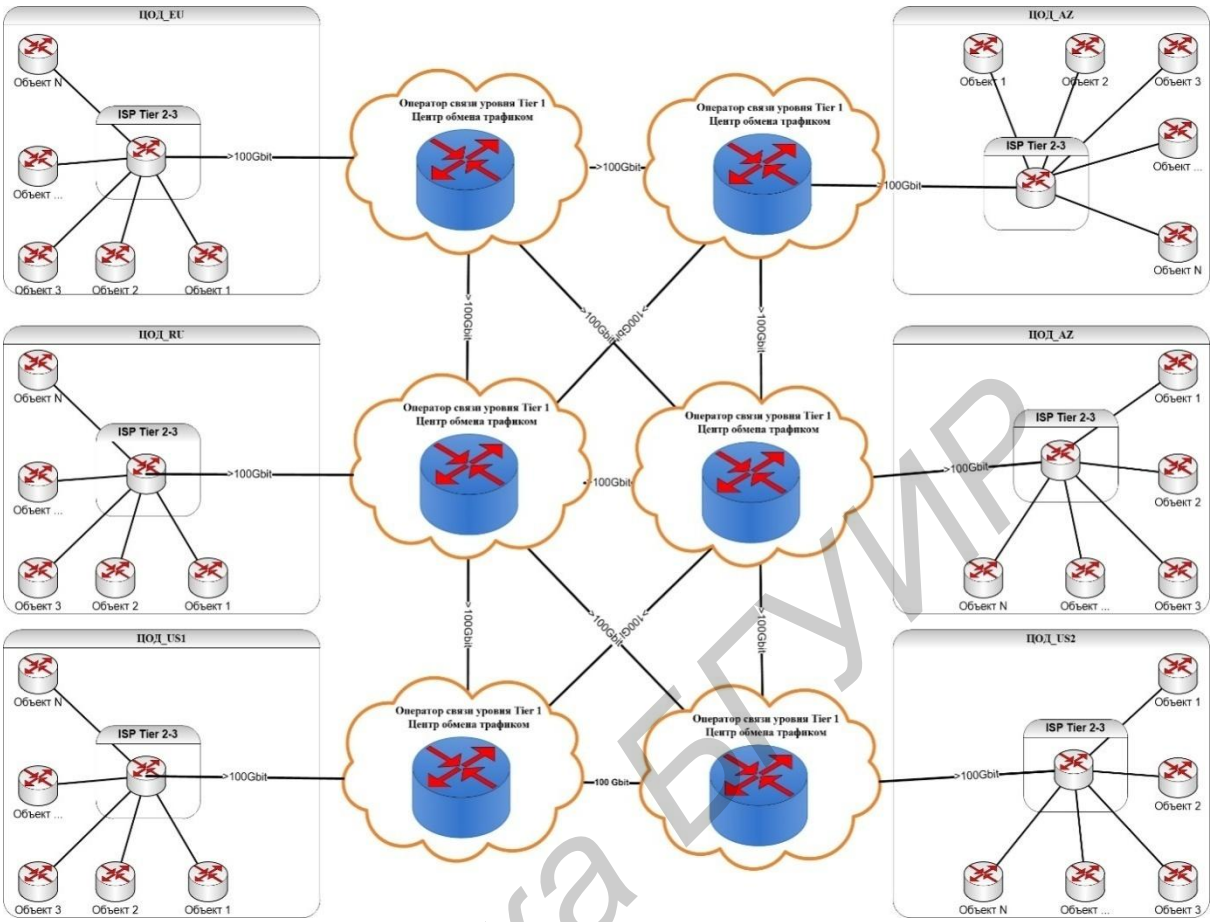

Рисунок 1.1 Схема организации передачи данных.

представлены базовые составляющие, принципы построения КСПД :

a) физическое резервирование каналообразующего оборудования (кластеризация) и каналов связи (дублирование) с целью минимизации времени простоев критически важных бизнес-сервисов (банкоматы, POS-терминалы, терминальный доступ сотрудников к фронт-офисным приложениям) в случае нарушения доступности сервис-провайдеров телекоммуникационных услуг;

b) определение приоритетов (приоритизация) различных типов трафика и требований по поддержанию единой политики передачи базирующихся на них критически важных сервисов (QoS) [13 РекомендацияITU-TY.1541]. для оптимального использования всей полосы пропускания каналов связи, представленных в КСПД в режиме 24x7.

Построим общую схему маршрутизации между нескольких AS, согласно исходным данным, в которых было отражено взаимодействие между множества ASN, как собственных так и частных. На рисунке 4.1 показа часть организованной схемы.

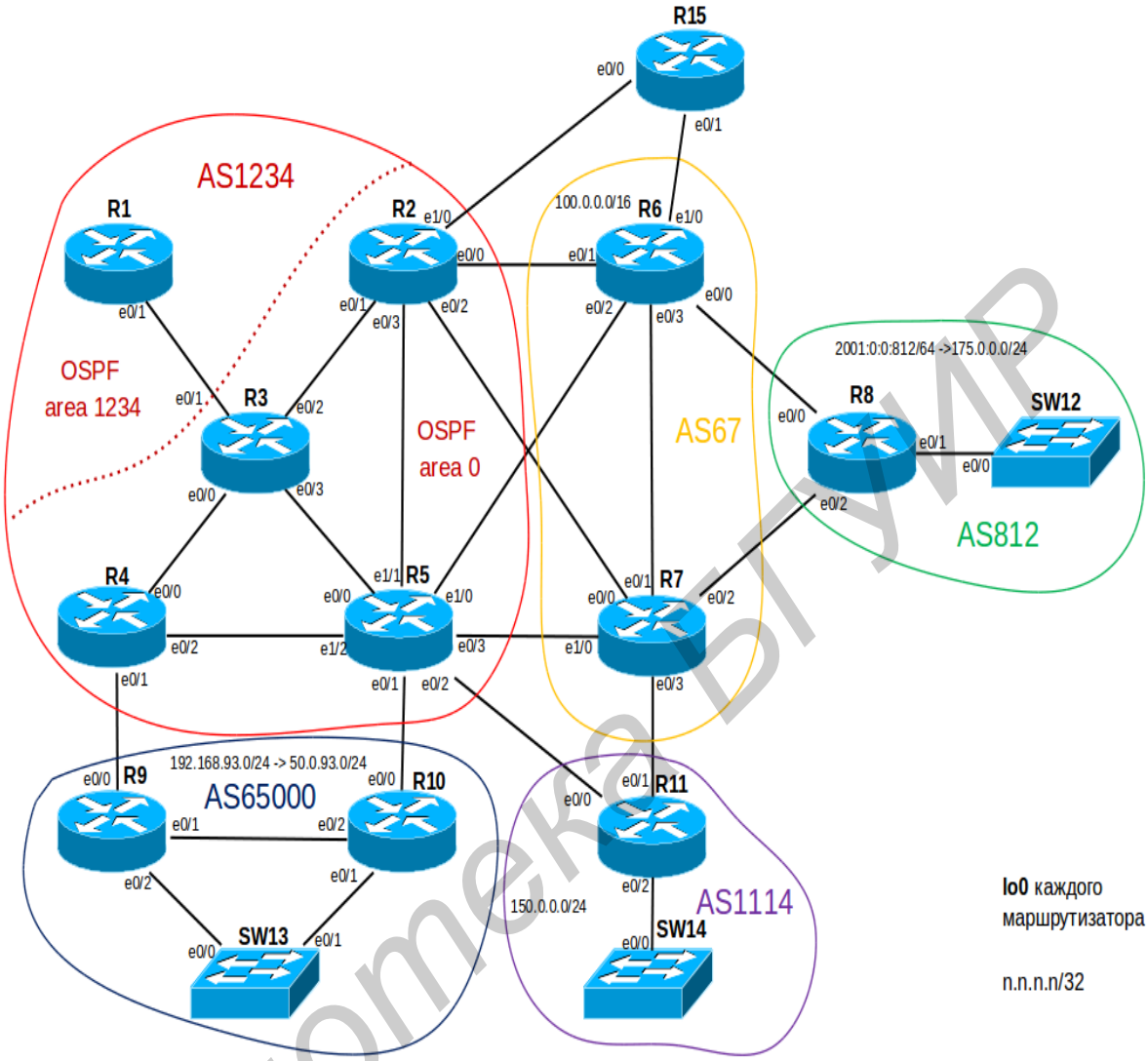

Рисунок 4.1 Общая схема маршрутизации сети взаимодействия ISP.

1. AS1234 – крупный провайдер ISP1. Владеет сетью 50.0.0.0/16;
2. AS67 – провайдер ISP2. Владеет сетью 100.0.0.0/16;
3. AS812 – клиент Customer1. Владеет блоком IP-адресов IPv4 175.0.0.0/24, но внутри своей сети использует исключительно IPv6;
4. AS65000 – клиент Customer2. Получает от провайдера блок адресов 50.0.109.0/24. Внутри сети использует приватные адреса из подсети 192.168.109.0/24. AS65000 — приватная;
5. AS1114 – клиент Customer3. Владеет блоком IP-адресов 150.0.0.0/24. Их же и использует для внутренних нод.

Для простоты на p2p линках между маршрутизаторами в разных AS будем использовать адреса вида 200.0.xy.0/24,

где x,y – номера маршрутизаторов, x>y.

p2p линки внутри провайдеров также будут иметь маску /24 (понятно, что это расточительство, но так будет значительно проще настраивать маршрутизацию) и вид 50.0.xy.0 (100.0.xy.0 для AS67),

где x,y – номера маршрутизаторов, x>y.

Конфигурирование корпоративной сети показало, что 100% универсальной защиты трафика по средствам BGP на сегодняшний день нет, но данный метод необходимо использовать по базовой защите от DDoSатак исключающий человеческий фактор.

В свете увеличения объемов мирового траффика неотъемлемым атрибутом является повышение активностиDoS/DDoS атак,в соответствии с полученными данными, был разработан способфильтрации на основании принадлежности блоков IP адресов определенному ASNпровайдеру/Дата Центру.

Данный способ весьма актуален в рассматриваемой корпоративной сети, так как рассматриваемая сеть организована и располагается на площадках уровня Tier 2 и Tier 3 и использует пиринговый трафик между собственными ЦОД по средствам Tier 1, к которому подключены мировые ЦОД Tier 2, т.е ЦОД оказываются в одной плоскости и менее защищены от атак. В работе по защите ЦОД от DDOSв исключения можно будет добавить собственные ЦОД, т.к генерация вредоносного трафика на их площадка исключена.

Основные подходы группировки IP по различным признакам:

1) Блокировка отдельных IP атакующих ботов;
2) Блокировка целых подсетей, к которым принадлежат боты;
3) Блокировка целых стран/городов, к которым принадлежат атакующие боты;
4) Блокировка всех IP адресов, кроме разрешенных явно;
5) Блокировка IP адресов на основании определенного алгоритма (включая использование специализированного аппаратного обеспечения);

Но при этом упускается еще один способ группировки (а следовательно и блокировки) IP адресов — их принадлежность к автономным системам (ASN). ASN это группа IP адресов, которые обслуживаются одним провайдером либо Дата Центром. Условно, это более высокий уровень иерархии, следующий сразу за понятием сеть/подсеть, но имеющий организационное происхождение.

В результате проделанной работы разработано программное обеспечение по защите и методы оптимизации работы распределенных центров обработки данных высокой доступности уровня ISPTier 2 ASN, а также защиты площадок провайдера и конечных Вэб-серверов

Практическая ценность проекта состоит в том, что компания получила совершенную магистральную сеть между центров обработки данных с повышенным уровнем доступности, экономии входящего-исходящего трафика за счет сокращения DDoSатак, высоким уровнем утилизации оборудования за счет своевременного прекращения обработки вредоносного

трафика, а также автоматизация работы с приложениями оповещения угроз, и существенно сократить временные издержки на поиски решений и отражения DDoS атак.

Научная новизна темы данной магистерской диссертации заключается в усовершенствовании системы безопасности магистральных провайдеров связи от DDoS атак, а также анализе существующих угроз и из организации в сети Интернет их влияние на работу провайдеров уровня Tier 2-3. Было экспериментально доказано, что организация различных видов защиты от DDoS атак оправдана и целесообразна и положительно влияет на работу систем провайдера уровня Tier 2-3, в зависимости от размеров атак и поставленных задач атакующих .

В результате выполнения работы был разработан модуль и внедрена система автоматического обнаружения DDoS атак. Данный прикладной аппаратно-программный комплекс позволил отслеживать и анализировать сетевую активность на входном и выходном канале связи, и выполнять необходимые действия на организацию защиты площадок ASN провайдера.

Результаты работы докладывались наследующих конференциях:

1. XI БЕЛОРУССКО-РОССИЙСКАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ II Минск БГУИР 2015 ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 4-5 июня, 2015 года, Тема доклада: «Защита корпоративных сетей связи от внешних атак».