Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий

Кафедра измерительных информационных технологий

Проект допущен к защите

Зав. кафедрой

_____ Г.Ф.Малыхина

«____» _____ 2015 г.

ВЫПУСКНАЯ РАБОТА БАКАЛАВРА

Тема: Безопасность сети образовательного учреждения от внешних угроз

Направление: 10.03.01 Информационная безопасность

Выполнил студент гр. 43505/20 К.Н.Неронов

Руководитель, уч. степень, должность А.В.Милицын

Санкт-Петербург

2015 г.

Федеральное государственное автономное образовательное учреждение высшего образования

"Санкт-Петербургский политехнический университет Петра Великого"

Институт компьютерных наук и технологий

Кафедра измерительных информационных технологий

Утверждаю
"____" _____2015 г

Зав.кафедрой ИИТ *Малыхина Г.Ф.*

_____
подпись

ЗАДАНИЕ

на бакалаврскую работу

студенту группы 43505/20 Неронову К.Н.

1. Тема работы: «*Безопасность сети образовательного учреждения от внешних угроз»*

2. Срок сдачи: *18 июня 2015*

3. Исходные данные к работе:

Работа посвящена решению проблемы безопасности сети образовательного учреждения от внешних угроз.

4. Содержание расчетно-пояснительной записки (обзор подлежащих разработке вопросов):

- Анализ возможных угроз;
- Выбор комплекса мер по защите, существующей ЛВС от внешних угроз;
- Реализация комплекса мер по защите, существующей ЛВС.

5. Перечень графического материала:

-Рисунки;
-Таблицы.

6. Дата выдачи задания:

26 февраля 2015

Научный руководитель доц. Милицын А.В.

Задание принял к исполнению"_____"_____2015 г

_____
подпись студента

РЕФЕРАТ

С. 32, Табл. 3, Рис. 5, Прил. 3

ЗАЩИТА СЕТИ, АТАКА НА ЛОКАЛЬНУЮ СЕТЬ, ПРОГРАМНО-АППАРАТНОЕ РЕШЕНИЕ ЗАЩИТЫ , ПРОКСИ-СЕРВЕР, SQUID.

Целью данной дипломной работы является выбор и настройка необходимого программно-аппаратного решения обеспечивающего безопасность локальной сети образовательного учреждения от внешних угроз, поступающих из глобальной сети.

В бакалаврской работе должен произведен выбор оптимальной защиты для сети образовательного учреждения отвечающий необходимым критериям.

ABSTRACT

NETWORK SECURITY, ATTACK ON LOCAL NETWORK, SOFTWARE AND HARDWARE SECURITY SOLUTION, PROXY, SQUID.

The aim of this thesis is to choose and configure the necessary hardware and software solution provides the security of the local network of educational institutions from external threats coming from the global network.

The bachelor work made the choice of optimal protection for the network of educational institutions meet the necessary criteria.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение информационной безопасности на сегодняшний день является одной из приоритетных задач системного администратора обслуживающего локальную сеть, подключенную, в свою очередь, к глобальной сети. К сожалению, сеть является не только удобным средством коммуникации и обменом информации, но и местом постоянной опасности, в котором можно стать жертвой разнообразных сетевых атак. Большая часть угроз связана с несовершенством стека протоколов TCP/IP. Так как эти протоколы были разработаны в то время, когда проблема обеспечение информационной безопасности не стояла так остро, это привело к ряду уязвимостей, которыми пользуются злоумышленники для проведения сетевых атак.

Огромное количество угроз порождает огромное количество методов и средств информационной защиты. В компьютерных сетях применяться различные технологии защиты: сетевые экраны, антивирусные средства, прокси-серверы.

Целью данной дипломной работы является выбор и настройка необходимого программно-аппаратного решения обеспечивающего безопасность локальной сети образовательного учреждения от внешних угроз, поступающих из глобальной сети.

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

DDoS (distributed denial of servise) – распределенный отказ в обслуживании.

DoS (denial of servise) – отказ в обслуживании.

FTP (file transfer protocol) – протокол передачи файлов.

URL (uniform resource locator) – унифицированный указатель ресурса.

ИБ – информационная безопасность.

МЭ – межсетевой экран.

ПО – программное обеспечение.

СЗИ – система защиты информации.

СКС – структурированная кабельная система

ЛВС – локальная вычислительная сеть

WAN – Wide Area Network (глобальная компьютерная сеть)

TCP/IP – Transmission Control Protocol/Internet Protocol

БП – блок питания

IP – Internet protocol (интернет протокол)

ПО – программное обеспечение

ПК – пользовательский компьютер

IT – Information technology (информационные технологии)

PoE (Power over Ethernet) – технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными, через стандартный сетевой кабель (витую пару) в сети Ethernet.

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ ЗАЩИТЫ ИНФОРМАЦИИ В ЛВС.

1.1 Основные понятия о локальных сетях

Локальная вычислительная сеть (Local Area Network) –сеть, которая соединяет компьютеры на небольшом расстоянии.

Компьютеры могут соединяться между собой, используя различные среды доступа:

- ✓ витая пара;
- ✓ беспроводные технологии;
- ✓ оптические кабели.

Проводные соединения устанавливаются через Ethernet, беспроводные - через Wi-Fi, GPRS, Bluetooth и прочие средства.

Отдельная локальная вычислительная сеть может быть соединена с другими сетями, а также быть частью глобальной сети.

Обычно локальные вычислительные сети построены на технологиях Ethernet или Wi-Fi.

Преимущество объединения компьютеров в локальную сеть:

- ✓ Разделение программных средств: создает возможность использования централизованных программных средств.
- ✓ Разделение ресурсов: - позволяет использовать одно устройство несколькими компьютерами, допустим, использование одного принтера отделом.
- ✓ Многопользовательский режим: дает возможность одновременное использование централизованных прикладных программных средств.

Сеть позволяет пользователям обмениваться между собой файлами, быстрыми сообщениями и ресурсами.

Используя современное коммуникационное оборудование можно

связать в компьютерную сеть большое количество пользователей.

Основные принципы построения ЛВС:

- ✓ Открытость - возможность подключения дополнительных устройств (компьютеров, периферии и других устройств) без внесения изменений в существующие компоненты сети;
- ✓ Гибкость - сохранение работоспособности сети при выходе из строя любого рабочего места или линии связи;
- ✓ Эффективность - обеспечение необходимого качества обслуживания пользователей при минимальных затратах.

В настоящее время локальные вычислительные сети также довольно широко используются в учебных заведениях различного плана. Благодаря технологиям локальных сетей становится возможным организация компьютерных классов в школах или вычислительных центров в институтах.

Использование ЛВС внутри университета, также, как и любого другого учебного заведения, позволяет выполнять следующие функции:

- ✓ Создание объединенного файлового пространства, которое может предоставлять всем пользователям информацию, созданную в разное время и в разном программном обеспечении для работы с ней.
- ✓ Повышение достоверности информации и надежности ее хранения путем создания устойчивой к сбоям и потери информации вычислительной системы, путем создания копий необходимых данных.
- ✓ Обработка документов и построения на базе этого действующей системы анализа, прогнозирования и оценки обстановки с целью принятия оптимального решения и выработки глобальных отчетов.
- ✓ Обеспечение быстрого прозрачного доступ к информации авторизованному пользователю в соответствии с его правами и привилегиями.

Таким образом, в настоящее время без локальной вычислительной сети невозможно представить себе эффективную работу даже самой скромной по размерам организации, а тем более учебного заведения, что приводит к необходимости использования компьютерной сети и соответственно обеспечении ее безопасности.

1.2 Основные понятия информационной безопасности.

При защите локальной вычислительной сети необходимо разобрать основные понятия и задачи в этой области.

Под информационной безопасностью понимается состояние защищенности информационной системы, включая как информацию, так и поддерживающее ее оборудование. Информационная система находится в состоянии защищенности, если обеспечена ее доступность, конфиденциальность и целостность.

- ✓ Доступность – это гарантия того, что авторизованные пользователи всегда получат доступ к необходимым данным.
- ✓ Конфиденциальность – это гарантия того, что защищаемая информация будет доступна только авторизованным пользователям на открытие и изменение этих файлов.
- ✓ Целостность – это гарантия что информация хранится в достоверном виде, т.е. информация которая защищена от неавторизованного изменения, модифицирования, подделки.

Информация, находящиеся как в локальной, так и в глобальной сети, постоянно подвергается различным видам угроз.

Угроза – действие, которое направлено на нарушение одного из пунктов защищенности безопасности.

1.3 Типы атак на локальную сеть извне.

Внешние угрозы на локальную сеть являются преступлением.

Различают следующие атаки, которые проводятся с целью нарушить безопасность или стабильность работы сети:

Сниффинг (прослушивание сети).

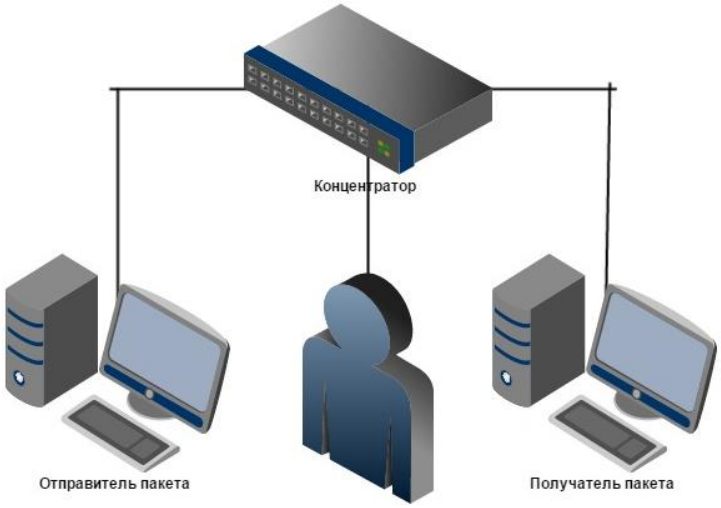

Рисунок 1- Сниффинг

Обычно данные передающиеся по компьютерным сетям не шифруются, что дает злоумышленнику, получившему доступ к сети передачи данных и имея сниффер (программный или программно-аппаратный комплекс) перехватывать пакеты данных (Рисунок 1) незаметно для пользователей сети. Так как некоторые сетевые приложения передают данные в незащищенном виде (POP3, Telnet, SMTP и другие) такая атака может нанести существенный вред локальной сети, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.). С помощью сниффера можно узнать какие типы данных передаются в сети, а также логины и пароли пользователей

Сканирование портов.

Используется для подготовки атаки на сеть или на определенный узел. С помощью сканирования портов можно выяснить возможные пути атак. Сам процесс сканирования представляет собой поиск UDP и TCP-портов, которые задействованы сетевыми сервисами на нужном компьютере для выявления их состояния. Такой процесс помогает понять, какие атаки будут успешными в данном случае. Кроме этого злоумышленник получает информацию о операционной системе пк, что позволяет лучше подготовится к атаке.

Атака-вторжения.

Целью данной атаки является перехват управления ресурсами сети. Это самый опасный тип вторжения, так как при успешной атаке злоумышленник получает практически всю информацию о системе. Атаки-вторжения используются для воровства конфиденциальных данных из локальной сети или подготовки к взлому подсетей данного предприятия или учреждения. К данной группе относится самое большое количество атак.

Отказ в обслуживании (Denial of Service)

Эта атака не всегда нацелена на получение контроля над сетью или получения доступа к информации в сети, главная цель такой атаки является вывод из работы сети или определенного ее компонента за счет превышения допустимых запросов, которые может обработать система. Таким образом узел сети или часть ее ресурсов становиться не доступной для авторизованных пользователей.

Большинство DoS-атак используют общие слабости сети, такие как открытые порты, использующиеся для соединения. Суть атаки заключаться в том, чтобы заблокировать все соединения, доступные для этих сервисов, огромным количеством запросов, которые сервис не в

состоянии обработать, не допуская к ресурсу обычных пользователей. Атака проводимая одновременно через большое количество сетевых узлов называется распределенной атакой отказа в обслуживании - DDoS (distributed DoS), изображена на рисунке 2.

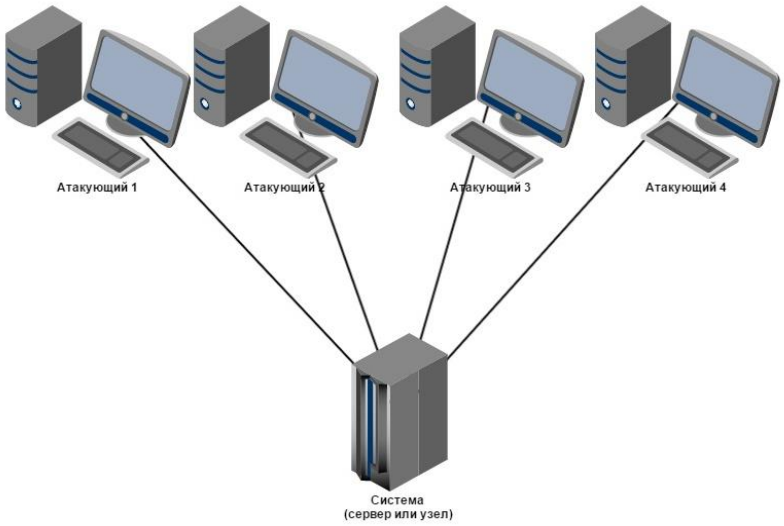

Рисунок 2 - Атака DDoS

Атака Ping Flooding

Ping это утилита проверяющая наличие и загруженность соединение в сетях TCP/IP.. Эта утилита отправляет эхо-запрос (Echo-Request) узлу сети и принимает ответ от него (Echo-Reaply). При выполнении команды учитывается время, которое проходит между отправкой и получением ответа от узла. Это время называется RTT (Round Trip Time). С его помощью рассчитывается задержи при доставке пакетов и частоту их потери. Сам запрос имеет длину в 64 байта, не считая заголовка(+20 байт). При огромной нагрузки на ЛВС, которые вызвана атаками злоумышленников, вызывает перегрузку линии, лишая возможности передавать полезные данные.

Протоколы заключенные в IP

В пакете IP есть поле, отвечающее за протокол пакета (ICMP, UDP, TCP). Злоумышленник при использовании нестандартного значения остается невидим для простейших средств контроля инфопотоков.

Атаки типа IP Spoofing

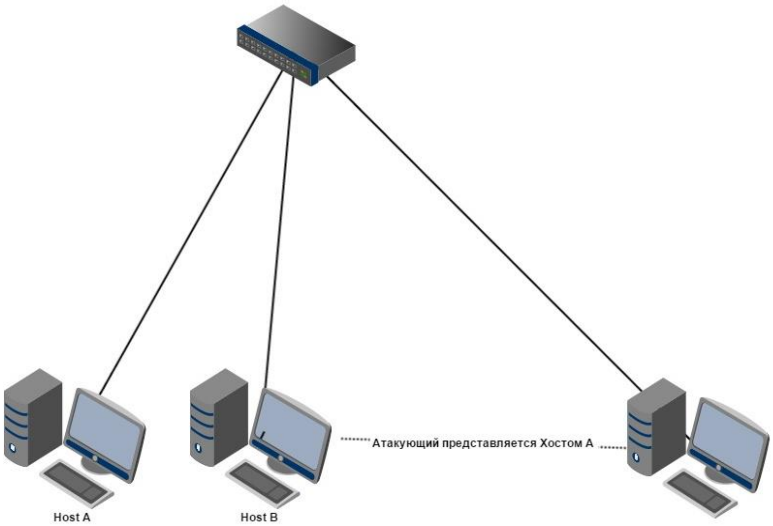

Рисунок 3- Атака типа IP Spoofing

Подмена исходного IP-адреса (Рисунок 3) –распространённая атака для скрытия источника другого типа атак. К атакам подобного рода относятся, и атака на системные журналы атакуя протокол Syslog. При атаке Syslog Spoofing на ПК жертвы передается сообщение от имени другого ПК из этой же сети, т.е. заметая следы и усложняя обнаружение источника атаки и уязвимости.

Вредоносные программы (вирусы, «черви», «троянские кони») - программы, скрывающиеся в других программных пакетах, несущие урон системе путем выполнения нежелательных функций.

Одним из типов вирусов является сетевой «червь», который перемещается по глобальной сети в поисках механизмы поддержки сети для определения узла, который подвержен заражению. Черви очень опасны так как целью

является не определенный компьютер, а вообще все компьютеры, подключенные к глобальной сети и имеющие необходимые уязвимости.
Также распространены «троянские кони» - это программы, которые имеют вид полезных приложений, а на деле выполняют вредоносные функции. Которые направлены на хищение данных, мошенничество или хулиганство. Эти функции активизируются в определенный момент (даты, состояния системы), либо по команде извне.

1.3 Вывод.

На основании вышесказанного можно сделать вывод, что глобальная сеть является опасной средой обмена информации и применение средств обеспечивающих информационную безопасность ЛВС является необходимым для корректной работы компьютерной сети любой организации и учебного заведения.

2. Обзор решений защиты локальной сети от внешних угроз.

Аппаратно-программный элемент системы защиты данных необходим для защиты ценных сведений, обрабатываемых и содержащихся в ПК, рабочих станциях, серверах, сетевых хранилищах, а также прочих устройствах, входящих в состав сети.

В этом дипломном проекте требуется разработать защиту компьютерной сети учебного заведения. В целях конкретизации задачи рассмотрим тщательнее методы защиты.

2.1.1 Межсетевые экраны

Сегодня работа учебных заведений жестко связано с Internet, а также с теми возможностями и сетевыми ресурсами, к которым она дает доступ. Именно поэтому вопрос подключать ли локальную сеть к Internet практически никогда не возникает. Наряду с этим возникает проблема, безопасной эксплуатации Internet, минимизируя риски для работы учреждения. Поэтому первоочередная задача — это обеспечить защиту ЛВС в плане внешних атак.

И эта сфера бурно и непрерывно развивается, причем крайне интенсивно. Основными методами защиты еще с давнего времени являются разнообразные сетевые экраны. Они дают базовый уровень защиты, они являются инструментами организации безопасности. Тот уровень защиты, которого позволяет добиться сетевой экран, может быть различен в зависимости от способа организации. Обычно используется политика компромисса между защитой, сложностью эксплуатации, ценой и т.д.

Модуль firewall заменяет роутер или шлюз, соединяющий ЛВС с миром. Безопасный сегмент сети организуется за ним. Пакеты, проходящие сквозь Firewall, обрабатываются отдельно, а не просто перенаправляются.

Пакеты, направленный модулям за пределами действия Firewall, не проходят. Поэтому потенциальный взломщик будет обязательно иметь проблемы с обходом Firewall.

Такая система проста и эффективна, защищая конкретную машину, их все в целом.

Недостатки системы FireWall обусловлены ее преимуществами, в итоге пользователь получает более сложный внешний доступ как для входящих, так и для исходящих пакетов информации. Для многих программных продуктов, которые функционируют с применением нетривиальных портов и без поддержки прокси-серверов, установка соединения в таком случае для них осуществляется с помощью открытия дополнительных портов. Это прибавляет дополнительные трудности, но без этого придется отказаться от использования подобных программ. Система FTP может и не проверяться, но если она имеется, доступ будет предоставляться только в FireWall-сервер и из него. Таким образом ПК в сети не смогут подключаться напрямую посредством FTP-связи ни с каким ПК извне. Выполнение процедуры telnet доступно только после входа на сервер. Обычно большинство межсетевых экранов не позволяют организовать внутренний ICMP-поток трафика внутрь сети.

2.1.2 Фильтрующие маршрутизаторы

Фильтрующие маршрутизаторы (ФМ) — это один из наиболее простых элементов межсетевого экрана. Маршрутизатор транспортирует информацию в разных направлениях между 2-мя (и более) различными сетями. Классический передает информацию из сети А и "направляет" его к целевой ЭВМ, которая находится в сети В. Проверяются многие параметры, как для отправляющей, так и для принимающей стороны. Кроме того, для организации полноценного отбора необходимым условием является тот фактор, поддерживает ли маршрутизатор изменение последовательности использования отдельных фильтров (для оптимизации отбора, это может порой привести к неверной смене, что даст разрешение на непреднамеренный доступ). Также следует проверить, есть ли возможность применять фильтры для передаваемых пакетов на отдельных интерфейсах в обоих направлениях. Когда маршрутизатор отфильтровывает лишь исходящие пакеты, тогда он будет внешним с точки зрения собственных фильтров и это делает его удачной целью для хакеров. Кроме такого изъяна маршрутизатора, это отличия фильтров, применяемых для входящих и исходящих данных, являются критически значимыми для маршрутизаторов с большим количеством интерфейсов. Еще один момент, заслуживающий внимания — возможность организовывать фильтрацию на основании данных заголовка IP и кондиций участков пакета.

2.1.3 Сетевые шлюзы

Сетевые шлюзы — это аппаратные или программные средства, приводящие в действие NAT.

NAT — процесс в сетях с протоколами TCP/IP, который дает возможность трансформировать IP-адреса проходящих пакетов.

Изменение адресов посредством NAT может быть выполнено практически любым сетевым приспособлением — для этой цели подойдет маршрутизатор, сервер обеспечения доступа, сетевым экраном. Принцип работы NAT основывается на замене обратных адресов во время передачи частей информации в одну из сторон и восстановлении конечного адреса в пакете, посылаемом в ответ. Вместе с исходящими и входящими адресами могут меняться и ID портов. NAT существенно уменьшает смысл создания уникальных IP для каждого информационного пакета. Это дает возможность подключиться к Internet организации с уникальной адресацией лишь в рамках локальной сети. Это достигается путём распространения данных адресов в глобально распределяемое пространство адресов. Кроме того, NAT может применяться для того, чтобы IP локальной сети вовсе не отображался.

Положительные стороны механизма NAT:

- ✓ Минимизирует потребность уникальных IP в глобальном плане, передавая несколько внутрисетевых IP-адресов для использования извне в качестве публичного IP (даже если передается несколько внутрисетевых адресов, их число все равно меньше).
- ✓ Предотвращает внешнее сообщение хостов сети, сохраняя возможность обратной связи (из сети во внешний мир). При установке соединения в самой сети организуется трансляция. Данный, поступающие в ответ извне, подгоняются под трансляцию и быстро проходят без проблем. Для всех пакетов,

которые идут извне, подобной трансляции нет, по этой причине у них не получится пройти.

Минусы NAT:

- ✓ Не каждый протокол поддерживает NAT.

  Существуют такие, которые не могут функционировать, если между сообщенными хостами происходит трансляция пакетных адресов (например, IPSec). Многие сетевые экраны, организующие трансляцию IP, могут помочь справиться с данной ситуацией, так как они могут изменить IP-адреса как в заголовках, так и не уровнях выше (к примеру, в для таких протоколов, как FTP).

- ✓ Трансляция адресов пакетов приводит к тому, что появляется связь «из многих в один» это чревато возникновением проблем авторизации клиентов сети. Поэтому нужно сохранять все сведения о проведении трансляций.

2.1.4 Прокси-сервера

Прокси-сервера являются инструментом, который меняет адресацию сети, проводя все запросы клиента через другой ПК. Как правило, имеется один компьютер с хорошо разработанной защитой, который выполняет функции прокси-сервера для комплекса протоколов (FTP, SMTP, Telnet, HTTP и прочих), однако существуют и персональные компьютеры для предоставления ряда прикладных услуг. Здесь не используется прямое подключение к глобальной сети, пользователь имеет доступ к прокси-серверу, задача данной машины состоит в настройке целевого соединения с внешней сетью. Существуют различные типы прокси-серверов, настраивать их конфигурации для пользователей можно таким образом, чтобы переадресация осуществлялась в автоматическом режиме, без предоставления соответствующей информации для клиента, который пытается наладить доступ. В ряде других случаев прокси-сервер может запросить подтверждение от клиента на подключение через него, и лишь после этого организовать подключение.

Использование прокси-серверов открывает большие возможности с точки зрения безопасности. Здесь можно добавить списки доступа к тем или иным протоколам, для той или иной категории клиентов. Также, в зависимости от требований пользователей, можно настроить определенную процедуру авторизации перед обеспечением доступа. При этом фильтрующий маршрутизатор можно настроить на открытие или закрытие доступа по протоколам FTP. Также имеется возможность наложить некоторые ограничения. Прокси-сервера можно настроить для обеспечения шифрования передаваемой информации, при этом гибкость такой настройки позволит применить широкий спектр криптографических. Перед этим следует активировать некоторые опции, чтобы функция передачи шифрованных данных между двумя ПК (один из которых внешний) была доступна. Межсетевые экраны, как правило, применяются

как инструмент блокировки хакерских атак, но кроме этого они не редко применяются и в качестве метода проверки регистрированных клиентов к ПК. Есть множество случаев, когда клиент не может получить стабильный доступ к требуемой информации в ответственные моменты. Это обусловлено тем, что порой выход в Internet обеспечивается через непроверенную ЭВМ или локальную сеть. Настроенный верно прокси-сервер дает доступ на узел лишь клиентам, отсеивая неавторизованных пользователей.

Сегодня лучшим межсетевым экраном признан тандем фильтрующего маршрутизатора и одного (при необходимости больше) прокси-сервера. Это дает возможность внешнему маршрутизатору запрещать все попытки применения нижнего IP-уровня в целях обхода безопасности (то есть блокировать IP-spoofing, подмену маршрутизации, неверное формирование пакетов). Кроме того, прокси-сервер обеспечивает защищенную работу протоколов высшего уровня. При использовании такой системы защиты достигается высокий уровень защиты сети.

Также важна степень отладки конфигурации система мониторинга запросов в локальной сети, ведь именно она дает права администратору определять все угрозы и своевременно их устранять.

Большая часть межсетевых экранов ведут протоколы, которые гибко регулируют, в целях создания наилучших условий для управления сетью. Данная система бывает централизованной, и настроена таким образом, чтобы предупреждать администратора в случае непредвиденных ситуаций. Постоянно следить за протоколами значит следить за безопасностью, а при обнаружении признаков хакерской атаки или попытки получить несанкционированный доступ — немедленно вмешиваться. Многие хакеры после взлома пытаются получить доступ и к журналам, чтобы скрыть следы своих действий, поэтому их следует хорошо защитить.

Типы применяемых фильтров. Межсетевые фильтры, функционирующие совместно с прокси-сервером, дают администратору

возможности регулировать потоки данных, идущие сквозь Firewall, однако они не отличаются высокой скоростью работы. Аппаратные устройства пропускать широкие потоки пакетов данных, однако они практически не настраиваются. Также существует уровень прокси, исследующий потоки данных, и после принимает решение, стоит ли их пропускать. При этом фильтрация работает на основе IP, ID портов, используемых интерфейсов и даже с учетом некоторых сведений из передаваемых пакетов.

Регистрация трансфера. Почти все Firewall оснащаются интегрированной системой записи сведений о всех операциях. При этом важно согласовать инструменты обработки лог-файлов и с системой их записи.

Администрирование. Многие Firewall оборудуются графической оболочкой. Более просты распоряжаются лишь файлами текстового типа. Стоит отметить, что многие Firewall позволяют работать удаленно.

Простота. Хороший Firewall — простой Firewall. Структура прокси-сервера не должна изменяться, а проверка его функционирования должна быть несложной.

2.2 Вывод

Рассмотрев разнообразие различных типов защиты, можем перейди к выбору и реализации защиты сети учебного заведения.

3. Выбор и реализация комплекса мер по защите существующей ЛВС от внешних угроз

3.1 Определение основных источников угроз информационной безопасности

Информационные ресурсы учебного заведения постоянно подвергаются угрозам из глобальной сети.

Наиболее важные данные внутри учебного заведения хранится в электронном виде и имеют ограниченное распространение, следовательно, к ним закономерно ожидать повышенный интерес со стороны злоумышленников.

Таким образом, локальная вычислительная сеть института должна быть защищена с учетом всех специфических особенностей хранимой информации, во внимания должны быть приняты угрозы, рассмотренные в первой главе.

3.2 Обоснование выбора средства защиты

В учебных заведениях достаточно часто возникают условия, когда, в локальных сетях большой поток пользователей, с одной стороны, пользуются ресурсами сети Интернет на разных компьютерах. Единовременно обеспечить достойный уровень безопасности, в данном случае, на компьютерах довольно нелегко. Также учебные заведения часто имеют пропускную способность канала, недостаточную для высокоскоростного доступа в Internet, скорость доступа к внешним ресурсам, в следствии чего, сильно снижается, это отображается на плохом качестве и скорости учебного процесса. Усиление пропускной мощности канала не устраняет полностью эту проблему. Такое происходит потому, что недостаточная скорость поставки Web-страниц вызвана

сопоставлением немалой протяженности сетей между пользователями и конечными ресурсами.

Для урегулирования этой проблемы требуется переместить данные ближе к пользователю, т.е. использовать промежуточный узел, который будет хранить копии популярных Web страниц внутри локальной сети

Кэширование дает возможность существенно повысить скорость доставки исходных данных и облегчить канал выхода в глобальную сеть.

Для защиты сети с выявленными особенностями мы будем применять кэширующий прокси-сервер совместно с роутером.

Роутером будет находится перед сервером и будет обеспечивать сеть доступом в интернет от двух провайдеров и фильтрацию трафика до обработки его сервером, таким образом облегчая его нагрузку

Кэширующий-сервер будет выступать своего рода посыльным между локальной сетью и Internet, который будет хранить в памяти часто запрашиваемые у пользователей Web-страницы. Кроме функции кэширования прокси-сервер, будет обеспечивать безопасность ЛВС.

3.3 Построение карты сети

Исходя из ранее выбранных способов защиты ЛВС, нарисуем структурную схему сети, рисунок 4.

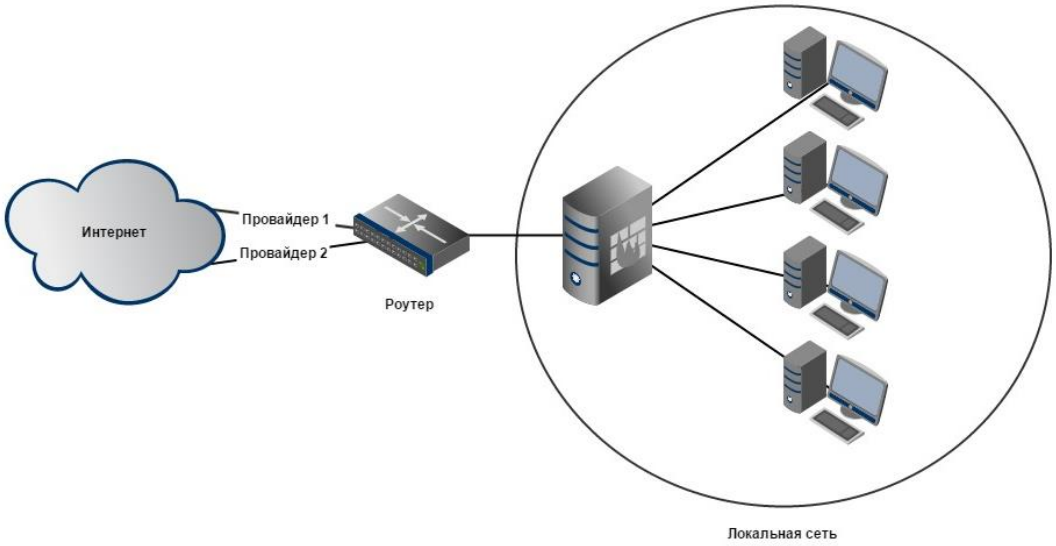

Рисунок 4-Карта сети

3.4 Выбор Роутера

Ранее мы выявили требования к данному устройству:

- ✓ Устройство должно быть промышленного класса для обеспечения бесперебойной работы
- ✓ Устройство должно иметь независимые Ethernet-порты, для организации работы двух провайдеров подключенных к локальной сети
- ✓ Устройство должно иметь быстрый процессор и широкие возможности по настройке внутреннего фаервола.

Под эти параметры нам подходит MikroTik RouterBOARD 2011L, рисунок 5.

Рисунок 5 - MikroTik RouterBOARD 2011L

Таблица 1 - Технические характеристики MikroTik RouterBOARD 2011L

Тип устройства	Router
Объем оперативной памяти	64 Мб
Количество портов	10 независимых Ethernet 10/100/1000 Мбит/сек
Процессор	600 мегагерцовый процессор Atheros MIPS 74K
управление	Консольнгый порт, веб-интерфейс, специальное ПО
Поддержка стандартов	Auto MDI/MDIX, Power Over Ethernet

Серия маршрутизаторов Mikrotik RB2011 - серия доступных многопортовых устройств.

RB2011iL-IN - модель с процессором Atheros AR9344 600MHz. Основное достоинство модели - пять 10/100Mbit FastEthernet и пять 10/100/1000Mbit Ethernet. Также 10й порт оснащен функцией PoE (Power over Ethernet), позволяющей передавать питание на подключённое устройство, если оно поддерживает питание по данному стандарту. Все характеристики представлены на таблице 1.

Также устройство поддерживает все функции и особенности RouterOS – специальной операционной системы разработанной производителем

маршрутизаторов.

Роутер поддерживает: динамические маршруты, хотспот, firewall, мониторинг в реальном времени и другие возможности.

Динамическая маршрутизация -это маршрутизация, применяемая для общения роутеров между собой. роутеры передают важную информацию о том какие сети к ним подключены.

Хотспот (Hotspot) – технология реализующие безопасное подключение гостевых пользователей к сети интернет, изолированно от ресурсов локальной сети.

Пример настройки двух провайдеров на роутере Mikrotik и применения правил фаервола изложены в приложениях А и Б.

3.5. Выбор и реализация прокси-сервера

Исходя из особенностей локальных сетей учебных учреждений, таких как приемлемая стоимость решения, высокая надежность и отказоустойчивость, мой выбор пал на апаратно-программный комплекс с использованием бесплатно распространяемого пакета Squid и надежного оборудования, которое позволит хранить большое количество кэшируемой информации.

3.5.1 Аппаратная составляющая

В качестве аппаратной базы для сервера была выбрана платформа Depo Storm 1160NT (Таблица 2) – готовое решение, рассчитанное на круглосуточную работу, имеющее большой жесткий диск для кэширования интернет страниц и процессор способный выдержать большую нагрузку.

Таблица 2 - Технические характеристики прокси-сервера:

Процессор	Xeon® E3-1200 v3
Чипсет:	Intel® C222
Память:	16Гб оперативной памяти по спецификации DDR3-1600/1333
Жесткие диски:	1 Тб
Сетевой интерфейс:	Двухпортовый интегрированный Gigabit Ethernet 1x Intel® i217LM
Система охлаждения:	1 вытяжной вентилятор , 1 вентилятор блока питания
Блок питания:	Блок питания мощностью 300Вт
Исполнение:	Отдельно стоящая башня – MiniTower. Размеры (ДВШ, мм) 425*362*184.
Расширение:	2 слота PCI-E 3.0

3.5.2 Программная составляющая

В качестве proxy- сервера была выбран сборный программный комплекс из операционной системы Debian, набора пакетов Squid для управление трафиком и визуальным интерфейсом Sams.

Debian - это свободно распространяемая, Unix-подобная, операционная система для компьютера, основной особенностью которой является стабильность и невосприимчивость вирусов Windows-подобных систем.

Squid - это решение широких требований к кэширующему и прокси серверу, которое масштобируемо для сетей от уровня небольшой локальной сети кафедры до сети большого научного комплекса. Squid является высокопроизводительным кеширующим прокси-сервер для клиентов, поддерживающий FTP и HTTP объекты данных. Одним из достоинств, является то, что он хранит кеш не только на HDD, но и часто обрабатываемые объекты находятся в быстром доступе – в оперативной памяти, среди этих объектов могут присутствовать сохраненные сайты и DNS адреса, что способствует увеличению скорости поиска необходимого ресурса в сети Internet.

Squid потребляет очень скромную часть ресурсов системы, что даёт возможность устанавливать его даже на самые посредственные конфигурации железа.

SAMS представляет собой программное средство для администрирования доступа пользователей к прокси-серверу SQUID

Состав Squid

Основным компонентом системы является кэширующий HTTP-сервер. Который предназначенный для организованного безопасного доступа студентов и преподавателей в интернет.

Принцип работы этого модуля прост - после запуска он начинает ждать запросы на порт прокси-сервера 3128. Для того чтобы пользователи могли получить доступ в интернет, им необходимо указать адрес HTTP прокси-сервер в настройках браузера.

Прокси-сервер принимает запросы от клиентов и генерирует ответ который основан на документах, сохранённых в локальном КЭШе. Он выступает в качестве сервера при приеме HTTP запросов от клиентов сети, и клиентом по отношению к удаленным серверам, с которыми он устанавливает контакт, когда не может ответить на запрос, используя данными из локального КЭШа.

Рассмотрим его работу более подробно. Когда Squid начинает работать, он находится в ожидания запросов от клиентов на специально назначенный порт. После получения запроса создаётся новый поток для каждого клиента. Поток обработки анализирует запрос.

Если запрос должен извлечь документ, тогда, документ копируется из КЭШа на компьютер клиента, при этом увеличивается на пункт число удачного использования кэша (cache hit).

Если же необходимого документа нет в КЭШе, тогда, запрос будет послан удалённому серверу, с которого запрашивается документ. При этом число неудачного использования КЭШа (cache misses), будет увеличено на единицу.

Клиенту передается ответ от удалённого сервера. В добавление к этому в случае удачного ответа на запрос и при условии, что данный сервер не находиться в списке доступных серверов к которым разрешен доступ без прокси-сервера, найденный документ будет сохранён в КЭШе на локальном диске.

Каждый раз при получении новой версии кэшируемого документа, она заменяет собой старую версию в КЭШе.

Squid может выполнять следующие функции:

– Запрет доступа к различным не желательным сайтам

– ведение журнала посещённых сайтов

– ограничение скорости доступа в интернет и т.д.

Как и большинство программных компонентов для Linux, Squid не имеет графического интерфейса настройки. Настройка параметров работы прокси-сервера производится из текстового конфигурационного файла, располагающегося \etc\squid\squid.conf.(Настройки предствленны в приложении В)

Для этого будет использована система SAMS, которая поможет вести контроль пользователей в привычном оконном режиме

SAMS (Squid Accaunt Management System) - это система для учета доступа пользователей через прокси сервер к ресурсам интернет. Всю работу по проксированию, кэшированию и перенапровлению берет на себя Squid, а SAMS занимается учетом трафика и управлением пользователями.

3.6 Вывод

После настройки данного программно-аппаратного комплекса мы можем визуально наблюдать как за активностью пользователей, так и видеть сообщения об угрозах(Рисунок 6).

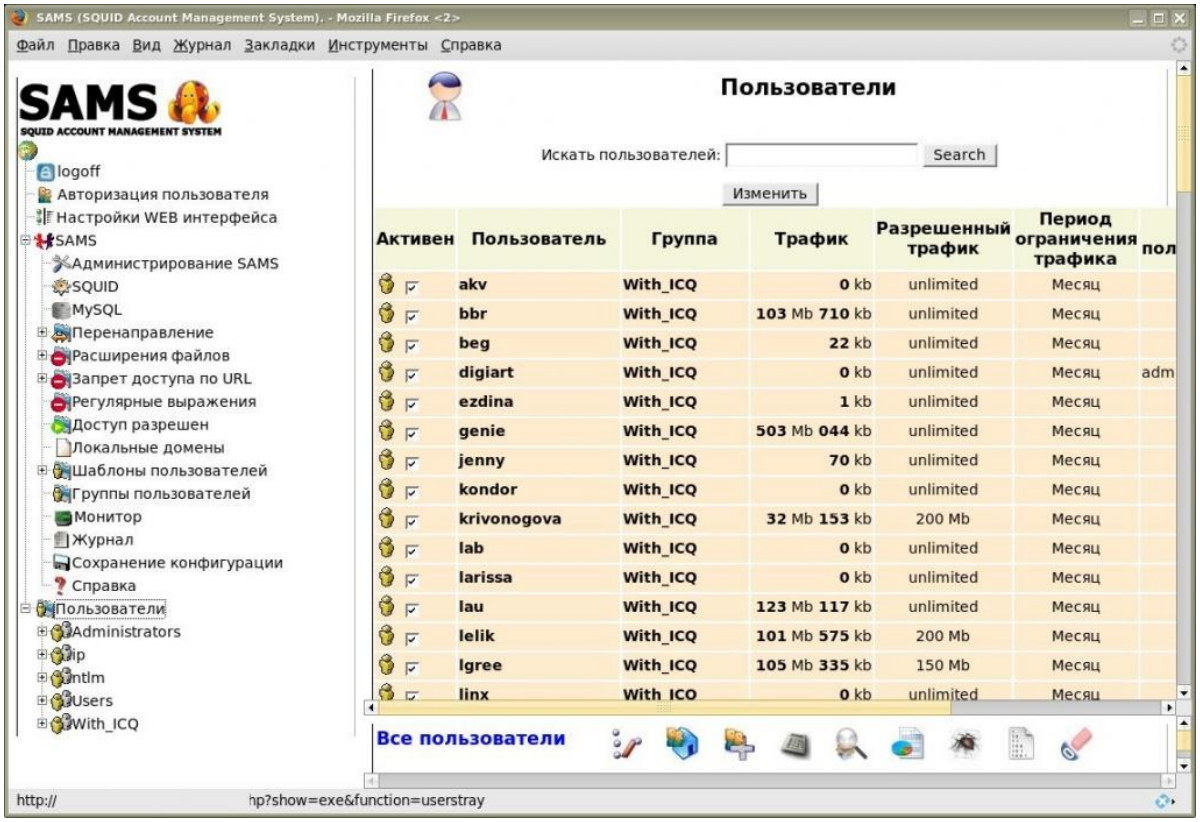

Рисунок 6- Окно Sams отображающее расход трафика по пользователям

.

ЗАКЛЮЧЕНИЕ

Данная дипломная работа посвящена обеспечению безопасности сети образовательного учреждения от внешних угроз. Для реализации данной задачи требовалось изучить возможные угрозы для ЛВС, а также выбрать решение обеспечивающее защиту, отвечающий необходимым критериям.
Также было подобрано программное обеспечение для прокси-сервера.
Таким образом, результаты проделанной мною работы полностью удовлетворяют заданию и данный дипломный проект можно считать удачно завершенным.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Безруков, Н.Н. Компьютерные вирусы / Н.Н. Безруков. - М.: Наука, 2011.- 345 с.- ISBN 978-5-0395-2489-243

2. Мостовой, Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. №4. 2010. – 104 с.

3. Кирсанов, Д. А. Понятный Internet. - М.: Символ-Плюс, 2011. – 198 с. – ISBN 978-5-0245-13590-4124-1

4. Мельников, В. А. Защита информации в компьютерных системах. – М.: Финансы и статистика, 2011. – 268 с. – ISBN 978-5-79469-3458-231

5. Максименков, А. В., Селезнев, М. Л. Основы проектирования информационно-вычислительных систем и сетей ЭВМ. –М.: Радио и связь, 2010. – 398 с. – ISBN 978-5-221-2359-131-001