МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем управления и информационных технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка системы обеспечения безопасности электронной почты корпоративной сети

Специальность Системы Информационной Безопасности_____

Выполнил(а) Аканов Тимур Ерикович_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель к.т.н., доцент кафедры СИБ Шайкулова Актоты Алиевна
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель кафедры СИБ Дмитриева Маргарита Валерьевна

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент кафедры БТИЭ Приходько Николай Георгиевич

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: ст.п.,Дмитриева Маргарита Валерьевна
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Рецензент: _____
(ученая степень, звание, Ф.И.О.)

_____ «_____» _____20____г.
(подпись)

Алматы 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем управления и информационных технологий

Кафедра «Системы информационной безопасности»

Специальность «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Аканову Тимуру Ериковичу
(Ф.И.О.)

Тема проекта «Разработка системы обеспечения безопасности электронной почты корпоративной сети»

Утверждена приказом по университету № 147 от «11» ноября 2019 г.

Срок сдачи законченного проекта «1» июня 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – Windows Server 2019, Маршрутизатор pfsense, DNS server, DHCP server, Windows Outlook 2019, Почтовые адреса сотрудников организации.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы – разработка системы обеспечения безопасности электронной почты корпоративной сети. Акцент делается на защите на уровне маршрутизации, средствами PFSENSE Задача создать black list, настройка антиспамовой фильтрации .

Основная рекомендуемая литература:
1.В. Олифер, Н. Олифер "Компьютерные сети. Принципы, технологии, протоколы;
2.Уильям Станек "Microsoft Windows Server 2012;
3.Справочник администратора, Крейг Хант, "TCP/IP — Сетевое администрирование".

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Проектирование корпоративной сети	17.02.2020 – 20.02.2020	
Настройка Windows Server 2012 AD	21.02.2020 – 28.02.2020	
Создание DNS , Dynamic Host Configuration Protocol .	01.03.2020 – 08.03.2020	
Создание виртуального маршрутизатора .	09.03.2020 - 18.03.2020	
Организация проверки подлинности, доверия.	19.03.2020 – 27.03.2020	
Организация защиты от спама. Антиспамовая фильтрация.	28.03.2020 - 07.04.2020	
Организация резервного копирования	08.04.2020 - 18.04.2020	
Настройка Windows Outlook	19.04.2020 - 30.04.2020	
Анализ рисков ИБ. БЖД	01.05.2020 - 09.05.2020	

Аннотация

В дипломном проекте была создана виртуальная корпоративной сеть, для передачи электронной почты. Показан практический способ реализации информационной безопасности при помощи настройки виртуального маршрутизатора.

В части, относящейся к расчету рисков, отображены показатели безопасности некоторых активов организации до и после внедрения разработанного проекта.

Раздел безопасности жизнедеятельности описывает основные требования, предъявляемые к помещениям, в которых будет использован проект, а также показаны расчеты требуемой величины освещенности и кондиционирования помещения.

Аңдатпа

Дипломдық жобада электрондық поштаны жіберу үшін виртуалды корпоративтік желі құрылды. Виртуалды маршрутизатор параметрлерін қолдана отырып, ақпараттық қауіпсіздікті жүзеге асырудың практикалық әдісі көрсетілген.

Тәуекелдерді есептеуге қатысты бөлігінде ұйымның жобаны іске асырғанға дейін және одан кейінгі кейбір активтерінің қауіпсіздік көрсеткіштері әзірленген.

Тіршілік әрекетінің қауіпсіздігі бөлімі жоба қолданылатын үй-жайларға қойылатын негізгі талаптарды сипаттайды, сонымен қатар жарықтандыру мен ауаны салқындатудың қажетті мөлшерін есептеуді көрсетелген.

Annotation

In the diploma project, a virtual corporate network was created for demonstration of a corporate e-mail. A practical way of implementing information security using virtual router settings is also shown at this project.

In the part related to risk calculation, safety indicators of some assets of the organization are displayed before and after the implementation of the developed project.

The labour safety section describes the basic requirements for the premises in which the project will be used, and also shows the calculations of the required amount of lighting and air conditioning.

Содержание

Введение

Электронная почта (электронная почта, электронная почта) является основным видом сетевого сервиса. После регистрации у провайдера пользователь, который получает «сетевое имя», получает «почтовый ящик», который является каталогом на диске провайдера, и право читать входящую почту как файл в этом каталоге. Для обмена письмами используется специальная адресная система. В Интернете адреса пишутся латинскими буквами, цифрами или символами. Формат адреса всегда один и тот же: <username> @ <switch>, то есть слева от знака @ находится имя пользователя, зарегистрированного в этой системе, а справа - имя компьютера с «почтовым ящиком». Например: nccom. @ pest.msk.su, cosm@online.ru, victor@urc.ac.ru.

Данное время развитие компьютерных сетей и коммуникаций значительно расширяет возможности использования информационных технологий для обмена информацией между различными пользователями. Помимо внедрения различных методов обмена информацией в повседневную работу, актуален вопрос ее безопасности: конфиденциальность, целостность и авторские права. Пользователь хочет убедиться, что никто не читает сообщения, отправленные ему, кроме указанного получателя. Получатель хочет убедиться, что информация получена из ожидаемого источника. Технологии криптографической защиты, использующие открытые ключи, часто используются для обеспечения безопасности информации, распространяемой по всему миру. В деловом мире с распространением систем электронной почты количество конфиденциальной информации, передаваемой через Интернет, быстро растет. В результате актуален вопрос автоматизации и защиты рабочего процесса по электронной почте: я хочу убедиться, что никто не читает отправленные сообщения, кроме указанного получателя. Вы должны убедиться, что электронные документы, отправленные во время заказа и хранения, не повреждены. Например, клиентская область системы электронной почты - наличие защищенных модификаций внутреннего программного обеспечения, такого как MS Outlook, позволяет потребителям создавать собственные корпоративные системы управления электронными документами любой сложности: от бухгалтерского учета до частной собственности. компании в системе расчетов крупного коммерческого банка. Используя эти инструменты, можно организовать взаимодействие торговых предприятий с дилерами и предоставлять им коммерческую информацию через Интернет. Крупные промышленные предприятия могут создавать на их основе собственный рабочий процесс. Горнодобывающие и перерабатывающие предприятия могут создать систему взаимодействия между удаленными филиалами и многое другое. Круг задач, решаемых такими прикладными системами, бесконечен.

1 Безопасность электронной почты

1.1 Безопасность систем электронной почты в корпоративной сети

Электронная почта имеет много преимуществ, но эти преимущества создают серьезные риски, связанные с ее использованием. Например, недоступность электронной почты, когда пользователи начинают использовать электронную почту для рассылки спама, простота использования и отсутствие контроля могут привести к утечке информации, распространению вируса, отправке документов различных форматов и так далее.

Таким образом, достоинство электронной почты оказалось под угрозой, так как электронная почта содержит различные «опасные» приложения, в том числе компьютерные вирусы, вредоносные программы, трояны и т. Д. стал очень удобным инструментом для распространения.

Если надлежащий контроль над использованием электронной почты не предусмотрен, это может привести к очень серьезным последствиям и даже непоправимому ущербу.

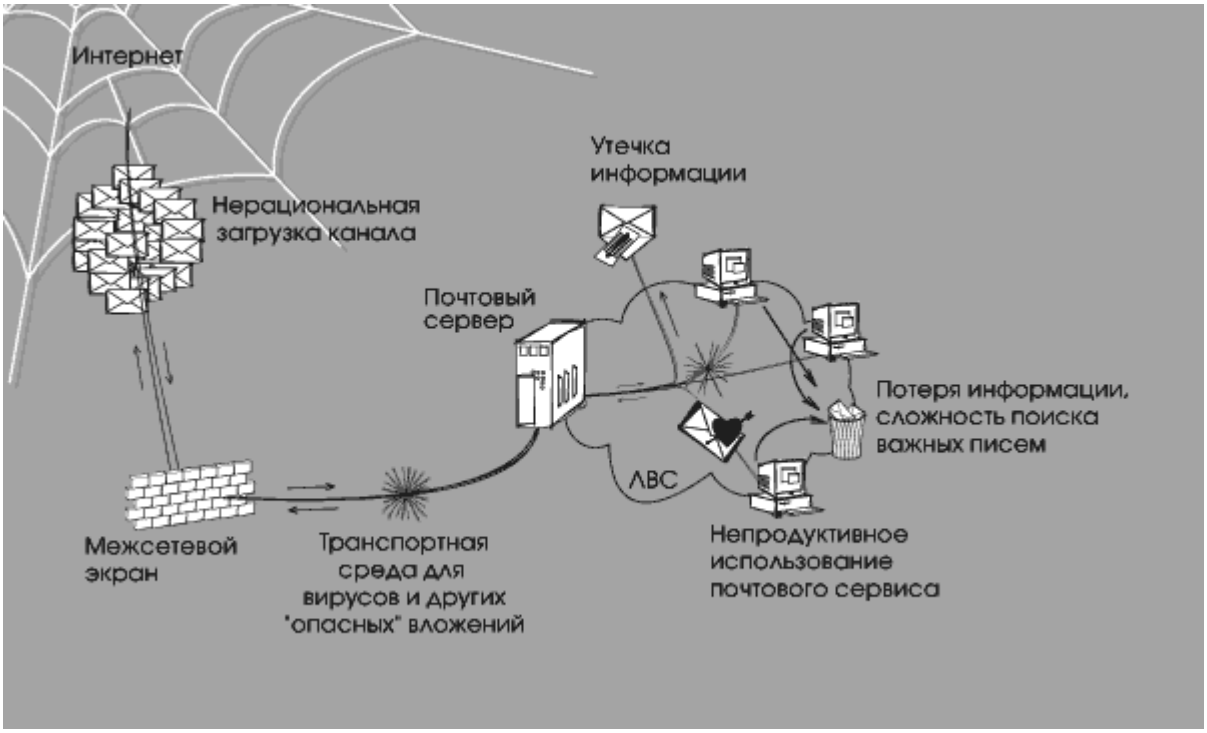

Рисунок 1- Негативное воздействие различных факторов на незащищенную почтовую систему

Для корпоративной сети различные типы атак, которые «блокируют» почтовую систему, представляют значительную угрозу. Это в первую очередь передача больших файлов или нескольких архивных файлов в виде вложений в сообщения электронной почты.

Попытка «открыть» такие файлы или «развернуть» архив может привести к зависанию системы. В то же время эти типы преднамеренных атак

одинаково опасны, такие как отказ в обслуживании и почтовые бомбы, когда пользователи отправляют электронные письма с большими вложениями, не задумываясь о последствиях открытия такого файла на компьютере получателя.

Почтовые бомбы являются одним из самых простых типов сетевых атак. Вредоносное ПО отправляет одно большое сообщение или несколько (десятки тысяч) сообщений на компьютер пользователя или почтовый сервер компании, что приводит к сбою системы.

Почтовые бомбы могут быстро уничтожить личный почтовый ящик, не давая им получать новую почту. Кроме того, интенсивная бомбардировка почты или просто отправка больших электронных писем может отключить почтовый сервер. Иногда почтовые вложения бомбы архивируются несколько раз, поэтому серверу требуется время, чтобы освободить их при обработке входящей почты.

Эффективным способом избавиться от «засорения» почтовой системы и ее перегрузки является фильтрация по количеству передаваемых данных, количеству вложений в сообщения.

Спам ведет к блокировке спам-трафика. Как правило, это включает в себя различные услуги, товары и так далее. письма, содержащие навязчивые предложения. Такие электронные письма относятся к «группе риска» по распространению вируса. Большое количество нежелательной почты загружает каналы, «нежелательные», для удаления нежелательной почты требуется время, и вы с большей вероятностью случайно удалите нужные сообщения.

Разумеется, распространение рекламы, например, не предназначено для «закрытия» почтовой системы организации, но косвенно приводит к негативным последствиям. Использование списков список рассылки, включающий всех пользователей одной и той же корпоративной сети и одновременный прием рекламных сообщений для этих пользователей, угрожает компании снижением производительности ее сетевых ресурсов.

Переписка с внешними корреспондентами представляет большую опасность из-за характера электронной почты (направление доставки писем, а также их копирование и отправка, аутентификация отправителя / получателя, невозможность возврата писем после отправки). , Кроме того, невозможно или сложно отслеживать копии отправленного письма. Содержимое сообщения может быть прочитано при его отправке через Интернет, поскольку тема и содержание электронного письма часто указываются в виде простого текста.

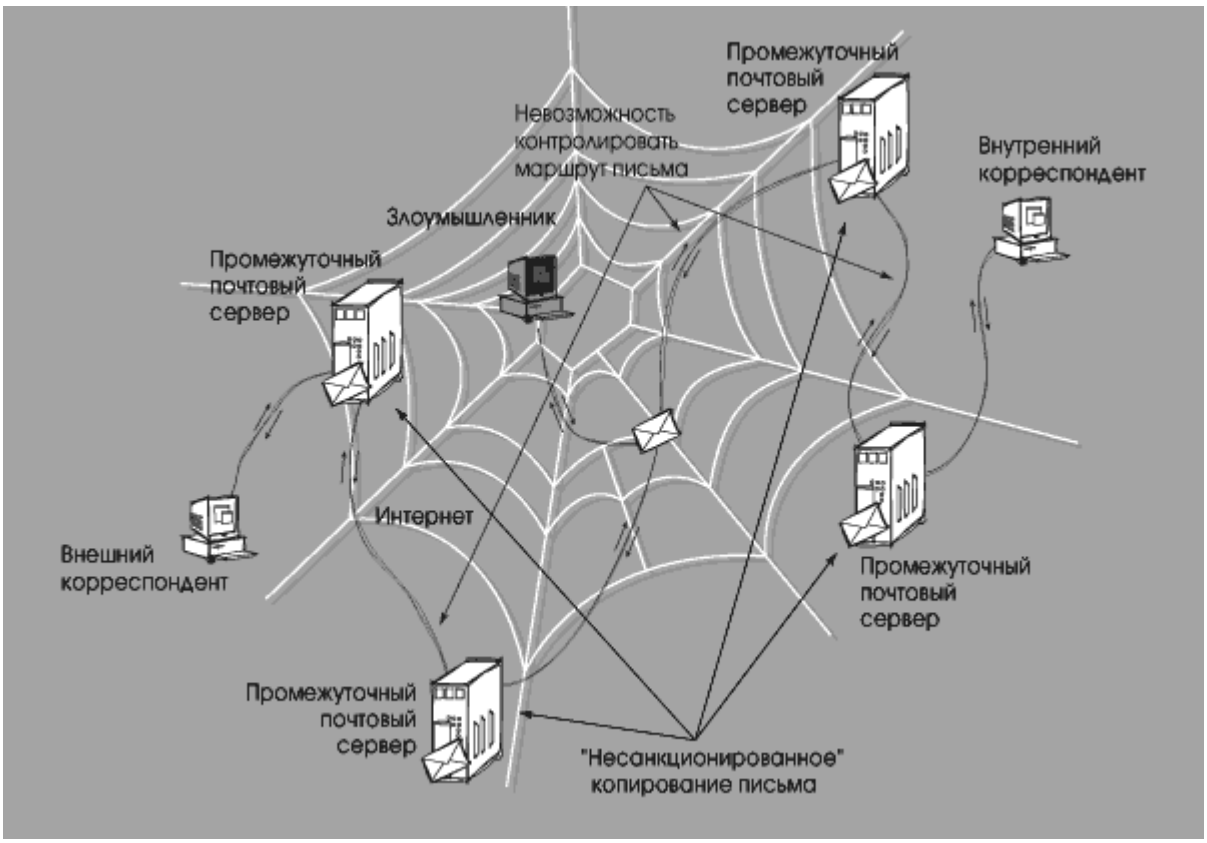

Рисунок 2 - Проблемы, возникающие при пересылке электронной почты через Интернет

Все эти функции, а также простота копирования электронного письма и невозможность контролировать это действие позволяют сотруднику предоставлять корпоративную информацию кому-либо, как внутри, так и за ее пределами, анонимно и без разрешения, немедленно или без разрешения. спустя некоторое время

Кроме того, такая информация может включать информацию о компании (тексты соглашений, информацию о планируемых транзакциях и т. д.). Пароли, системные данные, код программного обеспечения или другую конфиденциальную информацию. Это, в свою очередь, грозит серьезным нарушением конфиденциальности и может иметь негативные последствия для компании.

1.2 Методы защиты от спама и фишинга в электронной почты в корпоративной сети

Ежегодно предприятия теряют 500 миллионов долларов из-за спама, американские компании теряют 22 миллиарда долларов, а европейские компании теряют 51 миллиард долларов.

Вы уже знаете, как бороться со спамом, используя DNSBL, белые и черные списки.

PTR записи. Основной проблемой современных почтовых систем является спам. Есть много способов с этим справиться, но главное -

проанализировать отправителя, учитывая, что письмо содержит всю необходимую информацию.

Давайте проведем аналогию с обычными буквами. Конверт или почтовый пакет всегда должны содержать адрес отправителя, адрес получателя и печати почтовых отделений с этим почтовым отправлением. Точно так же тема электронной почты содержит информацию о характеристиках отправителя, получателя и почтовых серверов, участвующих в обработке почты.

Предположим, вы получили письмо в виде подозрительной квитанции от вашего любимого деда Константина Макаровича, но по какой-то причине на почтовой марке отправителя изображено не почтовое отделение в селе Макаровка, а с другой стороны колхоза Гадюкино. год. Будете вы открывать такую посылку, рискуя обнаружить вместо банки варенья из райских яблочек споры сибирской язвы, или отправите ее назад .

Рассмотрим пример защиты от спама с помощью запроса PTR-записи. PTR-запись (от англ. pointer – указатель) связывает IP-адрес с именем домена. Запрашивая PTR, MTA принимает почту только в том случае если домен отправителя совпадает с доменом отправляющего сервера.

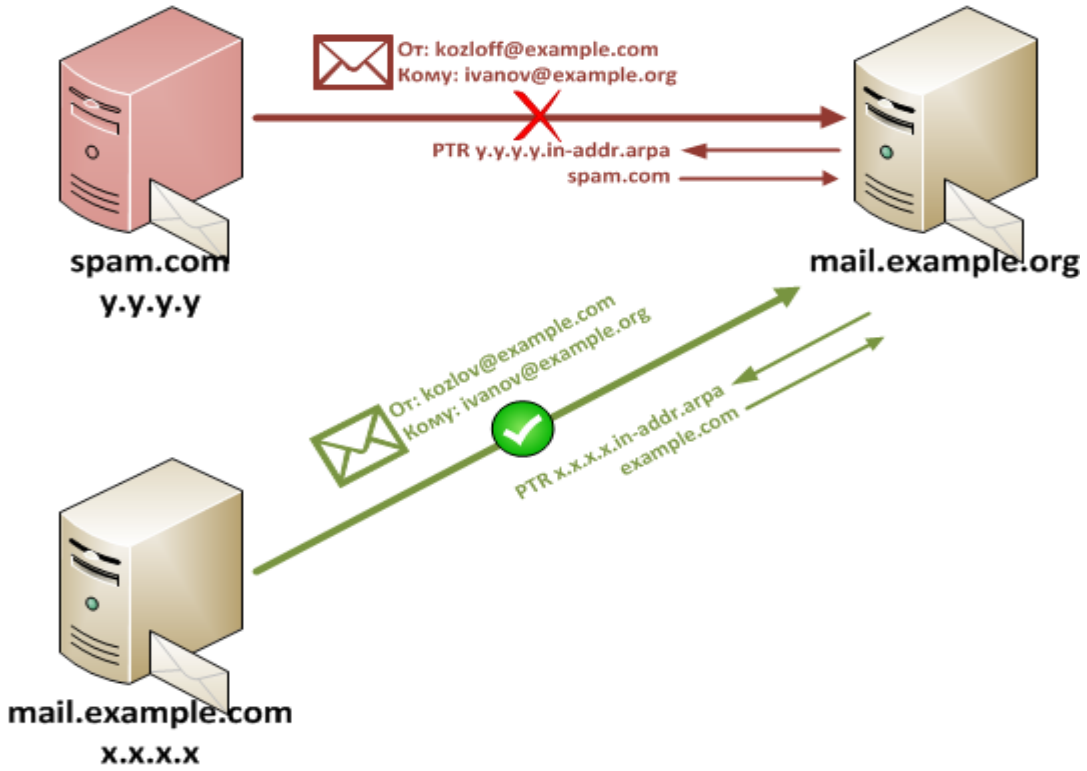

Рисунок 3 - Разрешение спам-серверам

Разрешить некоторым спам-серверам отправлять spam.com сообщение с известного сервера example.com поддельному отправителю. В случае фильтрации из черного списка такая электронная почта доставляется, поскольку отправитель получает пользователя из доверенного домена (как и ожидают спамеры).

Для борьбы со спамом MTA создает запрос записи PTR для IP-адреса отправляемого сервера, который сообщается в сеансе SMTP. Запрос PTR для IP-адреса y.y.y.y возвращает доменное имя spam.com, которое не соответствует домену отправителя, и это сообщение не будет принято. Сообщения также принимаются от сервера x.x.x.x, поскольку домен из записи PTR для IP-адреса x.x.x.x (например ,.com) совпадает с доменом отправителя.

Однако если мы укажем, что у нас есть сервер-отправитель spam.com, это сообщение будет успешно проверено с использованием записи PTR, даже если домен сервера отправителя не совпадает с доменом сообщения.

Это почему? Это связано с тем, что проверка PTR-записи позволяет вам определить правду о личности отправляющего сервера. Но ни в коем случае отправитель не аутентифицирует себя. Вот и все. На примере обычной почты мы проверяем соответствие обратного адреса и почтового индекса отправителя, если пункт назначения - Москва, и почтовый индекс указывает на Петропавловск-Камчатский, то PTR не отправил такое письмо, если пункт назначения и почтовый индекс совпадают, то все в порядке. Ваша задача - подумать о том, чем занимается ваш любимый дедушка в Петропавловске-Камчатском.

Записи SPF - Структура политики отправителя (SPF) - Структура политики отправки

Возвращайся к нашему дедушке. Предположим, он сказал вам, что летом он покинул соседнюю деревню Макаровка в деревне Ивановка и хотел отправить письмо Марте Васильевне. В этом случае вы с уверенностью примете письма деда из Макаровки и Ивановки, но отклоните письма деда из Петропавловска-Камчатского.

Аналогичная технология в почтовых системах реализована с использованием технологии SPF. Короче говоря, эта технология позволяет создавать специальные записи DNS, в которых указывается, кто имеет право отправлять почту от имени домена. В простейшей версии запись выглядит следующим образом:

example.com. IN TXT "v=spf1 +a +mx -all"

Что это значит? Не следует принимать все узлы (-all), поскольку узлы, указанные в A-записях (+ a) и MX-записях (+ mx), могут отправлять почту в домен example.com.

MX-запись - это особый тип DNS-записи, которая содержит имена почтовых серверов, обрабатывающих входящую почту из определенного домена. Может быть несколько записей MX, и в этом случае MTA попытается установить соединение с сервером в очереди с наивысшим приоритетом. Если запись MX отсутствует, запрашивается запись (запись адреса, соответствующая имени домена с IP-адресом), и делается попытка доставить почту на указанный там хост.

Серые списки. Принцип этого метода основан на том факте, что программное обеспечение, которое реагирует на спам, отличается от «поведения» обычных почтовых серверов.

При использовании серого списка все неизвестные SMTP-серверы включаются в эти списки, но также сообщения от такого сервера не принимаются. Серверы получают временный код ошибки, и если почта является доброй, она возвращается с этого адреса.

Спамер отправляет сообщение обратно на другой адрес, затем спам удаляется или сохраняется в специальной папке. Таким образом, значительная часть нежелательной почты (около 90%) удаляется, а важные письма приходят без потерь - в этом и заключается сила этого метода, что и привело к его популярности.

Недостатком является время, необходимое для дополнительной проверки электронной почты (иногда до 30 минут), и это неудобно при работе с срочной перепиской. Однако задержка возникает только тогда, когда первое письмо приходит с неизвестного сервера, поэтому этот метод может быть удобен для некоторых организаций.

Анализ темы

Для создания электронных писем спамеры используют специальное программное обеспечение, которое автоматически создает и распространяет сообщения. Такие программы имеют существенный недостаток: они отправляют ошибки в оформлении темы, поэтому спам-сообщение не соответствует почтовому стандарту RFC. Благодаря такому расчету фильтры антиспама обнаруживают нежелательные сообщения. Такая защита очень надежна и эффективна.

Анализ вложений. Изначально фильтр вложений проверял только «тело» сообщения с темой и текстом сообщения. Тем не менее, антиспам проверки теперь выполняются для сообщений и даже изображений, прикрепленных к ним. Он эффективно «быстро учится», адаптируется к новым типам нежелательной корреспонденции и практически не работает.

Определение признаков массовости. Этот метод очень прост: большие буквы содержат полностью идентичные или слегка отличающиеся сообщения. Технология в основном предназначена для крупных организаций с большим объемом почты.

Современные ИТ-компании для защиты от спама и фишинга используют несколько методов, которые создают комплексную защиту сразу. Наиболее часто используемые методы в специализированном программном обеспечении - это черный и серый списки, анализ букв. Авторитетные антиспам-сканеры - GFI MailEssentials, Kaspersky Anti-Spam, Kaspersky Security для почтового сервера, McAfee Security, Symantec MailSecurity, ESET MailSecurity - до 99% всех нежелательных сообщений.

1.3 Безопасность корпоративной системы электронной почты

Учитывая вышеупомянутые риски, связанные с использованием электронной почты, организации должны принять соответствующие меры для защиты от них.

Подход к защите должен быть комплексным и всеобъемлющим - необходимо сочетать организационные меры с использованием соответствующих технических средств.

Организационные мероприятия включают разработку и внедрение почтовой политики в компании. Технические средства должны обеспечивать реализацию этой политики, как путем мониторинга почтового трафика, так и путем надлежащего реагирования на нарушения. Для защиты компании от рисков, связанных с использованием электронной почты, необходимы: политика использования электронной почты и средство реализации политики.

1.3.1 Политика использования электронной почты

Для решения проблем безопасности необходимо создать специальный набор правил - политики электронной почты - это письменные инструкции и другие документы, отправляемые сотрудникам, которые регулируют процессы, связанные с использованием системы электронной почты.

Эти документы и инструкции имеют правовой статус и обычно предоставляются для проверки сотрудниками организации. Политика электронной почты является неотъемлемой частью корпоративной политики информационной безопасности и неотделима от нее.

Политика должна детально определять меры по обеспечению безопасности использования электронной почты в компании, должна содержать указания и рекомендации по использованию и хранению электронной почты.

С технической точки зрения политика устанавливает правила использования электронной почты, то есть определяет:

- что контролируется: прохождение каких сообщений входящей, исходящей или внутренней электронной почты должно быть разрешено или запрещено;

- на кого распространяется: категории лиц, которым разрешено или запрещено отправлять исходящие или получать входящие сообщения электронной почты;

- как реагирует система: что необходимо делать с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты.

Следует отметить, что политика использования электронной почты является приоритетной по отношению к средствам ее реализации. Сначала необходимо сформулировать политику и создать правила для использования электронной почты, определить, как созданная система должна реагировать на некоторые нарушения этой политики, а затем перевести правила на компьютерный язык инструмента, используемого для мониторинга выполнения программы. положения политики электронной почты.

1.3.2 Система контроля содержимого электронной почты

Политика использования электронной почты реализуется через аппаратное и программное обеспечение - систему управления контентом электронной почты.

Системы управления содержимым электронной почты представляют собой набор аппаратного и программного обеспечения, способного анализировать содержимое электронной почты различными компонентами и структурами для реализации политики электронной почты.

Спектр возможностей всех категорий систем управления контентом электронной почты достаточно широк и значительно варьируется в зависимости от производителя. Однако наиболее общие требования установлены для всех систем, что позволяет решать проблемы, связанные с управлением почтовым трафиком.

Наиболее распространенные требования включают в себя:

- анализ текста электронной почты (анализ ключевых слов и выражений с использованием встроенных словарей). Эта функция позволяет своевременно обнаруживать и предотвращать распространение конфиденциальной информации, выявлять наличие непристойного или запрещенного контента, останавливать защиту от спама и предоставлять другие материалы , запрещенные политикой безопасности;

- управление отправителями и получателями электронных писем. Эта функция позволяет фильтровать почтовый трафик, тем самым реализуя некоторые функции брандмауэра в почтовой системе;

- анализируйте электронные письма на их компоненты (заголовки MIME, текст сообщения, вложенные файлы и т. Д.), Удаляйте «опасные» приложения и впоследствии собирайте компоненты электронной почты;

- изолируйте или приостановите большие сообщения (например, через несколько часов), пока канал связи не будет загружен до минимума. Распространение таких сообщений в почтовой сети компании может привести к перегрузке сети, поэтому блокирование или задержка доставки не позволят этого;

- распознавание графических, видео и аудио файлов. Как правило, такие файлы имеют большой размер, и их распространение может привести к потере сетевых ресурсов. Следовательно, распознавание и откладывание этих типов файлов не приведет к снижению эффективности компании;

- обработка сжатых/заархивированных файлов. Это позволяет проверять сжатые файлы на наличие запрещенного контента;

- распознать исполняемые файлы. Как правило, такие файлы имеют большой размер и редко связаны с бизнесом компании. Исполняемые файлы также являются основным источником почтовых вирусов. Следовательно, распознавание и откладывание этих типов файлов не приведет к снижению эффективности компании и не приведет к заражению системы;

- управление спамом и блокировка. Распространение спама приводит к перегрузке сети и потере рабочего времени. Функция защиты от спама и блокировки экономит сетевые ресурсы и снижает эффективность компании;

- возможность определить количество вложений в письмах. Повторная отправка электронной почты с несколькими вложениями может привести к переполнению сети, поэтому мониторинг соответствия количеству вложений, указанному в политике информационной безопасности, обеспечивает безопасность ресурсов корпоративной сети;

- управление и блокировка программ закладок (cookie), вредоносного мобильного кода (Java, ActiveX, JavaScript, VBScript и т. Д.), А также файлов, которые выполняют автоматическую передачу (называется «Автоматическая почта»). Эти типы инвестиций являются очень рискованными и приводят к утечкам информации из корпоративной сети;

- разделите ресурсы почтовой системы компании на категории («администрация», «отдел кадров», «финансы» и т. Д.) И ограничьте доступ к различным категориям сетевых ресурсов для сотрудников компании (в зависимости от времени суток);

- реализовать различные варианты ответа, в том числе: удалить или временно заблокировать сообщение; карантин для отсрочки и дальнейшего анализа сообщения; «вылечить» зараженный файл; уведомление администратора безопасности или любого другого адресата о нарушении политики безопасности и т. д.

Поддерживать полноценный архив электронной почты, возможность хранить электронную почту онлайн с высоким уровнем доступности данных. На основании информации, хранящейся в архиве, дальнейший анализ почтового потока компании, системное регулирование, анализ событий, связанных со злоупотреблением почтовыми услугами компании и т. д.

Рисунок 5 представляет собой таблицу типичных систем управления контентом электронной почты. Схема обработки сообщений обычно включает в себя следующие этапы:

- рекурсивная декомпозиция электронной почты;

- анализ содержания электронной почты;

-категоризация электронной почты (присвоение определенной категории);

- действие на письмо по результатам присвоения категории

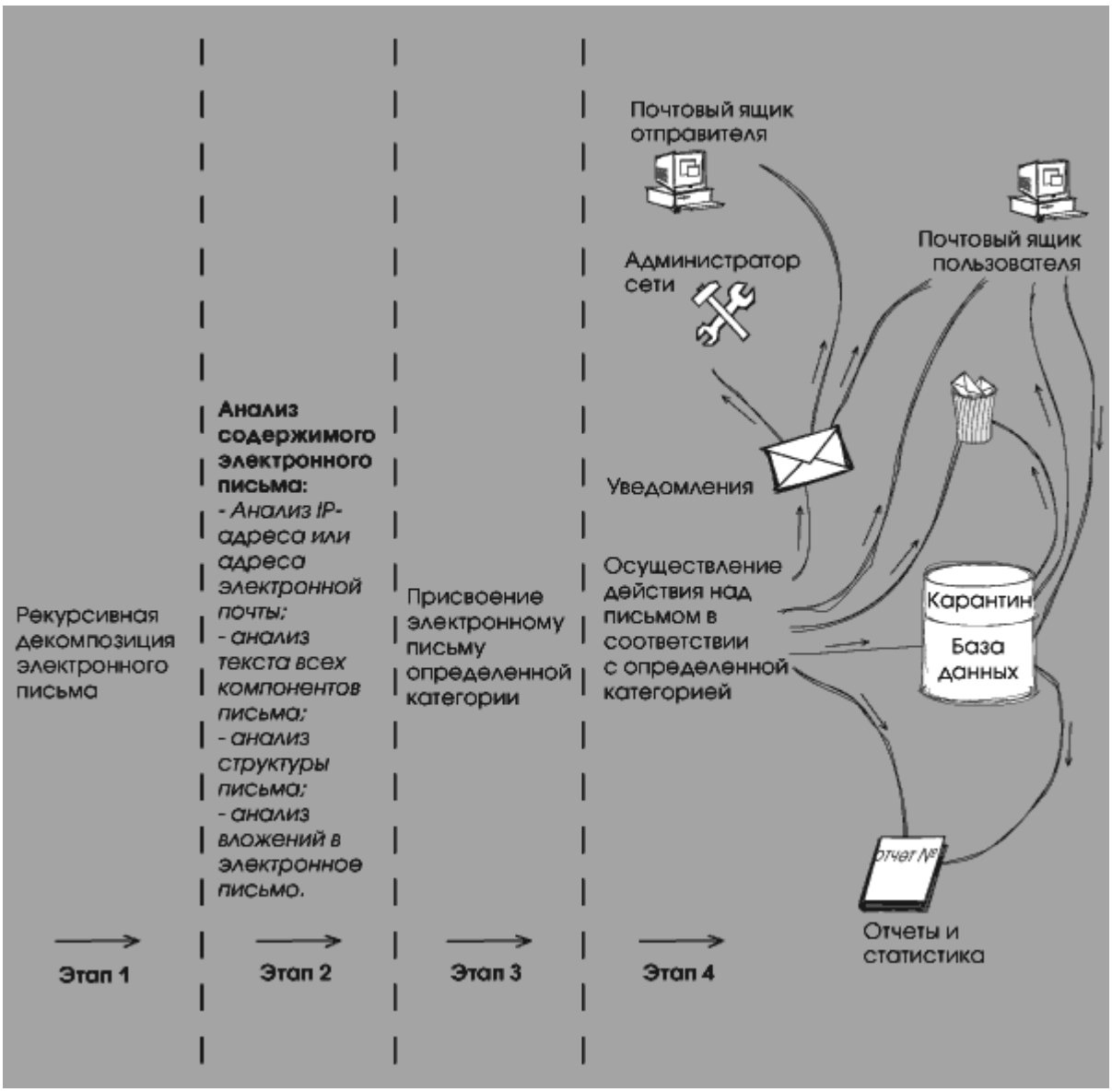

Рисунок 4 - Схема обработки сообщения системой контроля содержимого электронной почты

1.3.3 Сравнительный анализ систем "Дозор-Джет" и MAILsweeper

Анализ рынка программного обеспечения для защиты информации и сравнение его функциональных возможностей показывает, что среди продуктов, предлагаемых в настоящее время на рынке, - система отслеживания и архивирования электронной почты Dozor-Jet, Jet Infosystems и MAILsweeper. , ClearSwift (Великобритания).

Dozor-Jet и MAILsweeper - это программные продукты, которые имеют общий набор функций, которые позволяют классифицировать информацию в один класс защиты. Эти функции:

1. Фильтрация писем на основе анализа их содержания;

2. Использование в анализе технологии рекурсивной декомпозиции, т. Е. Анализа электронной почты на ее компоненты (заголовки сообщений, заголовки MIME, текст сообщения, вложенные файлы и т. д.);

3. Использование специальных методов оценки при анализе контента;

4. По результатам такого анализа выполнить определенные действия в письме.

Dozor Jet можно классифицировать как систему промышленного уровня, поскольку этот продукт работает на платформе UNIX и включает в себя подсистему архивирования на основе СУБД Oracle. Система Dozor Jet используется в организациях с 5 гигабайтами почтового трафика в день и более 5000 почтовых адресов. Это, в свою очередь, требует использования оборудования, обеспечивающего высокую производительность системы и отказоустойчивость.

MAILsweeper устанавливается на серверах под управлением операционной системы MS Windows. MAILsweeper не использует системы хранения информации промышленного уровня.

Dozor Jet имеет мощную систему фильтрации сообщений, которая позволяет реализовывать почтовые политики любой сложности. Фильтрация также выполняется для всех компонентов сообщения: атрибуты конверта, заголовки сообщения, заголовки MIME, текст сообщения, вложенные файлы.

Расширенный набор проверок и действий позволяет системному администратору создавать собственные методы проверки сообщений и вложений и выполнять различные действия с ними. Почта фильтруется в зависимости от ситуации. Последовательность применения правил фильтрации в системе является динамической, что означает применение любого набора правил в порядке, установленном администратором безопасности.

Рассматриваемые системы отличаются тем, как они классифицируют сообщения. Таким образом, Dozor-Jet имеет систему классификации букв, которая позволяет назначать несколько электронных писем нескольким семантическим категориям одновременно. Работа классификатора основана на простой, но очень эффективной технологии байесовского фильтра, которая одинаково хорошо работает на русском и английском языках. Автоматическая настройка классификатора значительно повышает эффективность подсистемы фильтрации и предотвращает ложные срабатывания при выделении «запрещенных» писем.

В MAILsweeper категоризация основана исключительно на лексическом анализе (сопоставление слов и фраз) и «весе» слова (частота использования в тексте), что не обеспечивает хорошую защиту от ложных срабатываний и может привести к потере необходимой информации.

Работа с буквами в Dozor Jet предполагает морфологический анализ слов, который позволяет искать все лексические формы данного слова. Почтовый не имеет такого анализа. Эта функция становится еще более важной из-за особенностей русского языка, который имеет сложную грамматическую структуру слов.

Dozor Jet включает подсистему архивирования промышленного уровня, основанную на СУБД Oracle. В архиве хранится большое количество корпоративной электронной почты в Интернете, с высоким уровнем

доступности данных и длительным хранением в течение десяти и более лет. Архив предлагает широкий спектр вариантов хранения и поиска. Стоит отметить такие особенности, как контекстный поиск в архиве, поиск в архиве с учетом морфологической структуры русского языка, деление архива на исторические регионы (распространение), экспорт электронной почты в зарубежные СМИ.

У почтового ящика нет почтового архива. Система архивирует сообщения в виде файла. Все письма в архиве. Dozor Jet позволяет регистрировать электронные письма. Регистрация - это хранилище информации о конкретной теме электронной почты (авторе, получателе, размере и т. Д.) И ее структуре MIME. Регистрация, в отличие от хранения всего сообщения, экономит место на дисковых массивах и ускоряет поиск необходимой информации.

Что касается почтового архива, следует отметить, что в его арсенале ClearSwift имеется модуль, специально разработанный для MAILsweeper и называемый Archivist. Этот модуль предназначен для поиска необходимых атрибутов в архиве электронной почты по следующим атрибутам: получатель, получатель, тема письма, дата получения / отправки, имя файлов приложения.

Dozor Jet обладает широким спектром возможностей отчетности. В зависимости от доступности архива система может получать образцы любой сложности в соответствии с созданными запросами (возможность создавать конкретные запросы SQL, создавать любые отчеты с использованием Oracle Report, Crystal Report). Системный архив содержит всю «учетную» информацию о почте (темы, типы приложений, их размер и т. Д.), Что позволяет получать отчеты по различным параметрам почтового трафика. Подмодуль «Статистика» содержит набор отчетов в формате MS Excel.

MAILsweeper генерирует отчеты только с использованием Crystal Report. Вам также нужен сервер Microsoft SQL для создания отчетов.

Благодаря технологии обнаружения эвристического кодирования, система Dozor Jet, независимо от кодировки кириллицы (CP1251, CP866, ISO8859-5, KOI8-R, MAC), может анализировать сообщения, в том числе незашифрованный текст (например, проверять файлы в сжатом формате) или сообщать неправильно. Кодировка текста в заархивированных файлах также определяется.

Шифрование MAILsweeper не гарантирует обработку неопубликованных или неправильно объявленных текстов электронных писем, поскольку кодирование определяется только заголовками MIME.

Dozor Jet имеет модульную структуру, которая позволяет добавлять дополнительные функции в систему, не затрагивая ее ядро. Это позволяет добавлять внешние приложения в систему обработки электронной почты, которая расширяет функцию Dozor-Jet. Таким образом, продукт может быть интегрирован с системами управления документами, различными подсистемами информационной безопасности (брандмауэры, инструменты виртуальной защищенной сети, антивирус, системы электронной цифровой

подписи и т. д.) и корпоративными системами управления информационными ресурсами (HP OpenView). Всего Dozor Jet имеет девять различных модулей. Dozor Jet также имеет возможность вызывать внешние приложения (сторонние приложения), которые обеспечивают дополнительную обработку электронной почты.

MAILsweeper включает в себя один модуль Archivist для работы с почтовыми архивами. Кроме того, система (как в системе Dozor Jet) имеет возможность вызывать внешние приложения.

Продолжая тему модульности системы, Dozor Jet добавляет специальный модуль для проверки и настройки цифровой подписи, который при активации обеспечивает контроль над целостностью информации, отправляемой по электронной почте. Кроме того, Dozor Jet может автоматически шифровать исходящие сообщения в формате S / MIME.

В отличие от Dozor Jet, система MAILsweeper может обнаруживать наличие электронной цифровой подписи в сообщении, но не имеет возможности шифровать сообщения, а также проверять подлинность и цифровую подпись.

Dozor Jet - единственный сертифицированный продукт на рынке для систем управления контентом электронной почты. Государственная техническая комиссия провела испытания системы Дозор-Джет и ее технических спецификаций и «Защита от несанкционированного доступа к информации». Программное обеспечение информационной безопасности».

MAILsweeper - это продукт, который не сертифицирован соответствующими органами для использования в Республике Казахстан.

Реактивный патруль является отечественной разработкой. Jet Infosystems оказывает техническую поддержку своим клиентам на любом уровне напрямую от производителя. Это позволяет быстро решить любые вопросы, связанные с работой системы. ClearSwift предоставляет техническую поддержку только через сертифицированных партнеров (NPC Informtsaschita)

Таблица 1- Таблица сравнения основных характеристик систем "Дозор-Джет" и Mailsweeper

	"Дозор-Джет"	MAILsweeper для SMTP
Версия	2.6	4.3
Платформа	UNIX	Windows
Используемые процессоры	SPARC/PA-RISC/Intel	Intel
Операционная система	Sun Solaris, HP-UX, Linux	Windows
Интерфейс управления	Web-навигатор	Графический, с использованием Microsoft Management Console

Продолжение таблицы 1

Система обработки электронной почты	Последовательность применения правил определяется динамически Расширяемый набор проверок и действий Первое применяемое правило создается на основании любых условий К одному письму может применяться несколько правил	Правила применяются в строго определенной последовательности в соответствии с их приоритетностью и иерархией проводимых проверок Расширяемый набор действий Первое применяемое правило фильтрует сообщения на основании почтовых адресов Не имеет возможности продолжить применение правил после выполнения текущего правила или применить другой набор правил
Анализ текстов	Возможность поиска слов с учетом словообразования (как английского, так и русского) Полнофункциональные регулярные выражения	Совпадение слов и строк Ограниченное подмножество регулярных выражений
Категоризация сообщений	Адаптивная система категоризации, основанная на Байесовских фильтрах Автоматическая корректировка категоризатора	Категоризация на основе лексического анализа (совпадения слов и выражений) и "веса" слова (частотности употребления в тексте)

Продолжение таблицы 1

Действия по результатам обработки сообщения	Блокировать Отправить уведомление Зарегистрировать Поместить в архив Применить набор правил Доставить Установить права доступа Пометить Запустить внешнюю программу Переслать на определенный адрес	Блокировать Отправить уведомление Поместить в карантин Доставить Доставить в соответствии с расписанием Переслать на определенный адрес Копировать в архивный файл Запустить внешнюю программу
Модификация данных	Удаление вложения определенного типа	Удаление вложения определенного типа Включение в тело письма определенного текста
Проверка сообщений на вирусы	Средствами третьих производителей Наличие интерфейса для антивирусных программ Реализован унифицированный интерфейс к антивирусам: Symantec Anti-Virus (Symantec) AVP (Лаборатория Касперского) Dr.Web (Диалог-Наука)	Средствами третьих производителей Command Interceptor (Command Software Systems) VetNT (Computer Associates) FPROT (Frisk F-Secure Anti-Virus, компании F-Secure) SAVAPI (H+BEDV) Command line (McAfee Norman Virus Control (Norman) TBA и Sophos Anti-Virus (Sophos) Symantec Anti-Virus (Symantec)

Продолжение таблицы 1

Архив сообщений	Реализован на основе	Архивация в виде

	СУБД Oracle или PostgreSQL (для Lite-версии) Помещение писем в архив по любым критериям Помещение в архив всего письма или его регистрационной информации	файлов Архивирование в директорию или на определенный адрес в сети Архивирование только всего письма
Контекстный поиск по архиву	Имеет модуль контекстного поиска в архиве электронной почты Также осуществляется по текстам вложенных файлов	Реализуется только дополнительно установленным модулем Archivist, который использует Indexing Service, входящий в состав Windows 2000/NT
Атрибутивный поиск по архиву	По любым атрибутам письма	по адресату/получателю теме письмадате получения/отправки наименованию файлов-приложений
Морфологический поиск по архиву	Имеет модуль поиска по архиву с учетом морфологического строения русского языка	Не имеет
Возможность хранения архива электронной почты на внешних носителях	Имеет модуль хранения электронной почты на внешних носителях	Не имеет
Возможность долговременного архива электронной почты	Имеет модуль разделения архива на исторические области (Partitioning)	Не имеет
Генерация отчетов	2 типа встроенных отчетов по любым атрибутным и текстовым запросам в MS Excel возможность построения отчетов пользователем с помощью	Для построения отчетов требуется наличие Microsoft SQL server Построение отчетов при помощи Crystal Report

1.4 Электронная почта - протоколы SMTP, POP3, IMAP4

Электронная почта является одним из важнейших информационных ресурсов в Интернете, самым популярным средством электронного общения. Любой пользователь Интернета может получить свой почтовый ящик онлайн.

Отправить вам электронное письмо:

- отправка и получение сообщений;
- автоматический ответ на переписку корреспондентов по их адресам;
- отправить копии письма сразу нескольким получателям;
- отправить полученное письмо на другой адрес;
- используйте логические имена вместо адресов (числовые или доменные имена);
- создать несколько разделов почтового ящика для всей корреспонденции и т. д.

Если принять во внимание, что вы можете получать или отправлять сообщения через Интернет в двадцать международных компьютерных сетей, которые не обслуживают онлайн, становится ясно, что почта предоставляет только более широкий диапазон возможностей. Информационная служба интернета.

Преимущества электронной почты

Электронная почта имеет несколько преимуществ по сравнению с обычными способами уведомления (традиционная почта или факс). Они включают:

- эффективность и простоту использования.

Электронная почта - это глобальная система, которая позволяет отправлять электронные письма в любую точку мира в считанные минуты независимо от времени суток. Вам не нужны глубокие знания компьютерных технологий для отправки и получения электронной почты, поэтому этот сервис широко используется не только в бизнесе, но и для личного общения.

Доступность где угодно. Основным преимуществом электронной почты является ее доступность. Хотя большие пространства еще не «освоены» электроникой, быстрое развитие электронных коммуникаций в конечном итоге приведет к «глобальной сети», охватывающей весь земной шар.

Разнообразие форматов писем и вложений. Удобство использования электронной почты - это возможность «передавать» большие объемы информации в разных форматах. Одно письмо содержит графическую, видео, текстовую информацию, файлы базы данных, приложения и многое другое. может быть дано в то же время.

Дешевый сервис. Отправка электронной почты намного дешевле, чем обычно, делая междугородние или особенно международные телефонные звонки. Электронная почта позволяет отправлять электронную почту нескольким получателям одновременно без дополнительных затрат.

- надежность и скорость доставки инфраструктуры.

Поскольку электронная почта отправляется с сервера отправителя на сервер получателя через Интернет, процесс происходит быстро, даже если эти серверы расположены по разные стороны света. Фактически, например, отправка текстового сообщения из Казахстана в Америку занимает 1-2 минуты.

Электронная почта похожа на обычную почтовую службу. Переписка готовится пользователем на рабочем месте или с помощью программы подготовки почты или простого текстового редактора. Затем пользователь должен вызвать программу пересылки почты (обычно программа подготовки почты вызывает программу отправки автоматически). Он сортирует почту и отправляет ее получателям.

1.5 Компоненты электронной почты Интернет

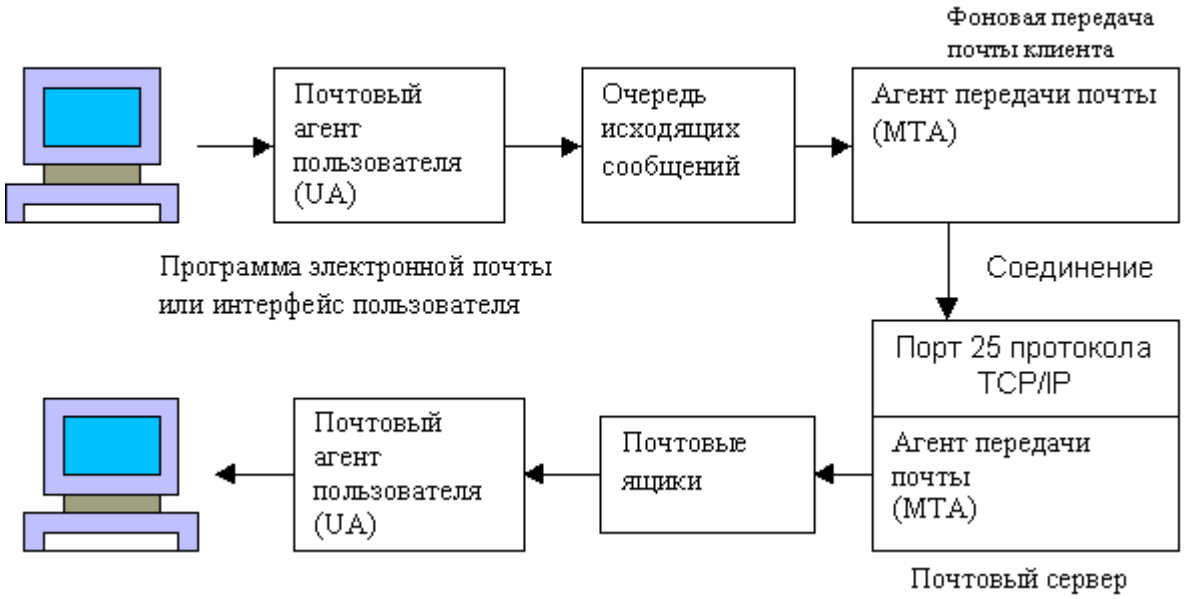

Рисунок 5 - Реальные компоненты постовой системы Интернет

Модель электронной почты каждого пользователя имеет локальный почтовый ящик, где хранятся все сообщения. Для работы с почтовым ящиком существуют специальные программы, называемые пользовательскими почтовыми агентами, сокращенно UA (User Agent).

Агенты почтовых пользователей не получают сообщения с удаленных компьютеров; они показывают только содержимое почтового ящика пользователя. За прошедшие годы для платформы UNIX было разработано несколько различных агентов (UA). Например, пользователи Unix знакомы с ОАЭ.

MH, Mail, Elm, Mush и Pine.

Для пользователей Windows самой известной программой UA, возможно, является Microsoft OutLook Express. The Bat.

Важной частью почтового сервера является MTA (Mail Transfer Agent), который отвечает за отправку сообщений электронной почты от одного пользователя другому. Получателями могут быть пользователи как системы, так и удаленной системы. MTA также несет ответственность за направление письма всеми доступными способами для его доставки получателю.

Часто существует несколько почтовых сайтов между отправляющим и получающим хостами. Каждый агент MTA отвечает за доставку сообщения до конечного пункта назначения, и, если доставка невозможна, он должен вернуть его отправителю.

Следующим компонентом электронной почты является почтовый агент (MDA). Его задача - отправить письмо из почтового ящика на сервер по запросу почтового клиента. Может работать с MDA POP3 или IMAP.

Вопреки распространенному мнению, MDA не имеет ничего общего с процессом рассылки. Это компетенция MTA. Если вы проведете аналогию, вы можете представить себе MDA с почтовым отделением, которое обрабатывает прием и отправку почты, и MDA с почтальоном, который доставляет входящую почту к вам домой.

Если почтовый работник болеет, это не повлияет на работу почтового отделения, вы не сможете получать письма домой. Также, MDA, его сбой не приводит к сбоям в работе почтового сервера, только почтовый клиент не сможет получать почту.

Рассмотрим структуру почтового сервера, а также то, что происходит, когда пользователь пытается отправить почту.

В нашем примере пользователь из Иванова, расположенный в домене example.org (ivanov@example.org), пишет письмо Козлову в домене example.com (kozlov@example.com). Для Иванова процесс отправки почты состоит из создания сообщения и нажатия кнопки «Отправить» в почтовом клиенте.

Почтовый клиент подключается к MTA через SMTP и сначала сообщает свои учетные данные. После предоставления разрешения пользователю MTA получает сообщение и пытается доставить его дальше. MTA может использовать свой список пользователей, системный список, LDAP или AD список пользователей для авторизации.

Существует также способ: POP-аутентификация перед SMTP, когда пользователь входит в MDA перед отправкой почты, это, в свою очередь, подтверждает подлинность пользователя для MT.

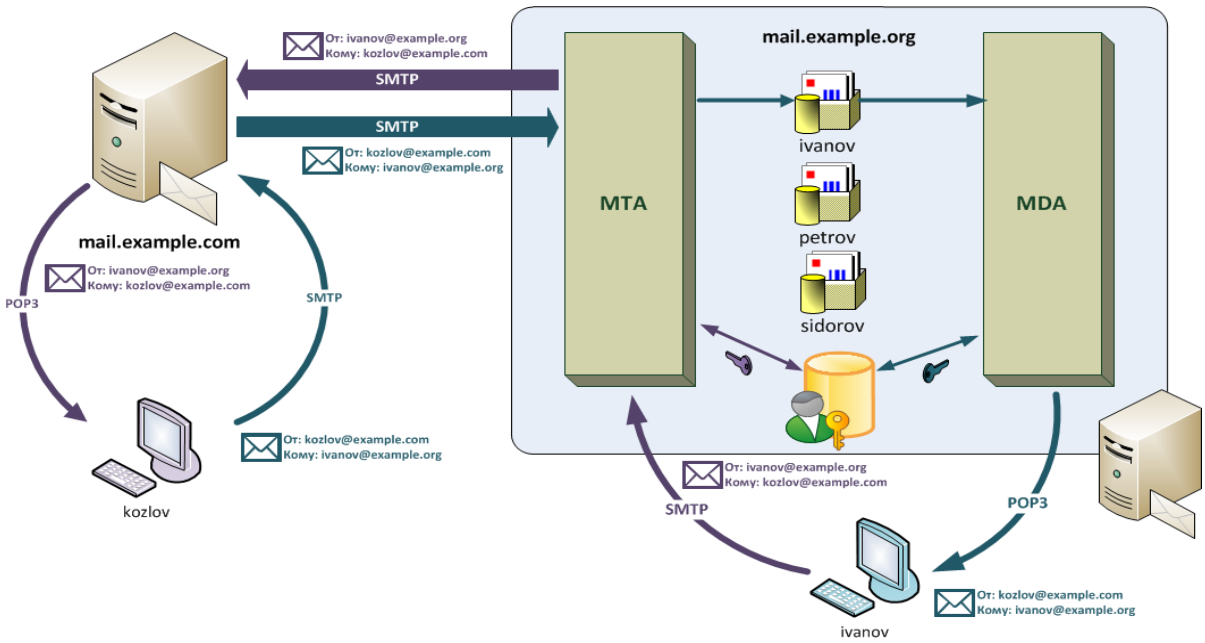

Рисунок 6 - SMTP аутентификация

Следующим шагом является анализ официальной информации письма, идентифицирующий домен получателя MTA. Если эти данные MTA принадлежат доменам, которые он обслуживает, получатель обыскивается и письмо помещается в его почтовый ящик. Если Иванов написал письмо Петрову или Сидорову, это случилось.

Если домен получателя не обслуживается адаптером MTA, создается запрос DNS, который запрашивает записи MX для домена. MX-запись - это особый тип DNS-записи, которая содержит имена почтовых серверов, обрабатывающих входящую почту из определенного домена.

Может быть несколько записей MX, и в этом случае MTA попытается установить соединение с сервером в очереди с наивысшим приоритетом. Если запись MX отсутствует, запрашивается запись (запись адреса, соответствующая имени домена с IP-адресом), и делается попытка доставить почту на указанный там хост. Если сообщение не может быть отправлено, оно возвращается отправителю (в почтовом ящике пользователя).

Предположим, Козлов получил письмо от Иванова и написал ответ. Сервер, обслуживающий домен Example.com, делает то же самое и пытается отправить почту на наш сервер.

Простой протокол передачи почты (SMTP). Протокол передачи почты (SMTP) описывает систему команд и условий для обычных пользователей для отправки сообщений другим пользователям на основе адресов электронной почты. SMTP позволяет обмениваться почтовыми сообщениями между пользователями одной и той же или разных компьютерных сетей.

Система поддерживает:

- отправить одно сообщение одному или нескольким получателям;

- отправлять сообщения, в том числе текстовые, голосовые, видео или графические материалы.

Агент пересылки почты является ключевым компонентом системы доставки почты через Интернет. Как упомянуто выше, MTA предоставляет сетевой компьютер для сетевой системы электронной почты.

После того, как UA отправляет сообщение в очередь выхода, MTA принимается для случая. Получает сообщение и отправляет его в другой AIT. Этот процесс продолжается до тех пор, пока сообщение не достигнет конечного компьютера. Большинство протоколов MTA используют протокол SMTP для отправки сообщения по TCP-соединению.

Сообщения форматируются в соответствии с правилами виртуального сетевого терминала (NVT), то есть NVT ASCII. NVT похож на протокол виртуальной сети и затем необходим для того, чтобы скрыть различия в восприятии разными компьютерами разных сигналов, таких как передача, возврат, отключение сети, очистка экрана и т. Д. Символ в NVT состоит из семибитного набора ASCII и представляет собой букву, цифру или знак пунктуации. Семибитный набор ASCII часто называют NVT ASCII.

Взаимодействие внутри SMTP основано на принципе двусторонней связи между отправителем и получателем почтового сообщения. В этом случае отправитель запускает соединение и отправляет запросы на обслуживание, получатель отвечает на эти запросы. Фактически, отправитель действует как клиент, а получатель - как сервер.

Команды SMTP. Простые почтовые протоколы обеспечивают двусторонний обмен сообщениями между локальным клиентом и удаленным сервером MTA. Клиент MTA отправляет команды серверу MTA, который, в свою очередь, отвечает клиенту. Другими словами, SMTP требует, чтобы вы получили ответ от команды SMTP.

Обмен командами и ответами на них называется почтовой операцией. Данные, как мы уже говорили, передаются в формате NVT ASCII. Команды также выдаются в формате NVT ASCII. Команды даны в форме ключевых слов, а не специальных символов, и указывают на необходимость выполнения определенной операции. В таблице 2 приведены ключевые слова (команды), определенные в спецификации SMTP - RFC 821.

Таблица 2 - Команды простого протокола передачи почты (SMTP)

Команда	Обязательна	Описание
HELO	X	Идентифицирует модуль-передатчик для модуля-приемника (hello).
MAIL	X	Начинает почтовую транзакцию, которая завершается передачей данных в один или несколько почтовых ящиков (mail).
RCPT	X	Идентифицирует получателя почтового сообщения (recipient).

Продолжение таблицы 2

DATA		Строки, следующие за этой командой, рассматриваются получателем как данные почтового сообщения. В случае SMTP, почтовое сообщение заканчивается комбинацией символов: CRLF-точка-CRLF.
RSET		Прерывает текущую почтовую транзакцию (reset).
NOOP		Требует от получателя не предпринимать никаких действий, а только выдать ответ ОК. Используется главным образом для тестирования.(No operation).
QUIT		Требует выдать ответ ОК и закрыть текущее соединение.
VRFY		Требует от приемника подтвердить, что ее аргумент является действительным именем пользователя. (См. примечание.).
SEND		Начинает почтовую транзакцию, доставляющую данные на один или несколько терминалов (а не в почтовый ящик).
SOML		Начинает транзакцию MAIL или SEND, доставляющую данные на один или несколько терминалов или в почтовые ящики.
SAML		Начинает транзакцию MAIL и SEND, доставляющие данные на один или несколько терминалов и в почтовые ящики.
EXPN		Команда SMTP-приемнику подтвердить, действительно ли аргумент является адресом почтовой рассылки и если да, вернуть адрес получателя сообщения (expand).
HELP		Команда SMTP-приемнику вернуть сообщение-справку о его командах.
TURN		Команда SMTP-приемнику либо сказать ОК и поменяться ролями, то есть стать STMP-передатчиком, либо послать сообщение-отказ и остаться в роли SMTP-приемника.

Согласно спецификациям, команды, вычеркнутые в Таблице 2 (X), должны участвовать в любой реализации SMTP. Оставшиеся команды SMTP могут быть выполнены дополнительно.

Каждая команда SMTP должна заканчиваться пробелом (если это аргумент) или комбинацией CRLF. Слово «данные» используется в описании команды, а не <сообщение>. Он отметил, что SMTP позволяет передавать двоичную информацию, такую как графические или аудиофайлы, в

дополнение к тексту. Другими словами, SMTP может отправлять не только текстовые сообщения, но и данные любого контента.

Последовательность команд SMTP как упоминалось выше, SMTP обеспечивает двустороннюю связь между агентами доставки почты (MTA), клиентом и сервером. Клиенты отправляют команды на сервер, а серверы отвечают клиентам. Однако SMTP представляет последовательность команд SMTP.

В следующем примере (полностью взятом из RFC 821) показана типичная почтовая транзакция. Мистер Смит (на usc.edu) отправляет сообщение, например, Джонсу, Грин и Брауну (на mit.edu). Почтовый агент Mit.edu получает письма от мистера Джонса и Брауна, но не знает, где находится почтовый ящик мистера Грина.

Для дальнейшего разговора каждая строка пронумерована и показана кому - передатчик или приемник. Текст справа от <RECEIVER> или <SENDER> содержит информацию, которая была фактически отправлена. Трехзначная цифровая комбинация в начале данных строк указывает коды ответов (их значение будет объяснено позже). SMTP-ответ похож на сообщение с подтверждением доставки, поскольку он появляется только тогда, когда получатель получает данные.

Таблица 3 - Последовательность команд SMTP

Команда	Описание
RECEIVER	220 mit.edu Simple Mail Transfer Service Ready
SENDER	HELO usc.edu
RECEIVER	250 mit.edu
SENDER	MAIL FROM: <Smith@usc.edu>
RECEIVER	250 OK
SENDER	RCPT TO:<Jones@mit.edu>
RECEIVER	250 OK
SENDER	RCPT TO:<Green@mit.edu>
RECEIVER	550 No such user here
SENDER	RCPT TO:<Brown@mit.edu>
RECEIVER	250 OK
SENDER	DATA
RECEIVER	354 Start mail input; end with <CRLF>.<CRLF>
SENDER	Blah blah blah...
SENDER	...etc. etc. etc.
SENDER	.
RECEIVER	250 OK
SENDER	QUIT
RECEIVER	221 mit.edu Service closing transmission channel

Как видно из строки 1, когда SMTP-клиент устанавливает TCP-соединение с 25 протокольными портами, SMTP-сервер отвечает кодом 220.

Это означает, что соединение установлено успешно:

1. RECEIVER: 220 mit.edu Simple Mail Transfer Service Ready

После того как MTA компьютеров mit.edu и usc.edu установили соединение и обменялись приветствием, первой командой, согласно спецификации, должна быть команда HELO. Как указано в строке 2, SMTP-клиент передает HELO, указывая имя своего компьютера в качестве аргумента. Другими словами, он сообщает: <Привет, я - usc.edu>. Команда HELO употребляется с аргументом, как показано ниже:

2. SENDER: HELO usc.edu

В ответ на HELO приемник выдает код 250, сообщая передатчику о том, что команда принята и обработана:

3. RECEIVER: 250 mit.edu

После установления TCP-соединения и идентификации (при помощи HELO) SMTP-клиент приступает к почтовой транзакции. Для начала он выполняет одну из следующих команд: MAIL, SEND, SOML или SAML. В нашем примере использована команда MAIL:

4. SENDER: MAIL FROM:<Smith@usc.edu>

Все четыре команды, MAIL, SEND, SOML и SAML, имеют одинаковый синтаксис:

MAIL <пробел> FROM:<reverse-path> <carriage-return line-feed>

Примечание: Команды SEND, SOML и SAML дополнительны и используются довольно редко.

Аргумент <Reverse> сообщает серверу, который отправил соответствующее сообщение, если произошла ошибка. Давайте посмотрим на это более подробно. На данный момент для нас важно иметь адрес источника доказательства (в нашем случае, Smith @ usc, edu). После того как сервер предоставил код ответа 250 (строка 5) и согласился обработать сообщение через Smith@usc.edu, вы указываете получателя сообщения. Это делается с помощью команды RCPT.

Команда RCPT содержит аргумент - имя получателя. Каждая команда имеет только одно имя, поэтому при наличии нескольких получателей команда RCPT выдается несколько раз. В нашем примере команды RCPT выполняются в строках 6, 8 и 10. Синтаксис RCPT аналогичен синтаксису команды MAIL:

RCPT <пробел> TO: <прямой путь> <CRLF>

Однако, в отличие от MAIL, аргумент RCPT начинается с <TO:>. Содержание аргумента не вперед, а вперед. На данный момент для нас важно, чтобы имя почтового ящика получателя было указано в поле сообщения. После выдачи команды RCPT клиент MTA ожидает получить ответ с кодом 250. Однако в ответ на восьмую строчку

8. Отправитель: RCPT ВХОД: <Green@mit.edu>

Сервер отвечает кодом 550:

9. Хост: 550 Нет такого пользователя

Код ответа на 550 означает, что MTA не может выполнить запрос клиента, потому что он не знает, как доставить почту указанному пользователю. То есть мистер Грин не имеет почтового ящика на этом компьютере (Green @ mit, edu). Протокол SMTP утверждает, что сервер должен уведомить клиента о том, что у получателя нет почтового ящика. Однако в описании SMTP не указано, как клиент ответит на это сообщение.

После отправки всех команд RCPT клиент начинает отправку данных с помощью команды DATA. Строка 12 показывает, как клиент MTA (передатчик) отправляет команду DATA, а строка 13 показывает, как сервер отвечает кодом 354. Этот код разрешает отправлять данные и CRLF- <point> -CRLF (только новая пунктирная линия).

12. Отправитель: ИНФОРМАЦИЯ

13. Получатель: 354 Начните вводить почту; <CRLF> заканчивается. <CRLF>

После получения кода 354 клиент начинает отправку данных. Сервер MTA, в свою очередь, помещает полученные данные в очередь для входящих сообщений. Сервер не отправит ответ, указывающий, что передача данных завершена, пока он не получит комбинацию CRLF-point-CRLF от клиента. Как показано в строках 16 и 17, сервер генерирует код 250 в ответ на результирующую комбинацию CRLF- <point> -CRLF. Как уже упоминалось выше, код ответа 250 означает успешную работу:

16. Отправитель :

17. Приемник: 250 в порядке

Для завершения почтовой транзакции клиент должен отправить команду QUIT в соответствии с правилами SMTP. Сервер, в свою очередь, отвечает кодом 221. Этот код подтверждает, что соединение с клиентом закрыто, а затем соединение фактически закрыто:

18. ОТВЕТ: ВЫЙТИ

19. Получатель: служба 221 mit.edu закрывает канал распространения.

Клиент может использовать команды NOOP, HELP, EXPN и VRFY в любое время во время операции. В ответ на каждую команду сервер отправляет определенную информацию клиенту. Конечно, в зависимости от ответа клиент может предпринять определенные действия, но описание SMTP ничего не говорит об этом. Например, клиент MTA может отправить команду VRFY, чтобы проверить правильность входа в систему. Если сервер отвечает, что имя не существует, клиент MTA, возможно, не сможет отправить почту этому пользователю. В спецификации SMTP, но нет инструкции - клиент может ничего не делать в ответ на команду VRFY. Клиент MTA ничего не может сделать в ответ на команды NOOP, HELP и EXPN - ответственность полностью лежит на разработчике реализации MTA.

Коды ответов SMTP. Описание SMTP требует, чтобы сервер отвечал на каждую команду клиента SMTP. Сервер MTA отвечает комбинацией

трехзначных чисел, называемых кодом ответа. В дополнение к коду ответа обычно предоставляется одна или несколько строк текстовой информации.

Примечание. Обычно только несколько строк текста содержат команды EXPN и HELP. В спецификации SMTP ответ на любую команду может состоять из нескольких строк текста.

Каждое число в коде ответа имеет конкретное значение. Первое число указывает, была ли команда успешной (2), неудачной (5) или еще не выполнена (3). Как показано в Приложении E RFC 821, простой SMTP-клиент может анализировать только первую цифру ответа сервера и продолжать действовать соответствующим образом. Вторая и третья цифры кода ответа объясняют значение первой. Если вы создаете приложение SMTP, обязательно прочитайте схему всех кодов ответов SMTP. Дорожные коды, разработанные в SMTP, являются отличным примером разумного ведения бизнеса. Таблица 4 показывает возможные значения кодов ответа SMTP, определенных RFC 821.

Таблица 4 - Коды ответа SMTP и их значение

Код	Значение
211	Ответ о состоянии системы или помощь.
214	Сообщение-подсказка (помощь).
220	<имя_домена> служба готова к работе.
221	<имя_домена> служба закрывает канал связи.
251	Данный адресат не является местным; сообщение будет передано по маршруту <forward-path>.
354	Начинай передачу сообщения. Сообщение заканчивается комбинацией CRLF-точка-CRLF.
421	<имя_домена> служба недоступна; соединение закрывается.
450	Запрошенная команда почтовой транзакции не выполнена, так как почтовый ящик недоступен.
451	Запрошенная команда не выполнена; произошла локальная ошибка при обработке сообщения.
452	Запрошенная команда не выполнена; системе не хватило ресурсов.
500	Синтаксическая ошибка в тексте команды; команда не опознана.
501	Синтаксическая ошибка в аргументах или параметрах команды.
502	Данная команда не реализована.
503	Неверная последовательность команд.
504	У данной команды не может быть аргументов.
550	Запрошенная команда не выполнена, так как почтовый ящик недоступен.
551	Данный адресат не является местным; попробуйте передать сообщение по маршруту <forward-path>.
552	Запрошенная команда почтовой транзакции прервана; дисковое пространство, доступное системе, переполнилось.

Продолжение таблицы 4

553	Запрошенная команда не выполнена; указано недопустимое имя почтового ящика.
554	Транзакция не выполнена.
250	Запрошенное действие почтовой транзакции успешно завершилось

Многоцелевое расширение интернет почты (MIME). Многоцелевые расширения почты Интернета (MIME) улучшают возможности протокола SMTP, который может отправлять только 7-битные форматы ASCII на терминалы.

Другими словами, существуют ограничения SMTP. Например, не следует использовать языки, которые не поддерживают 7-битные символы (французский, немецкий, иврит, русский, китайский, японский). Вы также не можете использовать его для отправки двоичных файлов или отправки видео или аудио информации.

Многоцелевое расширение Internet Mail (MIME) - это дополнительный протокол, который позволяет отправлять сообщения с использованием данных, отличных от ASCII SMTP. MIME не является почтовым протоколом и исключает SMTP; это только расширяет его.

MIME преобразует данные не ASCII в ASCII и передает их SMTP-клиенту. Принимающий SMTP-сервер получает данные в формате ASCII и передает их в MIME для преобразования в исходный формат.

Легко сказать, что MIME - это набор программного обеспечения, который преобразует данные не ASCII в данные ASCII и наоборот.

Чтобы определить параметры преобразования MIME, определите пять тем, которые будут добавлены в исходный раздел заголовка SMTP:

- mine - версия (mine - версия);
- тип содержимого;
- контент - передача – кодирование;
- содержание – Id;
- содержание - описание.

Давайте посмотрим на них более подробно.

MIME - это версия. Тема определяет версию многоцелевого расширения, которое будет использоваться. Если текущая версия 1.1, то MIME - версия 1.1.

Тип содержимого.

Этот заголовок определяет тип данных в информационном блоке, используемом в сообщении. Тип содержимого и подтип содержимого разделяются косой чертой («прямой слеш»). В зависимости от подтипа тема может иметь другие параметры. Содержание - тип: <тип / подтип; настройки>.

MIME допускает семь различных типов данных. Они показаны в следующей таблице и более подробно обсуждаются ниже.

Таблица 5 - Типы и подтипы MIME

Тип	Подтип	Описание
Текст	Обычный	Неформатированный текст
Из многих частей	Смешанный	Информационный блок содержит упорядоченные различные типы данных
	Параллельный	То же самое, что выше, но неупорядоченное
	Обзорный	Похожий на смешанный, но по умолчанию /RFC822*
	Альтернативный	Часть различных версий в одинаковом сообщении
Сообщение	RFC822	Информационный блок включает в себя сообщение
	Частичный	Информационный – это фрагмент большого сообщения
	Внешний блок	Информационный блок является только ссылкой на другое сообщение
Изображение	JPEG	Изображение в формате JPEG.
	GIF	Изображение в формате GIF.
Видео	MPEG	Видео в MPEG-формате.
Аудио	Базовое	Одиночный канал кодированной речи на 8 кГц.
Прикладной текст	PostScript	Язык описаний страниц, разработанный фирмой Adobe Systems.

1.Текст. Исходное сообщение в 7-битовом формате ASCII и не нуждающееся в MIME-преобразовании. Имеется только один подтип, в настоящее время используется тип: обычный.

2.Из многих частей. Содержания блока информации многообразное и состоит из независимых частей. Заголовок из многих частей необходим, чтобы определить границу между каждой частью. Граница используется как параметр. Это символ строки, который повторяется перед каждой частью на отдельной линии и имеет предшествующие символы — два дефиса.

В этом типе определены четыре подтипа: смешанный, параллельный, обзорный и альтернативный.

В смешанном подтипе части должны быть представлены получателю в точном порядке, как в сообщении. Каждая часть имеет различный тип и определенную границу.

Параллельный подтип похож на смешанный подтип, за исключением того, что порядок частей не имеет значения.

Обзорный подтип также похож на смешанный подтип, за исключением того, что, по умолчанию, задается тип/подтип сообщений, как это будет определено ниже.

В альтернативном подтипе одно и то же сообщение повторяет использование одних и тех же форматов. Следующий пример сообщения использует из многих частей смешанный подтип:

Content-Type: multipart/mixed; boundary=xxxx

—xxxx

Content-Type: text/plain;

.....

—xxxx

Content-Type: image/gif;

.....

—xxxx

- Сообщение. В типе "сообщение" информационный блок содержит непосредственное почтовое сообщение, его часть или указатель на сообщение.

Используют три подтипа:

- RFC822;
- частичный;
- внешний информационный блок.

Подтип RFC822 применяется, если информационный блок включается в другое сообщение (в том числе заголовок и информационный блок).

Подтип частичный нужен, если исходное сообщение фрагментировано в различные почтовые сообщения и это почтовое сообщение — одна из частей. Фрагменты должны быть собраны заново с помощью MIME. При этом должны быть дополнены три параметра: id (идентификатор), number (номер), total (всего).

Введение id идентифицирует все сообщение, он представлен во всех фрагментах. Номер определяет последовательный порядок фрагментов. "Всего" определяет число фрагментов, составляющих исходное сообщение. Вот пример сообщения с тремя фрагментами:

Content-Type: message/partial;

Id="berlin.sut.ru";

Number=1;

Total=3;

.....

.....

Подтип "внешний информационный блок" показывает, что информационный блок не содержит непосредственно сообщения, а только ссылку (указатель) на исходное сообщение.

Ниже дан пример:

Content-Type: message/partial;

Name=book";

site=sut.ru;
access-type="ftp";
.....
.....

Изображение. Исходное сообщение "неподвижное изображение" указывает, что это не анимация. Применяется два подтипа: Joint Photographic Experts Group (JPEG), который использует сжатие изображения, и Graphics Interchange Format (GIF).

Видео. Исходное сообщение "изображение, изменяющееся по времени (анимация)" имеет только один тип — Motion Picture Experts Group (MPEG). Если анимационное изображение содержит звук, он должен быть послан отдельно с использованием типа "содержание аудио".

Приложение. Исходное сообщение "тип данных" предварительно не определяется. Имеется только два подтипа: поток октетов и PostScript. Поток октетов применяют, когда данные не могут быть интерпретированы как последовательность 8-битовых байтов (двоичный файл). PostScript нужен, когда данные в формате Adobe Post Script.

Содержание — Передача – Кодирование.

Заголовок определяет метод кодирования сообщения для передачи в виде нулей и единиц.

Content – Transfer – Encoding: <type>

Пять типов кодирования (поле <type>) приведены ниже.

Таблица 6 - Содержание – передача – кодирование

Тип	Описание
7 бит	NVT ASCII-символы и короткие линии
8 бит	Не-ASCII-символы и короткие линии
Двоичный	Не-ASCII-символы с не лимитированной длиной линии
Базовый 64	64-битовые блоки данных, закодированные по 8 бит ASCII-символами
Предназначенный для печати	Не-ASCII-символы, закодированные как последовательность знаков ASCII

- 7 бит. 7-битовое NVT ASCII-кодирование. Хотя не надо делать никаких преобразований, но число символов в строке не должно превышать 1000 символов. ASCII определяет 128 букв, включая алфавит, числа, знаки пунктуации и сигналы. Заглавная буква "С", например, кодируется 100011, а цифра "3" — 0110011. Таким образом, с помощью нулей и единиц можно закодировать 128 символов.
- 8 бит. Это 8-битовое кодирование, одна из важнейших модификаций кода ASCII, называемая расширенный ASCII. К 7-битовому коду добавляется еще один бит и к используемым 127 символам можно добавлять другие, например, иностранные буквы или другие полезные символы. 8-битовые не-

ASCII-символы передаются с длиной 8-й строки не более 1000 символов. MIME не делает никакой перекодировки. Основные протоколы STMP могут передать не-ASCII-символы. Это, однако, не рекомендуется. Типы "Базовый 64" и "Предназначенный для печати" предпочтительнее.

Двоичный. Это 8-битовое кодирование. Не ASCII-символы передаются с длиной 8 бит. Протоколы STMP могут передать не ASCII-символы. Это, однако, не рекомендуется. Типы "Базовый 64" и "Предназначенный для печати" предпочтительнее.

Base 64 (Базовый 64). Это решение предложено для передачи данных, представленных в виде байтов, где старший бит не обязательно равен нулю. BASE 64 преобразует этот тип данных в символы, пригодные для печати, которые можно передавать как ASCII-символы, или в набор символов, поддерживаемых основными программами для передачи почты.

Base64 – способ кодирования произвольных двоичных данных в ASCII текст. По своей сути кодирование очень простое. Общеизвестно, что в один байт можно вложить 256 цифр, от 0 до 255. Однако, если вместо восьми бит использовать только шесть, то объем вложенной информации уменьшается до 64 цифр, от 0 до 63.

Любую цифру 6-ти битового байта можно представить в виде печатного символа. Таким образом, каждые шесть бит на входе кодируется в один из символов 64-буквенного us-ascii алфавита – это A-Z, a-z, 0-9,+,/ и знак “ = ” в качестве заполняющего символа в конце.

Таблица 7- Алфавит Base64

Значение Код	Значение Код	Значение Код	Значение Код
0 A	17 R	34 i	51 z
1 B	18 S	35 j	52 0
2 C	19 T	36 k	53 1
3 D	20 U	37 l	54 2
4 E	21 V	38 m	55 3
5 F	22 W	39 n	56 4
6 G	23 X	40 o	57 5
7 H	24 Y	41 p	58 6
8 I	25 Z	42 q	59 7
9 J	26 a	43 r	60 8
10 K	27 b	44 s	61 9
11 L	28 c	45 t	62 +
12 M	29 d	46 u	63 /
13 N	30 e	47 v	
14 O	31 f	48 w	= (заполнитель)
15 P	32 g	49 x	
16 Q	33 h	50 y	

Для передачи двоичных файлов повсеместно используется base64. Вкратце процесс кодирования можно описать так:

1. Битовый поток разбивается по 24 бита (по 3 байта), которые в свою очередь делятся на четыре части по 6 бит.
2. Каждая такая часть кодируется одним из 64 ASCII символов (отсюда название - base64).

Схематично такое "деление три к четырем" можно представить себе так:

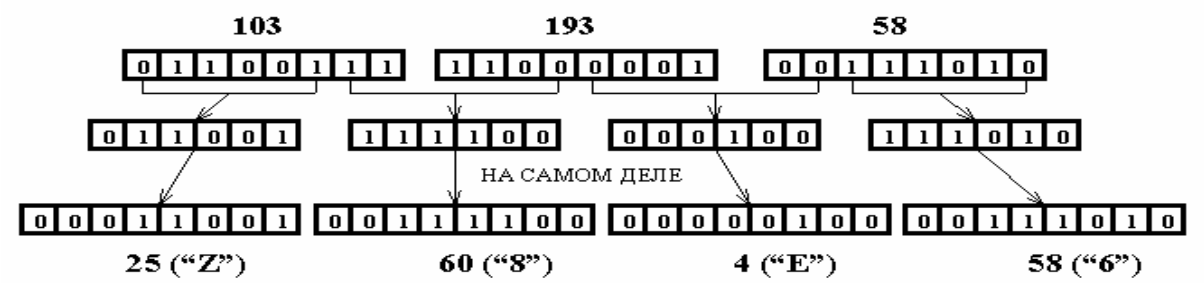

Рисунок 7 - Алгоритм кодирование base64

В этом примере три числа 103, 193 и 58 кодируются в базовом формате 64. В результате мы получили четырехзначную серию Z8E6.

Исходя из этого принципа, мы можем кодировать любую двоичную информацию в тексте и не увеличивать ее объем (на 30%). Затем через почтовый сервер наша информация достигает нужного места, чья почта шифрует текст в двоичный файл.

Если при преобразовании четырех символов друг в друга получаются только 3, 2 или 1, пустые байты заполняются знаком «=». Например: Z8E =, Z8 == или Z ===.

В заключение приведем несколько примеров использования MIME. Название указывает, что MIME 1.0 используется. Сообщение состоит из двух частей. На это указывает тип содержимого сообщения: Тип содержимого: многосторонний / альтернативный. Каждая часть определяется разделителем:

border = «---- = _Следующий раздел_001_01BE54E2.10C07C70»

Конец сообщения также помечен разделителем. Первый раздел содержит простой русский текст, закодированный для передачи koi8-r, с использованием 64 основных кодировок для его передачи. Вторая часть - это документ в формате MS Word. Кодировка была также использована для отправки. Кроме того, если почтовый клиент «знает», как управлять форматом DOC, информация отображается непосредственно в тексте сообщения: Content-Disposition: Embedded.

From user@email.net Wed Feb 10 16:15:17 1999
To: "Sergey Makarov (E-mail)"
Subject: FW: please resend it, because i can't translate it at work
Date: Wed, 10 Feb 1999 09:30:57 +0300
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.1960.3)

Content-Type: multipart/alternative;
boundary="---- =_NextPart_001_01BE54E2.10C07C70"
This message is in MIME format. Since your mail reader does not understand this format, some or all of this message may not be legible.
------ =_NextPart_001_01BE54E2.10C07C70
Content-Type: text/plain; charset="koi8-r"
Content-Transfer-Encoding: base64
DQoNCi0tLS0tT3JpZ2luYWwgTWVzc2FnZS0tLS0tDQpGcm9tOiBqb2huQHZ0YXUtYnNkLnBzdHUu
YWMucnUgW21haWx0bzpqb2huQHZ0YXUtYnNkLnBzdHUuYWMucnVdIA0KU2VudDogTW9uZGF5LCBG
ZWJydWFyeSAwOCwgMTk5OSAxOjM3IFBNDQpTdWJqZWN0OiANCg0KDQrN8yDt4Oru7eXpCPcICPYt
------ =_NextPart_001_01BE54E2.10C07C70
Content-Type: application/msword
Content-Disposition: inline
Content-Transfer-Encoding: base64
PCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDMuMi8vRU4iPg0KPEhUTUw+
DQo8SEVBRD4NCjxNRVRBIEhUVFAtRVFVSVY9IkNvbnRlbnQtVHlwZSIgQ09OVEVOVD0idGV4dC9o
dG1sOyBjaGFyc2V0PWtvaTgtciI+DQo8TUVUQSBOQU1FPSJHZW5lcmF0b3IiIENPTlRFTlQ9Ik1T
------ =_NextPart_001_01BE54E2.10C07C70-

Протокол POP3 -- Post Office Protocol.

Почтовый протокол (POP) - это протокол доставки почты пользователю из почтового ящика почтового сервера POP. Многие из концепций, принципов и концепций протокола POP выглядят и работают как SMTP. Команды POP такие же, как команды SMTP, которые отличаются некоторыми деталями.

В настоящее время существует две версии протокола POP - POP2 и POPZ, которые имеют примерно одинаковые возможности, но не совместимы друг с другом. Дело в том, что протоколы POP2 и POPZ имеют разные номера портов. POP3 не является расширением или модификацией POP2 - это совершенно другой протокол. POP2 определен в RFC 937 (Post Office Protocol-Version 2, Butler et al., 1985), а POP3 определен в RFC 1225 (Post Office Protocol-Version 3, Rose, 1991).

Назначение протокола POPP.

В прошлом многие сети отправляли почту напрямую с одного компьютера на другой. Если пользователь часто меняет рабочие компьютеры или один компьютер принадлежит более чем одному пользователю, возникли определенные проблемы. В настоящее время сообщения доставляются не на компьютеры пользователя, а в специальные почтовые ящики, которые круглосуточно работают (подключаются) к почтовому серверу организации.

Описание протокола POPP.

Структура протокола POPZ позволяет пользователю получить доступ к своему почтовому серверу и получить собранное для него сообщение. Пользователь может получить доступ к серверу POP с любой точки доступа в Интернет.

Он также должен запустить специальный почтовый агент (UA), работающий по протоколу POPZ, и настроить его для работы со своим почтовым сервером. Таким образом, в начале модели POP находится персональный компьютер, который выступает в роли клиента почтовой системы (сервера).

На рисунке 8 показана модель клиент-сервер с использованием протокола POP. Сервер POP расположен между агентом пользователя и почтовыми ящиками.

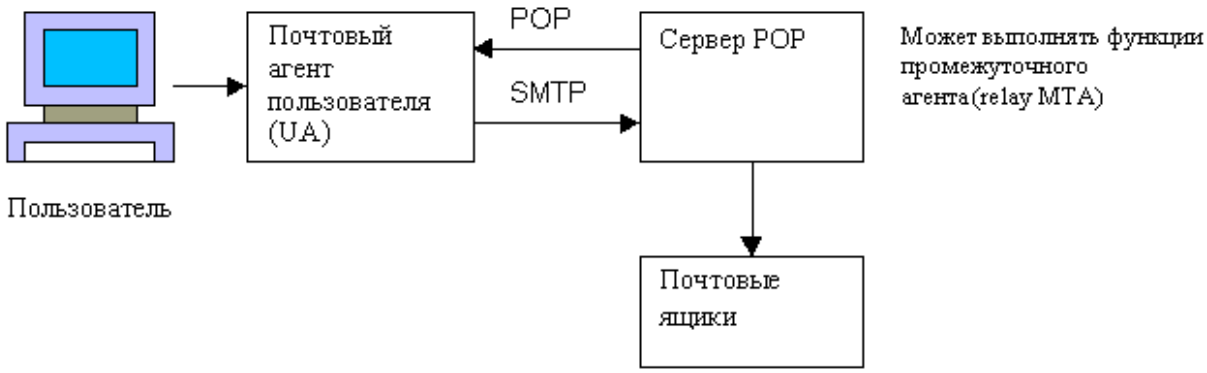

Рисунок 8 - Конфигурация модели клиент-сервер по протоколу POP

Также отметим, что сообщения доставляются клиенту по протоколу POP, но отправляются по протоколу SMTP. То есть компьютер пользователя имеет два отдельных агентских интерфейса для почтовой системы - доставку (POP) и отправку (SMTP). Разработчики протокола PORZ называют эту ситуацию «распределенными агентами» (UA UA). Концепция отдельных агентов кратко обсуждается в спецификации POPP.

Протокол POPP предусматривает три этапа процесса переписки: авторизация, транзакция и обновление.

Как только сервер PORZ и клиент установили соединение, начинается фаза авторизации. На этапе авторизации клиент идентифицирует себя с сервером.

Если авторизация прошла успешно, сервер откроет почтовый ящик клиента и начнется фаза транзакции. Там клиент запрашивает информацию с сервера (например, список почтовых сообщений) или просит его выполнить определенное действие (например, вывести почтовое сообщение).

Наконец, сеанс связи заканчивается на этапе обновления. В таблице 8 показаны команды протокола POPZ, необходимые для входа в Интернет в минимальной конфигурации.

Таблица 8 - Команды протокола POP версии 3 (для минимальной конфигурации)

Команда	Описание
USER	Идентифицирует пользователя с указанным именем
PASS	Указывает пароль для пары клиент-сервер
QUIT	Закрывает TCP-соединение
STAT	Сервер возвращает количество сообщений в почтовом ящике плюс размер почтового ящика
LIST	Сервер возвращает идентификаторы сообщений вместе с размерами сообщений (параметром команды может быть идентификатор сообщения)
RETR	Извлекает сообщение из почтового ящика (требуется указывать аргумент-идентификатор сообщения)
DELE	Отмечает сообщение для удаления (требуется указывать аргумент - идентификатор сообщения)
NOOP	Сервер возвращает положительный ответ, но не совершает никаких действий
LAST	Сервер возвращает наибольший номер сообщения из тех, к которым ранее уже обращались
RSET	Отменяет удаление сообщения, отмеченного ранее командой DELE

Протокол POPP определяет несколько команд, но они дают только два ответа: + OK (положительный) и -ERR (отрицательный). Оба ответа подтверждают, что к серверу обращаются и отвечают на общие команды. Как правило, за каждым ответом следует содержательное словесное описание. RFC 1225 предлагает несколько моделей сессий POPZ. Теперь рассмотрим несколько из них, которые позволят вам получить последовательность команд при обмене между сервером и клиентом.

Авторизация пользователя.

После того, как программа установит TCP-соединение с портом протокола POP3 (официальный номер 110), вы должны отправить команду USER с именем пользователя в качестве пароля. Если сервер отвечает + OK, вы должны отправить этому пользователю команду PASS с паролем:

CLIENT: USER marat

SERVER: +OK

CLIENT: PASS secret

SERVER: +OK marat's maildrop has 2 messages (320 octets)

(В почтовом ящике marat есть 2 сообщения (320 байтов) ...)

Транзакции POP3.

В конце периода авторизации переходит к этапу транзакции. Следующие примеры показывают возможный обмен сообщениями в это время.

Команда STAT возвращает количество сообщений и количество байтов в сообщении:

CLIENT: STAT

SERVER: +OK 2 320

Команда LIST (без параметра) возвращает список сообщений в почтовом ящике и их размеры:

CLIENT: LIST

SERVER: +OK 2 messages (320 octets)

SERVER: 1 120

SERVER: 2 200

SERVER: . ...

Команда LIST с параметром возвращает информацию о заданном сообщении:

CLIENT: LIST 2

SERVER: +OK 2 200 ...

CLIENT: LIST 3

SERVER: -ERR no such message, only 2 messages in maildrop

Команда TOP возвращает заголовок, пустую строку и первые десять строк тела сообщения:

CLIENT: TOP 10

SERVER: +OK

SERVER: <the POP3 server sends the headers of the message,a blank line, and the first 10 lines of the message body>

(сервер POP высылает заголовки сообщений, пустую строку и первые десять строк тела сообщения)

SERVER: . ...

CLIENT: TOP 100

SERVER: -ERR no such message

Команда NOOP не возвращает никакой полезной информации, за исключением позитивного ответа сервера. Однако позитивный ответ означает, что сервер находится в соединении с клиентом и ждет запросов:

CLIENT: NOOP

SERVER: +OK

Следующие примеры показывают, как сервер POP3 выполняет действия. Например, команда RETR извлекает сообщение с указанным номером и помещает его в буфер местного UA:

CLIENT: RETR 1

SERVER: +OK 120 octets

SERVER: <the POPS server sends the entire message here>

(POP3-сервер высылает сообщение целиком)

SERVER: . . . . . .

Команда DELE отмечает сообщение, которое нужно удалить:

CLIENT: DELE 1

SERVER: +OK message 1 deleted ...

(сообщение 1 удалено)

CLIENT: DELE 2

SERVER: -ERR message 2 already deleted

сообщение 2 уже удалено)

Команда RSET снимает метки удаления со всех отмеченных ранее сообщений:

CLIENT: RSET

SERVER: +OK maildrop has 2 messages (320 octets) (в почтовом ящике 2 сообщения (320 байтов))

Как и следовало ожидать, команда QUIT закрывает соединение с сервером:

CLIENT: QUIT

SERVER: +OK dewey POP3 server signing off

CLIENT: QUIT

SERVER: +OK dewey POP3 server signing off (maildrop empty)

CLIENT: QUIT

SERVER: +OK dewey POP3 server signing off (2 messages left)

Обратите внимание на то, что отмеченные для удаления сообщения на самом деле не удаляются до тех пор, пока не выдана команда QUIT и не началась стадия обновления. В любой момент в течение сеанса клиент имеет возможность выдать команду RSET, и все отмеченные для удаления сообщения будут восстановлены.

Протокол IMAP4.

POP3, который является одним из самых популярных протоколов для получения сообщений электронной почты с почтового сервера, имеет несколько недостатков. Наиболее важным из них является невозможность контролировать перемещение и хранение сообщений на сервере. Сообщения обычно загружаются сразу с почтового сервера, а затем они удаляются с сервера, то есть вы не можете выбирать сообщения.

Такая схема хороша только для интернет-провайдера, который обслуживает почтовый сервер вашей организации, так как экономит дисковое пространство на сервере. Однако эта ситуация не удовлетворяет пользователей, потому что, когда они получают почту, они ограничены только одним компьютером, на который можно загружать сообщения. Нет проблем, когда пользователи получают почту через локальную сеть и только на конкретном компьютере. Если они хотят получить письмо, как на работе, так и дома, сразу возникает много проблем. В этом случае сообщения отправляются после получения между двумя рабочими станциями, которые расположены в разных местах.

Протокол Internet Mail Access Protocol (IMAP) был разработан для решения таких проблем. Он был разработан в Университете Вашингтона и позволяет пользователям получать электронные письма из одного и того же почтового ящика из разных мест. Пользователь может управлять сообщениями в почтовом ящике и дополнительными функциями обслуживания почтовых ящиков на сервере.

Конечно, у этой монеты есть одна сторона - почтовый сервер должен обслуживать все сообщения на жестком диске. Это может создать опасную ситуацию на жестком диске, которая не будет беспокоить администратора почтового сервера. При управлении почтовым сервером на основе IMAP необходимо соблюдать осторожность, чтобы ограничить дисковое пространство, чтобы система перестала своевременно получать новые сообщения и предотвращала переполнение диска и отключение сервера.

Существенное различие между протоколом IMAP4 и протоколом POP3 поддерживает работу с системой каталогов сообщений (или папок) IMAP4. IMAP4 позволяет управлять каталогами (папками) удаленных сообщений, как если бы они находились на локальном компьютере.

IMAP4 клиент:

- создавать, удалять и переименовывать почтовые ящики;
- проверять наличие новых сообщений;
- удаление старых.

Поскольку IMAP4 поддерживает уникальный механизм идентификации для каждого сообщения в почтовом ящике клиента, он позволяет только читать сообщения из почтового ящика, которые соответствуют определенным условиям или их частям, изменять атрибуты сообщения и перемещать отдельные сообщения.

Принципы работы.

Протокол IMAP4 работает в верхней части протокола передачи, обеспечивая надежный и надежный канал передачи данных между клиентом и сервером IMAP4. При работе в TCP IMAP4 использует порт 143. Команды и данные IMAP4 отправляются через протокол передачи, отправленный сервером или пользователем.

Принцип передачи данных IMAP4 такой же, как и у других аналогичных протоколов. Сначала поприветствуйте клиента и сервер. Клиент отправляет команды на сервер, а сервер отправляет информацию и сообщения о состоянии запроса на сервер. Когда обмен завершен, канал закрывается.

Весь обмен данными между клиентом и сервером организован в виде строк, заканчивающихся символами <CRLF> или в виде последовательности байтов заданной длины.

Любая процедура начинается с команды клиента. Каждая команда клиента начинается с идентификатора или фамилии команды. Тег обычно представляет собой короткую строку букв и цифр (например, A0001, A0002 и т. д.). Тег - это уникальный идентификатор команды клиента. Ответы сервера

или следующие команды клиента могут связываться с этой командой своим собственным тегом.

Каждая команда клиентов начинает новую линию. Если команда предоставляет поток данных заданной длины или если команде требуется ответ от сервера для продолжения работы (например, во время аутентификации), она может получить несколько путей.

Строки данных, отправляемые с сервера в ответ на команду клиента, не должны иметь тега, но могут иметь знак «*». Это означает, что они являются промежуточными строками потока ответа, а их идентификатор команды находится в последней строке потока. Никакая другая команда не может переключиться на такой поток данных.

Если сервер обнаруживает ошибку в команде, он отправляет клиенту сообщение BAD с тегом команды error. Если команда обработана успешно, возвращается сообщение OK со значком команды. Если команда возвращает отрицательный результат, например, если эта команда не может быть выполнена, возвращается предупреждение NO со знаком неудачной команды.

Важной особенностью протокола IMAP является то, что взаимодействие между клиентом и сервером не основано на принципе «ответа на запрос», каждая сторона в свою очередь «уходит».

Клиент может отправлять новую команду на сервер, не ожидая ответа на предыдущую команду, конечно, если эти команды не связаны друг с другом или ответ одной не влияет на результат другой.

Сервер может обрабатывать несколько команд одновременно и отвечать на каждую из них. В этом случае ответ на команду может прийти позже, поэтому ответ сервера всегда включает свободное имя команды, которая ему принадлежит.

Для работы в этом режиме клиент и сервер должны регистрировать весь поток данных обмена, поскольку и сервер, и клиент могут ссылаться на команды и данные, введенные на предыдущих этапах сеанса обмена, в своих запросах и ответах.

Чтобы обеспечить гибкость и универсальность операций обмена сообщениями, почтовые системы IMAP присваивают сообщениям определенные атрибуты.

Атрибуты сообщений системы IMAP.

Каждое сообщение в почтовой системе для работы с IMAP имеет уникальный идентификатор, с помощью которого вы можете получить доступ к этому сообщению. Уникальный UID - это 32-разрядное число, которое идентифицирует сообщение в папке. Всем сообщениям в папке назначается максимальное количество сообщений UID, которые ранее были в этой папке. Уникальные идентификаторы сообщений хранятся от сеанса к сеансу и могут использоваться для синхронизации, например, мобильных пользовательских каталогов.

Каждая папка в системе также имеет уникальный идентификатор (UIDVALIDITY). Вместе с сообщением UID эта пара образует 64-битное

число, которое идентифицирует каждое сообщение. Если сообщение UID хранится постоянно, UIDVALIDITY в этом сеансе должно быть больше, чем в предыдущем сеансе.

В дополнение к уникальному идентификатору сообщение в системе IMAP имеет серийный номер, что означает, что все сообщения в этом почтовом ящике нумеруются последовательно. Если новое сообщение добавлено в почтовый ящик, ему будет присвоен номер, превышающий количество сообщений в почтовом ящике.

Когда вы удаляете сообщение из этой папки, порядковые номера всех сообщений пересчитываются, поэтому порядковый номер сеанса может измениться во время сеанса. Большинство команд IMAP4 работают с порядковыми номерами сообщений, а не с UID.

Флаги присваиваются сообщениям, отличным от числовых идентификаторов. Некоторые флаги могут быть действительными для данного сообщения от сеанса к сеансу, другие только для этого сеанса. Наиболее распространенными из них являются:

«\ Seen» означает, что сообщение было прочитано

«\ Отвечено» - ответил на сообщение

«\ Удалено» - сообщение, помеченное для удаления

"\ Project" - это сообщение еще не завершено

Сообщение «\ скоро» - «просто» прибыл в почтовый ящик, что означает, что этот сеанс будет первым, кто прочитает это сообщение.

«\ Скоро» - это пример флага, который не будет сохранен в следующем сеансе

Кроме того, дата и время получения сообщения сервером сохраняются на сервере IMAP. Например, если сообщение получено через SMTP, оно регистрируется:

- дата и время доставки до места назначения;
- общий размер сообщения;
- состав конверта сообщения (тема);
- структура сообщения (структура MIME).

Основные команды.

IMAP4 - это гибкий и многофункциональный протокол со многими функциями. Он обслуживает команду из более чем 20 различных клиентов для управления статусом своей почты. Подробное описание всех команд и ответов сервера IMAP4 можно найти в RFC-2060. Далее описаны только некоторые команды клиента, а примеры их обработки показывают общую схему взаимодействия между клиентом и сервером IMAP4.

IMAP4 поддерживает текстовые команды и ответы сервера, то есть последовательности символов ASCII. Строка команды или данных заканчивается строкой <CRLF>. Согласно спецификации MIME, 8-битные данные не могут быть отправлены «открыто» через IMAP4. Как правило, приложения IMAP4 кодируют свои base64 перед отправкой двоичных данных.

Сервер 1MAP4 обрабатывает команды в зависимости от одного из четырех мест:

1. Неаутентифицированное состояние, которое клиент должен зарегистрировать на сервере, чтобы начать работать.

2. Режим аутентификации, где клиент может выбрать папку сообщений для работы.

3. Состояние работы с почтовым ящиком, где клиент выполняет основную работу с сообщениями.

4. Отключите состояние, когда сервер завершает клиентскую операцию.

Кроме того, при описании команд символ «S:» указывает поток данных от сервера IMAP4, а символ «C:» указывает поток данных от клиента.

ВХОД команда. После того как соединение установлено с использованием транспортного протокола (например, TCP) и строка приветствия покидает сервер, клиент должен быть зарегистрирован в системе. Команда LOGIN часто используется для этого. Свидетельство для командной строки с идентификатором клиента и паролем:

S: * OK Служба IMAP4revl готова

C: A00l Войти Али Сезаро

S: A00l OK ВХОД ВХОД

Команда LOGIN отправляет пароль и идентификатор пользователя по сети в виде простого текста. Если пользователю необходимо защитить свою почтовую информацию, он может использовать команду AUTHENTICATE.

После регистрации в системе клиент должен выбрать каталог (папку) сообщений, над которыми он работает. Каталог выбирается командой SELECT. Аргументом команды является имя почтового каталога:

C A142 SELECT INBOX

S * 172 EXISTS

S * 1 RECENT

S * OK [UNSEEN 12] Message 12 is first unseen

S * OK [UIDVALIDITY 3857529045] UIDs valid

S * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)

S * OK [PERMANENT FLAGS (\Deleted \Seen *)] Limited

S A142 OK [READ-WRITE] SELECT completed

Сервер IMAP4 передает атрибуты этого каталога клиенту, прежде чем подтвердить, что обработка команды завершена. В приведенном выше примере:

1. В папке «INBOX» - 172 сообщения (строка «* 172 ВСЕГО»).

2. Один из них пришел недавно (строка «* 1 ПОСЛЕДНИЕ»).

3. В папке есть непрочитанные сообщения, минимальное количество непрочитанных сообщений - 12 («OK [UNSEEN 12] 12 сообщений не появляются первыми»).

4. Уникальный идентификатор времени папки INBOX в этом сеансе: 3857529045 (строка «* OK [UIDVALIDITY 3857529045J UID действительны»).

5. Сообщения в этой папке могут содержать флаги, помеченные в поле FLAGS («* FLAGS (\ Responded \ Marked \ Deleted \ Viewed \ Project)»).

6. Клиент может изменить флаги «\ удален» и «\ видимый» для сообщений («* OK [PERMANENTFLAGS (\ Off \ Seen \ *)] ограничено»).

7. Клиент имеет право написать и прочитать сообщение из INBOX (строка «A142 OK [READ-WRITE] SELECT complete»).

Команда SELECT устанавливает текущий каталог для работы клиента. Если пользователю нужна информация о состоянии каталога, используйте команду EXAMINE вместе с именем каталога в качестве доказательства для команды, например:

C: A932 NAME

S: * 17 БАР

Команда EXAMINE возвращает настройки команды SELECT и отличается от команды SELECT тем, что открывает только указанный почтовый ящик для чтения.

Если вам нужно запросить состояние папки без изменения текущего каталога, вы можете использовать команду STATUS. Для этой команды заданы следующие параметры:

- имя папки;
- тип запрашиваемой информации.

В зависимости от типа, команда может быть возвращена:

- количество сообщений в папке;
- количество новых сообщений;
- количество непрочитанных сообщений;
- каталог UIDVALIDITY;
- номер UID следующего сообщения, которое будет добавлено в эту папку.

Например:

C: A042 STATUS blob (MESSAGES UNSEEN)

S: * STATUS blob (MESSAGES 231 UNSEEN 12) '

S: A042 OK STATUS completed

Вы можете использовать команду LIST для получения списка папок (подкаталогов), расположенных в определенной папке и доступных клиенту.

Командные аргументы:

- название каталога;
- список подкаталогов, которые мы хотим получить (пустая строка - "" означает текущий каталог) и маску имен подкаталогов.

В зависимости от реализации почтовой системы и структуры описания иерархии папок, имена каталогов и маски подкаталогов могут интерпретироваться по-разному. Например, вы можете получить список папок в корне:

C: СПИСОК A004 «/» *

S: * LIST (\ Noinferiors) «/» INBOX

S: * LIST (\ Noinferiors) «/» ВНЕШНИЙ ВИД

S: * LIST (\ Noinferiors) «/» WasteBox

S: A004 OK LIST завершен

Ответ сервера содержит список папок в соответствии с иерархией и флагами этих папок (флаг «\ Noinferiors» означает, что эта папка не имеет иерархии и не может быть создана).

Получив информацию в каталоге, пользователь может прочитать любое сообщение или определенную группу сообщений, часть сообщения или определенные атрибуты сообщения. Для этого используйте команду FETCH.

Доказательством для этой команды является порядковый номер сообщения и критерии запроса. Критерии описывают тип возвращаемой информации.

Например, вы можете запросить заголовки и сообщения UID в папке или сообщения с определенными флагами или без них. Заголовки сообщения запроса с серийным номером, расположенным в INBOX

10 до 12, будет выглядеть так:

C: A654 FETCH 10:12 BODY[HEADER]

S: * 10 FETCH (BODY[HEADER] (350)

S: Date: Wed, 17 Jul 1996 02:23:25 -0700 (PDT)

S: From: manSglobe.com

S: Subject: Hi

S: To: imapSworld.edu

S: Message-Id: <B27397-0100000@world.edu>

S: MIME-Version: 1.0

S: Content-Type: TEXT/PLAIN; CHARSET=US-ASCII

S:)

S: *11 FETCH ....

S: * 12 FETCH ....

S: A654 OK FETCH completed

После просмотра сообщения пользователь может сохранить его с другими флагами, добавить или удалить флаги сообщения (например, установите флажок, чтобы удалить это сообщение). Для этого используйте команду STORE.

Командные аргументы:

- номера сообщений;
- идентификатор операции;
- список флагов.

Например, операция добавления флага удаления ("\Deleted") трем сообщениям выглядит следующим образом:

C: AOO3 STORE 2:4 +FLAGS (\Deleted)

S: * 2 FETCH FLAGS (\Deleted \Seen)

S: * 3 FETCH FLAGS (\Deleted)

S: * 4 FETCH FLAGS (\Deleted \Flagged \Seen)

S: AOO3 OK STORE completed

В ответ на выполнение команды отправляются строки новых флагов указанного сообщения.

Пользователь также может организовать поиск сообщений по определенным критериям. Для этого используйте команду ПОИСК. Критерии поиска состоят из комбинации нескольких поисковых терминов, а результат поиска содержит множество сообщений, расположенных на пересечении этих терминов.

Условия распространяются на:

- состав, структура или тема сообщения;
- по размерам флагов;
- идентификаторы;
- периоды уведомления дней.

Результатом команды является строка, состоящая из последовательных номеров сообщений, которые соответствуют критериям поиска. Например, 1 марта 2016 года. Поиск всех непрочитанных сообщений от Смита выглядит следующим образом:

C: A282 SEARCH UNSEEN FROM "Smith" SINCE l-Mar-2016

S: * SEARCH 2 84   882

S: A282 OK SEARCH completed

Результатом поиска будут сообщения с последовательными номерами 2, 84 и 882.

IMAP4 позволяет не только искать и читать сообщения в каталогах, этот протокол позволяет добавлять, копировать и перемещать сообщения в каталоги. Добавление сообщения в папку можно осуществить командой APPEND:

C: AOO3 APPEND saved-messages (\Seen) {310}

C : Date: Mon, 7 Feb 1997 21:52:25 -0800 (PST)

C: From: Fred Foobar <foobar@Blurdybloop.COM>

C: Subject: afternoon meeting

C: To: mooch@owatagu.siam.edu

C: Message-Id: <B27397-0100000@Blurdybloop.COM>

C: MIME-Version: 1.0

C: Content-Type: TEXT/PLAIN; CHARSET=US-ASCII

C:

C: Hello Joe, do you think we can meet at 3:30 tomorrow

C : S AOO3 OK APPEND completed

Отметим, что команда APPEND не осуществляет доставку сообщения по указанному адресу, она только размещает в данном каталоге набор строк в виде сообщения.

Если сервер IMAP4 поддерживает 8-битовые данные, можно добавлять тексты сообщений в 8-битной кодировке, иначе текст должен быть закодирован в одну из 7-битных кодировок.

Команда COPY копирует сообщения с заданными порядковыми номерами в указанный каталог, например:

C: AOO3 COPY 2:4 MEETING
S: AOO3 OK COPY completed

Более подробное описание этих и других команд управления каталогами и сообщениями вы можете найти, например, в RFC-2060.

Пример сценария

Далее приведен простейший сценарий сессии работы IMAP4-клиента с сервером.

S: * OK IMAP4revl Service Ready
C: A00l login alladin sesam
S: A00l OK LOGIN completed
C: A002 SELECT inbox
S: * 18 EXISTS
S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S: * 2 RECENT
S: * OK [UNSEEN 17] Message 17 is the first unseen message
S: * OK [UIDVALIDITY 3857529045] UIDs valid
S: A002 OK [READ-WRITE] SELECT completed

C: A003 FETCH 12 body[header]
S: * 12 FETCH (BODY[HEADER] {350}
S: Date: Wed, 17 Jul 1996 02:23:25 -0700 (PDT)
S: From: gray@cac.Washington.edu
S: Subject: IMAP4revl WG mtg summary and minutes
S: To: imap@cac.Washington.edu
S: Message-Id: <B27397-0100000@cac.Washington.edu>
S: MIME-Version: 1.0
S: Content-Type: TEXT/PLAIN; CHARSET=US-ASCII
S:
S:)
S: A003 OK FETCH completed

C: A004 STORE 12 +flags \deleted
S: * 12 FETCH (FLAGS (\Seen \Deleted))
S: A004 OK +FLAGS completed

C: A005 LOGOUT
S: * BYE IMAP4revl server terminating connection
S: A005 OK LOGOUT completed

2 БЕЗОПАСНОСТЬ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

2.1 Межсетевые экраны

Межсетевой экран, firewall - программный или программно-аппаратный элемент компьютерной сети, который отслеживает и фильтрует проходящий через него трафик в соответствии с установленными правилами.

Другие названия:

Brandmauer (немецкий: Brandmauer) - термин, производный от немецкого языка;

Брандмауэр - это английский термин.

Хакеры используют для взлома уязвимостей:

- протоколы модели сети OSI;
- программное обеспечение, установленное на компьютерах сети.

Основной задачей брандмауэров является защита периметра или сегментов сети, а также отдельных узлов от несанкционированного доступа.

Наиболее распространенное место установки брандмауэров - по периметру локальной сети для защиты внутренних хостов от внешних атак.

Однако их можно размещать не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.

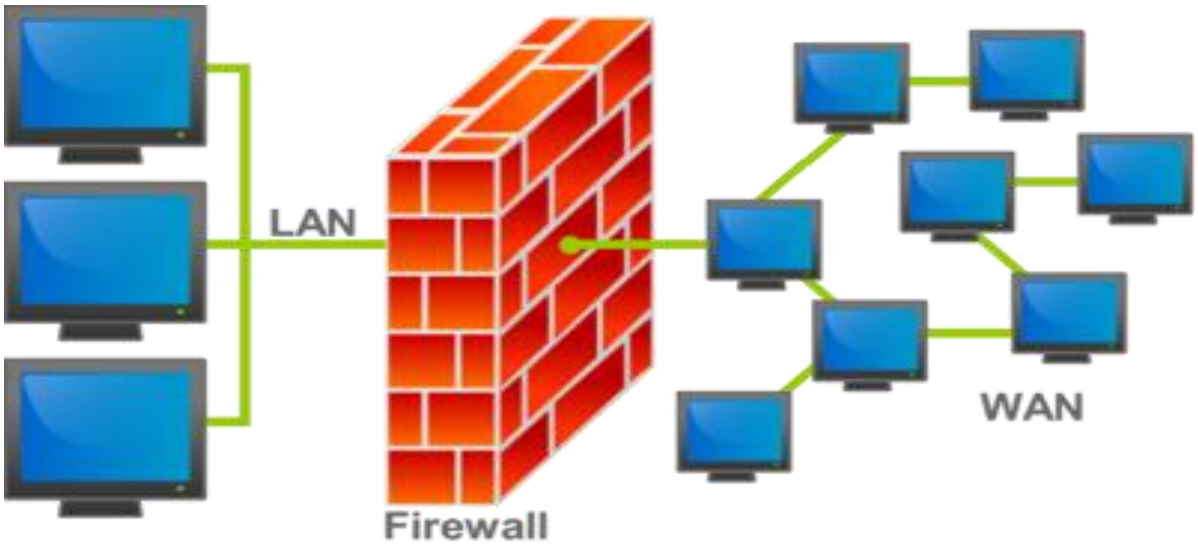

Рисунок 9 - Межсетевой экран на границе сетевого периметра.

Блокируйте или блокируйте трафик, сравнивая характеристики межсетевых экранов с предопределенными моделями.

Брандмауэр пропускает весь трафик и принимает решение о каждом проходящем пакете: разрешить ли его прохождение. Для этого используйте набор правил фильтрации.

Брандмауэр может реализовывать несколько политик доступа к службам. Как правило, политика доступа к сетевым сервисам основана на одном из следующих принципов:

1. Отказаться от доступа в Интернет из Интернета и разрешить доступ в Интернет из Интернета.

2. Разрешить ограниченный доступ к внутренней сети из Интернета, что разрешено только определенным авторизованным системам, таким как информационные и почтовые серверы.

2.2 Основные протоколы используемые в работе межсетевого экрана

Основные протоколы, используемые в брандмауэрах.

Протоколы - это стандарты, определяющие формы и методы отправки сообщений, процедуры их интерпретации, правила работы различного оборудования в сети.

Сетевой протокол - это набор правил, который позволяет вам общаться и обмениваться между двумя или более компьютерами, подключенными к сети.

Основные протоколы используемые в работе МЭ:

- TCP/IP;
- UDP;
- OSPF;
- DHCP;
- DNS;
- HTTP;
- FTP/ TFTP;
- POP3;
- SMTP;
- SSH;
- TLS/SSL;
- SIP.

TCP/IP - набор протоколов передачи данных, получивший название от двух принадлежащих ему протоколов:

TCP (англ. Transmission Control Protocol - протокол управления передачей);

IP (англ. Internet Protocol - досл. «межсетевой протокол»).

UDP (англ. User Datagram Protocol - протокол пользовательских дейтаграмм) - это транспортный протокол для передачи блоков данных (дейтаграмм) в сетях IP без установления соединения, обеспечивает доставку дейтограмм, но не требует подтверждения их получения.

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это сетевой протокол, позволяющий хостам

автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. Эти адреса выбираются из предопределенного пула

IP-адресов, который управляется сервером DHCP.

DNS (Domain Name System) - это служба, которая преобразует текстовое имя домена в цифровой IP-адрес.

DNS - это сеть серверов баз данных, распространяемых через Интернет. Все серверы взаимосвязаны, и когда получен запрос на расшифровку, и по какой-то причине вы не можете определить его самостоятельно, сервер отправляет этот запрос, используя специально разработанные схемы, прежде чем преобразовать доменное имя в IP-адрес.

HTTP (Hyper Text Transfer Protocol) - это протокол для передачи гипертекста. Основная задача протокола HTTP - принимать и передавать гипертекстовые документы - веб-страницы, которые мы просматриваем в браузере.

FTP (File Transfer Protocol) / TFTP (Trivial File Transfer Protocol) - протоколы для отправки файлов с выделенного файлового сервера на компьютер пользователя.

FTP позволяет абоненту обмениваться двоичными и текстовыми файлами с любым компьютером в сети. После установления соединения с удаленным компьютером пользователь может скопировать файл с удаленного компьютера в свое свойство или с компьютера в удаленный файл.

POP3 (Post Office Protocol) - это стандартный почтовый протокол. POP-серверы обрабатывают входящую почту, а протокол POP используется для обработки запросов на получение почты от почтовой программы клиента.

SMTP (Simple Mail Transfer Protocol) - это протокол, который определяет набор правил для отправки сообщений. SMTP-сервер возвращает подтверждение, сообщение об ошибке или запрашивает дополнительную информацию.

SSH (Secure SHell) - это протокол уровня приложения, который шифрует весь трафик, включая пароли, который позволяет удаленно контролировать операционную систему и туннелировать TCP-соединения. SSH позволяет выбирать разные алгоритмы шифрования.

TLS / SSL (Secure Sockets Layer / Transport Layer Security) - использует асимметричную криптографию для проверки подлинности ключей обмена, которая обеспечивает безопасный обмен информацией в сетях, симметричное шифрование для защиты конфиденциальности распределенных пакетов.

SIP (протокол инициации сеанса) - это протокол создания сеанса, который описывает создание и завершение сеанса пользователя в Интернете, включая обмен мультимедийным контентом (IP-телефония, видео- и аудиоконференции, обмен мгновенными сообщениями, онлайн-игры).

Протокол описывает, как запросить соединение у другого, потенциально физически удаленного клиента, расположенного в той же сети, используя уникальное имя клиентского приложения.

Брандмауэры D-Link.

D-Link запускает серию брандмауэров NetDefend следующего поколения - комплексное решение для защиты корпоративной сети. Серия NetDefend учитывает растущие требования к сетевой безопасности, защите от хакерских атак, вирусов и конфиденциальности информации.

Рисунок 10 - Позиционирование межсетевых экранов D-Link NetDefend

Рисунок 11 - Обзор производительности и портов DFL-260E и DFL-860E

Рисунок 12 - Обзор производительности и портов DFL-1660 и DFL-2560

Все брандмауэры этой серии поддерживают удаленное управление через веб-интерфейс. К ним относятся мониторинг и поддержание состояния и безопасности сети, включая отправку электронной почты, системные события, журналы и статистику в реальном времени.

Брандмауэр DFL-860E.

Межсетевой экран NETDEFEND DFL-860E предназначен для использования в сетях малых и средних организаций.

Межсетевой экран DFL-860E оснащен:

- два порта WAN;
- один порт DMZ;
- 8 портов LAN с интерфейсом Ethernet 10/100/1000 Мбит / с.

Использование двух портов WAN обычно используется, когда два интернет-провайдера предоставляют доступ в Интернет.

Конфигурация интерфейсов DFL-860E по умолчанию:

Управление разрешено с любого LAN-интерфейса по адресу https://192.168.10.1, только LAN-интерфейс отвечает на команду "ping".

доступ к внутренним компьютерам, что затрудняет доступ к внешним компьютерам, тем самым усиливая его защиту от несанкционированного доступа.

NetDefendOS поддерживает два типа преобразования адресов:

- динамическая трансляция сетевых адресов (NAT) - динамическая трансляция сетевых адресов;

- статическая трансляция адресов (SAT) - статическая трансляция адресов.

NAT предоставляет механизм для преобразования исходного IP-адреса в другой адрес. Для каждого соединения, в дополнение к исходному IP-адресу, NetDefendOS автоматически переводит номер порта источника.

Вот и все. Чтобы установить соединение, IP-адреса нескольких источников становятся одним IP-адресом, и соединения отличаются только уникальным номером порта каждого соединения.

Следующая диаграмма иллюстрирует концепцию NAT.

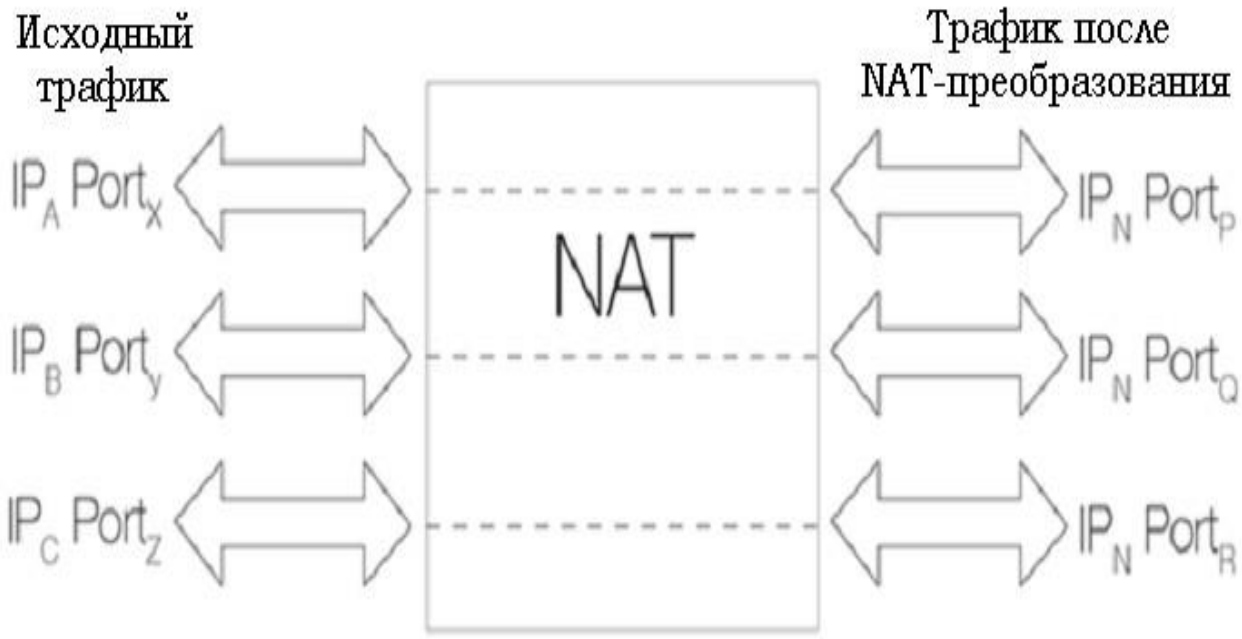

Рисунок 13 - Диаграмма концепции NAT

Три подключения к IP-адресам A, B и C преобразуются в один IP-адрес N с использованием NAT, а исходные номера портов изменяются на другие.

Когда вы устанавливаете следующее соединение NAT, NetDefendOS случайным образом идентифицирует следующий доступный номер порта источника. Механизм случайного назначения портов повышает безопасность.

NetDefendOS имеет три способа определения IP-адреса, используемого в NAT:

- используйте IP-адрес интерфейса. Когда устанавливается новое соединение, ему назначается выходной интерфейс в соответствии с расписанием маршрутизации. Когда NetDefendOS выполняет преобразование адреса, IP-адрес результирующего интерфейса используется в качестве нового IP-адреса источника. Этот метод определения IP-адреса используется в качестве метода по умолчанию.

Назначьте определенный IP-адрес. Вы можете назначить определенный IP-адрес в качестве нового основного IP-адреса. для этого

этот IP-адрес должен быть объявлен ARP в выходном интерфейсе, иначе брандмауэр NetDefend не получит обратный трафик. Этот метод используется, когда исходный IP-адрес должен отличаться от адреса исходного интерфейса.

Используя этот метод, например, провайдер, который использует механизм NAT, может назначать разные IP-адреса разным клиентам.

- Используйте IP-адрес в пуле NAT. Пул NAT в качестве основного IP-адреса - IP-адреса,

определяется администратором сети. В этом случае следующий доступный IP-адрес в пуле принимается как IP-адрес NAT.

В следующем примере демонстрируется практическое применение механизма NAT при настройке нового соединения.

Последовательность этих событий показана на следующей диаграмме:

1. Пользователь корпоративной сети отправляет запрос в Интернет, который приходит на внутренний интерфейс межсетевого экрана;

2. Устройство NAT получает пакет и вводит запись в таблицу управления соединением, которая управляет передачей адреса.

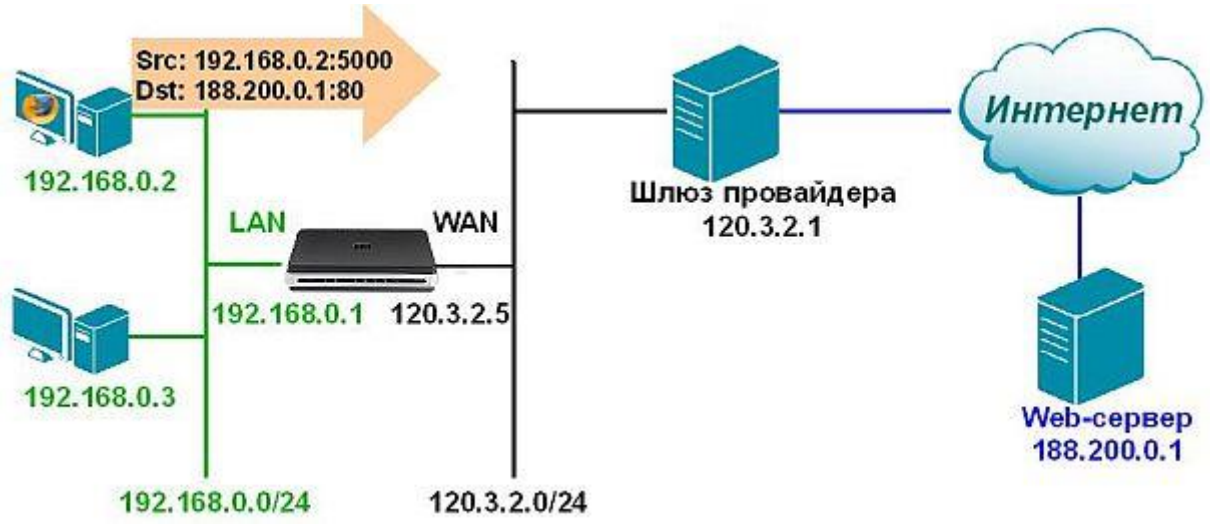

Рисунок 14 - Запись в таблице соединений

МЭ получает пакет и делает запись в таблице отслеживания соединений, которая управляет преобразованием адресов. Затем подменяет адрес источника пакета собственным внешним общедоступным IP-адресом и посылает пакет по месту назначения в Интернет.

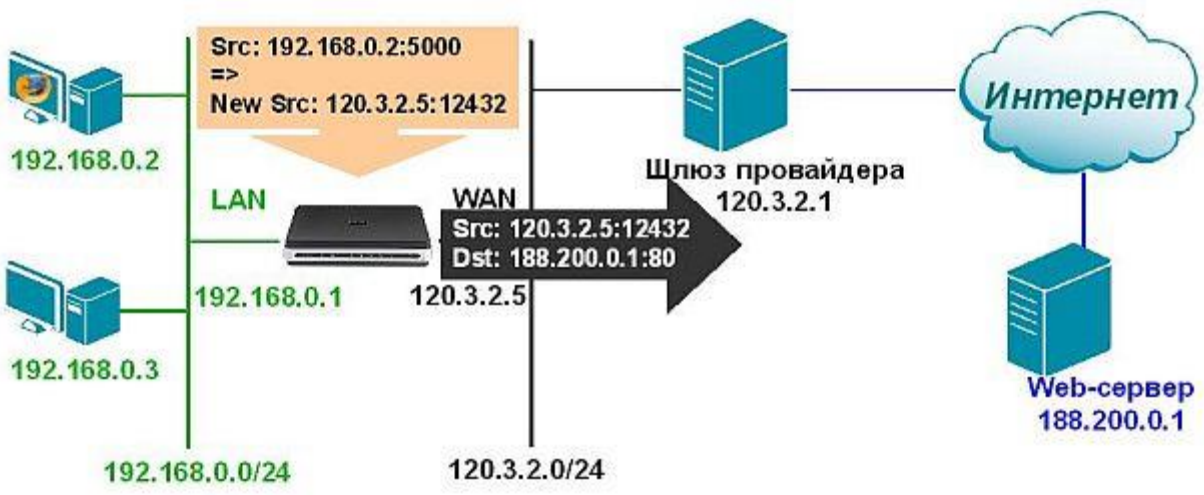

Рисунок 15 - Преобразование адресов при использовании функции NAT

Узел назначения получает пакет и передает ответ обратно МЭ, который в свою очередь, получив этот пакет, отыскивает отправителя исходного пакета в таблице отслеживания соединений, заменяет IP-адрес назначения на соответствующий частный IP-адрес и передает пакет на исходный компьютер.

Поскольку МЭ посылает пакеты от имени всех внутренних компьютеров, оно изменяет исходный сетевой порт и данная информация хранится в таблице отслеживания соединений.

Рисунок 16 - Преобразование адресов при использовании функции NAT

Статическая трансляция адресов (SAT) - статическая трансляция адресов.

Преобразование статического сетевого адреса переводит внутренние IP-адреса один за другим на внешние адреса. Это позволяет преобразовать IP-адрес внутренней сети во внешний IP-адрес.

Статический NAT позволяет подключаться к внутренним и внешним системам, таким как Интернет-хост.

Этот тип преобразования особенно рекомендуется для организации публичного доступа к системе, расположенной в интрасети. Для этого

создайте правило SAT, чтобы преобразовать реальный системный адрес во внешний адрес. Этот адрес будет доступен для внешних пользователей. В этом случае никто не может получить информацию о внутренней сети для внешних атак.

Статические функции SAT перечислены ниже:

- это одностороннее преобразование;
- может быть запущен из внешних и внутренних сетей;
- пункт назначения обмена может быть любым адресом.

В отличие от механизма NAT, SAT требует нескольких определений

Правил ИС, но мало. Первое правило SAT определяет только механизм трансляции адресов. Система продолжает поиск разрешений, правил NAT или FwdFast. Только когда найдено, например, правило с действием «Разрешить», оно фактически разрешено трафик через брандмауэр.

Самый простой способ использовать SAT - это конвертировать один IP-адрес. Это часто бывает, когда внешним пользователям предоставляется доступ к защищенному серверу с частным IP-адресом в зоне DMZ.

Ниже приведена схема обмена информацией между серверами в зоне DMZ, локальной сетью и локальными клиентами в Интернете.

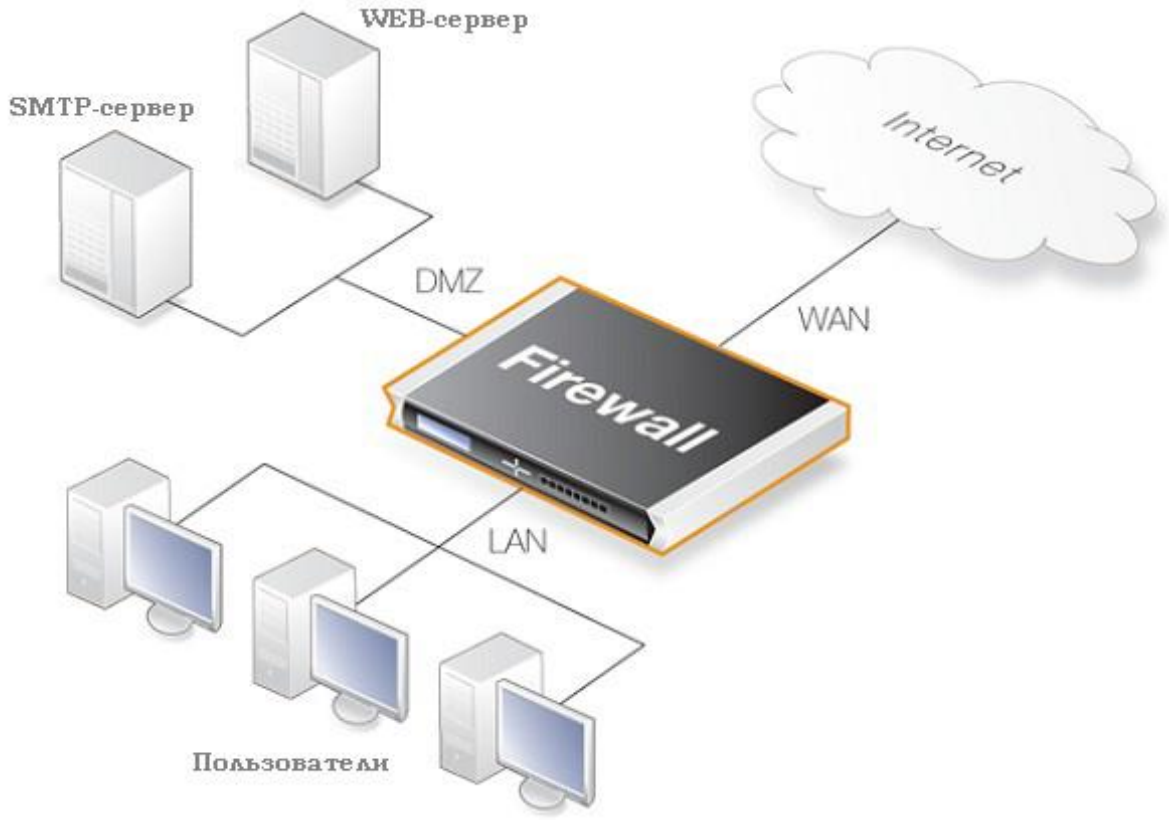

Рисунок 17 - Схема обмена информацией между серверами в зоне DMZ

Демилитаризованная зона (DMZ) может развертывать ресурсы, доступные для непроверенных клиентов, обычно с доступом к серверам через Интернет.

Серверы имеют высокий риск внешних атак и несанкционированного доступа к зашифрованным материалам.

Изолируя такие серверы в зоне DMZ, мы изолируем их от наиболее опасных подсетей, что позволяет NetDefendOS лучше управлять потоком данных между зоной DMZ и подсетями и быстро устранять сбои системы.

Безопасность, которая может происходить на серверах DMZ.

Государственная инспекция пакетов (ГПИ).

Брандмауэр контролирует состояние сетевых подключений (например, TCP или UDP) и может хранить атрибуты каждого подключения. Эти атрибуты известны как состояние открытого соединения и могут включать в себя информацию, такую как IP-адреса и номера портов, участвующие в соединении, и серийные номера пакетов, проходящих через соединение. Со временем инспекция состояния отслеживает состояние входящих и исходящих пакетов, а также соединение и сохраняет данные в динамических таблицах.

Когда клиент создает новое TCP-соединение, он отправляет пакет с битом SYN в заголовке пакета. Все пакеты с набором битов SYN считаются новыми соединениями для ME.

Если служба, запрошенная клиентом, доступна на сервере, сервер отвечает пакетом, в котором установлены биты SYN и ACK.

Затем клиент отвечает пакетом, в котором установлен только бит ACK и установлено соединение.

При мониторинге состояния соединения, EB пропускает все пакеты, исходящие от клиента, гарантируя, что, если они являются частью установленного соединения, хакеры не смогут устанавливать нежелательные соединения с защищенного компьютера.

Контролируя состояние соединения, SB обеспечивает дополнительную эффективность с точки зрения проверки партии. Это связано с тем, что для существующих соединений ME вместо проверки набора правил ME следует проверить состояние таблицы, которая может быть обширной.

Пример механизма госинспекции.

Брандмауэр контролирует сеанс FTP и проверяет данные на уровне приложения. Когда клиент просит сервер открыть отзыв (команда FTP PORT), брандмауэр извлекает номер порта из этого запроса.

В списке хранятся адреса клиентов и серверов, номера портов. При попытке установить соединение для передачи данных по протоколу FTP брандмауэр просматривает список и проверяет, действительно ли соединение отвечает на запрос клиента.

Соединения хранятся динамически, поэтому открыты только те порты, которым требуется FTP. В конце сеанса порты блокируются, что обеспечивает высокий уровень безопасности.

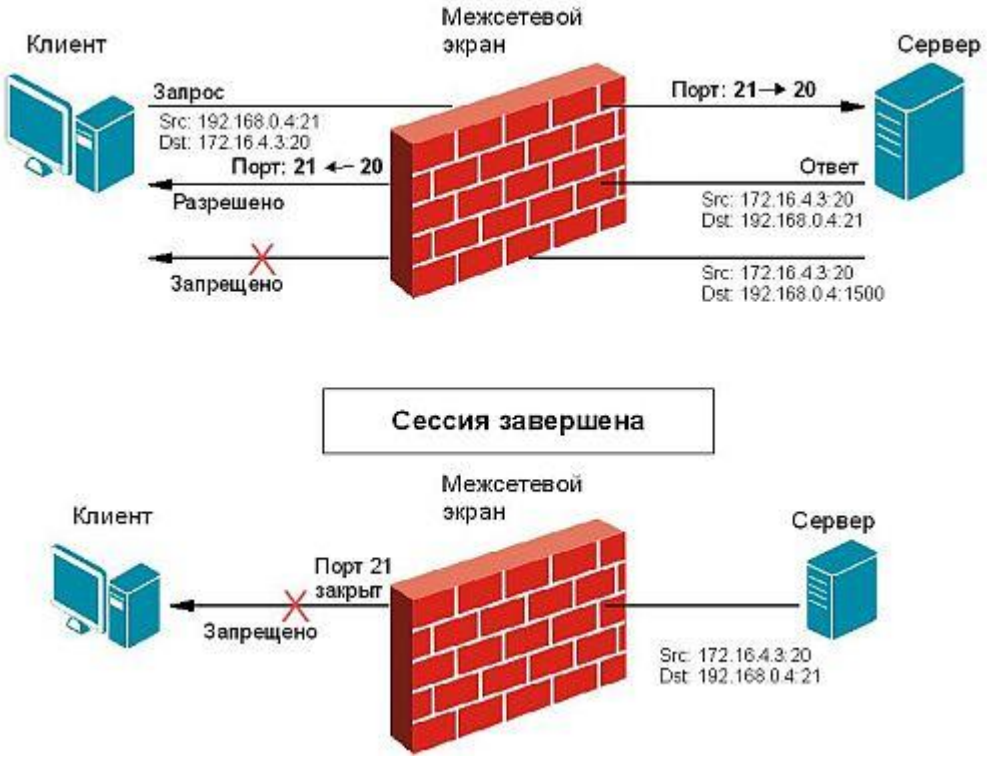

Рисунок 18 - Пример работы механизма Stateful Inspection с FTP-протоколом

NetDefendOS структурные элементы.

Основными структурными элементами в NetDefendOS являются интерфейсы, логические объекты, сервисы и различные типы правил (или наборов правил).

Интерфейсы являются наиболее важными логическими блоками в NetDefendOS.

Весь трафик, проходящий через систему, использует один или несколько интерфейсов. Правила безопасности применяются ко всем интерфейсам для управления трафиком во всех направлениях и защиты локальной сети.

Объекты являются ключевыми элементами, определенными для простоты использования и управления межсетевыми экранами в серии межсетевых экранов DFL.

Они предоставляют пользователю IP-адреса, интерфейсы, правила, сервисы, учетные записи пользователей и многое другое. позволяет назвать различные ключевые элементы, такие как

Службы (сервисы) - специальные программы, использующие определенные протоколы для предоставления различных приложений пользователям сети.

Брандмауэр позволяет создавать нестандартные сервисы. Кроме того, служба не предпринимает никаких действий с прошлым трафиком, для которого применяются правила IP.

Правила брандмауэра - это сердце брандмауэра. Правила - это основной фильтр, который разрешает или запрещает прохождение определенных типов трафика через межсетевой экран.

Набор правил связан со службами, которые определяют тип трафика, который они используют. NetDefendOS по умолчанию не принимает трафик, который не соответствует ни одному правилу в наборе правил IP.

Интерфейсы.

В общем, интерфейс - это набор определенных правил, методов и инструментов, с помощью которых взаимодействуют элементы любой системы.

Интерфейс - это набор стандартных аппаратных средств, программного обеспечения и средств проектирования, основанный на стандарте, который реализует взаимодействие различных функциональных элементов в информационной системе, обеспечивая электрическую и структурную совместимость этих элементов.

Основная идея использования стандартных интерфейсов состоит в объединении системных и внутрисистемных соединений для взаимодействия элементов сети.

Интерфейс, по которому трафик поступает в систему, называется основным интерфейсом (или интерфейсом ввода).

Соответственно, интерфейс, из которого трафик выходит из системы, называется интерфейсом назначения (или интерфейсом выхода).

Интерфейсы источника и назначения могут рассматриваться как шлюз для сетевого трафика в NetDefendOS или из нее.

NetDefendOS имеет начальный и целевой интерфейс для всего трафика.

В NetDefendOS интерфейсы делятся на несколько типов:

1. Физические интерфейсы - это ссылки на физические порты Ethernet.

2. Внутренние интерфейсы - включает интерфейсы VLAN и PPPoE.

3. Туннельные интерфейсы - используются для отправки и получения данных через VPN-туннели.

Внутренние интерфейсы.

NetDefendOS поддерживает два типа внутренних интерфейсов:

1. Интерфейс VLAN. Использование виртуального интерфейса VLAN определяется стандартом IEEE 802.1Q.

При передаче данных по виртуальной локальной сети IP-пакеты формируются в кадры Ethernet, помеченные VLAN.

2. Интерфейс PPPoE. Вы можете подключиться к серверам PPPoE с помощью интерфейса PPPoE (двухточечный протокол через Ethernet).

Туннельные интерфейсы

NetDefendOS поддерживает следующие типы туннельных интерфейсов:

1. Интерфейсы IPSec используются для создания виртуальных частных сетей (VPN) через туннели IPSec.

2. Интерфейсы PPTP / L2TP используются для создания туннелей PPTP / L2TP.

3. GRE-интерфейсы используются для создания GRE-туннелей.

Физические интерфейсы.

Каждый физический интерфейс представляет физический порт устройства. Таким образом, весь сетевой трафик, проходящий или ограниченный системой, в конечном итоге проходит через физический интерфейс.

В настоящее время NetDefendOS поддерживает единственный физический тип интерфейса - интерфейс Ethernet.

Стандарт IEEE 802.3 Ethernet позволяет различным устройствам подключаться к самостоятельно выбранным точкам или «портам» с использованием физического механизма передачи, такого как коаксиальный кабель. Используя протокол CSMA / CD, каждое устройство, подключенное через Ethernet, «прослушивает» сеть и отправляет данные на другое подключенное устройство, когда сеть занята. Если два устройства отправляют данные одновременно, алгоритмы позволяют отправлять их в разное время. Логический интерфейс Ethernet каждой системы NetDefendOS соответствует физическому порту Ethernet в системе. Количество портов, скорость соединения и способ реализации порта зависят от аппаратной модели.

Настройки интерфейса Ethernet.

Ниже приведены различные настройки для настройки интерфейса Ethernet:

Имя интерфейса. Имена интерфейсов Ethernet предопределены системой и обозначены именами физических портов. Интерфейс Ethernet системы с портом WAN называется WAN и так далее.

Интерфейсы Ethernet могут быть переименованы для наглядности. Например, если интерфейс с именем dmz подключен к беспроводной локальной сети, вы можете изменить имя интерфейса на радио для удобства.

Айпи адрес. Каждый интерфейс Ethernet должен иметь IP-адрес интерфейса - IP-адрес интерфейса, который может быть статическим или адресом, указанным DHCP.

IP Address 192.168.0.254

IP-адрес интерфейса используется в качестве основного адреса для подключения к системе через определенный интерфейс Ethernet. NetDefendOS обычно использует IP-адреса для определения IP-адресов интерфейсов Ethernet. Такие объекты обычно создаются системой автоматически.

В дополнение к IP-адресу интерфейса также указывается сетевой адрес для интерфейса Ethernet. Сетевой адрес предоставляет NetDefendOS информацию, напрямую доступную для IP-адресов через интерфейс.

IP Address 192.168.0.0/24

Другими словами, сетевой адрес идентифицирует IP-адреса в той же подсети, что и этот интерфейс. В таблице маршрутизации, связанной с интерфейсом, NetDefendOS автоматически создает сетевой маршрут через текущий интерфейс.

Шлюз по умолчанию. Вы также можете указать адрес шлюза по умолчанию для интерфейса Ethernet. Обычно это адрес маршрутизатора, который часто служит шлюзом в Интернет. Как правило, шлюз по умолчанию в таблице маршрутизации требует только одну сеть по умолчанию.

Добавьте DHCP-клиент. NetDefendOS включает опцию клиента DHCP для динамического назначения адресной информации подключенному серверу DHCP.

Если интерфейс используется для подключения к Интернету с использованием зарегистрированных IP-адресов провайдера, то DHCP не используется.

Кроме того, NetDefendOS поставляется с двумя специальными логическими интерфейсами, которые называются any и basic. Значение каждого из них:

- означает все возможные интерфейсы, включая любой основной интерфейс;
- ядро показывает, что система NetDefendOS сама контролирует движение трафика с этого интерфейса на этот интерфейс.

3 НАСТРОЙКА ПОЧТОВОГО СЕРВЕРА

3.1 DNS и DNS сервер

DNS (Domain Name System) - это система доменных имен, которая позволяет вам определять IP-адрес хоста с помощью доменного имени и наоборот. Поскольку каждый компьютер или сетевое устройство имеет свой собственный IP-адрес, вы должны знать этот IP-адрес для доступа к определенному компьютеру или устройству. Но не удобно запоминать определенную последовательность чисел, например, если вы обращаетесь ко многим компьютерам (это невозможно запомнить), поэтому лучше иметь систему доменных имен для не запоминания чисел, например, 192.168 .1.1 или mycomp. Вот простая ссылка.

DNS-сервер - это сетевая служба, система именования компьютеров и сетевых служб, которая отображает имена компьютеров и сетевые адреса и организует их в иерархическую доменную структуру. Система именования DNS используется в сетях TCP / IP, например, для поиска компьютеров и служб с понятными именами в Интернете и многих корпоративных сетях. Когда пользователь вводит имя DNS компьютера в приложение, DNS находит имя компьютера и другую информацию, такую как его IP-адрес или сетевые службы.

Этот процесс называется удалением имени.

Служба доменных имен является основным способом разрешения имен в Windows Server. При использовании DNS необходимо использовать роль сервера доменных служб Active Directory.

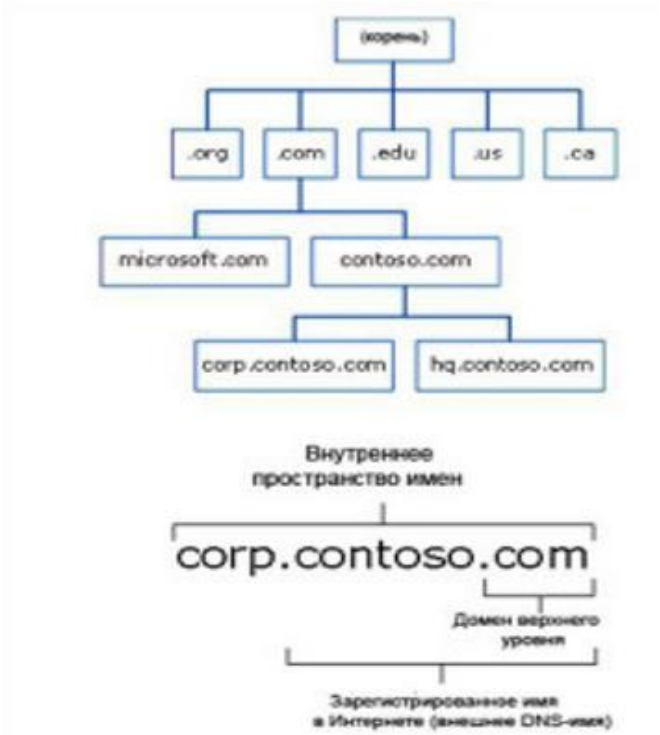

Рисунок 19 - Организация пространства имен DNS

Когда Microsoft начала создавать AD DS, основным приоритетом было обеспечение ее полного соответствия системе доменных имен (DNS). В результате AD DS не только полностью совместим с DNS, но и интегрирован с ним, поэтому без него не обойтись.

Пространство имен DNS - это ограниченная логическая область, созданная именем DNS и его поддоменами. Например, имена europe.comfortuaibc.com, asia.comfortuacc.com и coranuaabs.com являются частью одного и того же соседнего пространства имен DNS. Пространство имен DNS в AD DS публикуется в Интернете, например, на microsoft.com или msn.com, или скрыто от всех, в зависимости от стратегии и требований безопасности его пользователей.

Внешнее (опубликованное) пространство имен. DNS-имя, которое распознается в любом месте в Интернете, называется опубликованным или внешним пространством имен. Такое пространство имен часто используется в организациях, которые хотят отобразить структуру AD DS, которая широко используется в Интернете для полного удобства. Однако опыт показывает, что такая модель не очень удобна. Безопасность играет важную роль, поэтому система DNS должна быть настроена как отдельный компонент: AD AD DNS-зоны с доступом в Интернет не рекомендуются.

Внутреннее (скрытое) пространство имен. Для многих организаций публикация внутренней доменной структуры неприемлема по соображениям безопасности. Такие организации могут идентифицировать схемы AD DS с внутренними пространствами имен, которые не могут быть прочитаны из Интернета. Например, компания может иметь пространство имен DNS sso.sot и структуру AD DS, соответствующую пространству имен sso.international,

или что-то еще. Кроме того, любая комбинация действительна для внутреннего пространства имен, как .ot, .net, .gov и т. Д. Нет ограничений на использование доменов. Если вы хотите, вы можете даже назвать домен iloveoveydotain.verymuch (но, конечно, это не рекомендуется). По практическим причинам пространство имен .interna зарезервировано для личной адресации и в большинстве случаев очень удобно для использования.

Внедрение DNS в Windows Server 2012 осуществляется в соответствии с основными документами RFC, в которых определяется сущность работы DNS (запрос на пояснение). Следовательно, это удобно в существующих сетевых приложениях, поскольку Windows Server 2012 позволяет взаимодействовать с другими типами DNS, если они соответствуют требованиям, описанным в RFC.

IPv6 быстро развивается в мире информационных технологий, поэтому Windows Server 2012 является неотъемлемой частью операционной системы. Он полностью поддерживается в таких ролях, как DNS, DHCP и IIS. Windows Server 2012 имеет область.

GlobalNames для поддержки отдельных токенов, используемых в сочетании с IPv6.

WINS (Windows Internet Naming Service) - это второй тип преобразования имен, который сравнивает прежние имена Microsoft NetBIOS с IP-адресами. Технически возможно (и даже рекомендуется) переводить среду Windows Server 2012 без имени NetBIOS, но на практике известно, что очень трудно защитить среду от зависимости от WINS, поэтому во многих организациях остается возможным оставаться активной частью сети в течение как минимум нескольких лет. ИМЯ

Windows Server 2012 внес два основных изменения в службу.

DNS - это расширенное расширение безопасности DNS (DNSSEC) и расширенная поддержка PowerShell. Компонент DNSSEC, представленный в Windows 2008, дополнен онлайн-подписью и автоматическим управлением ключами в Windows 2012, что позволяет подписывать и управлять интегрированными областями Active Directory.

Полностью совместимый с DNS-подобными стандартами, AD DS расширяет стандартный набор инструментов DNS и предлагает новые функции, такие как DNS, интегрированные в AD, что значительно упрощает управление средой DNS. Кроме того, AD DS легко адаптируется к сторонней системе DNS, такой как UNIX BIND, например, при использовании BIND 8.2.x или выше.

Поскольку роль DNS важна в доменных службах Windows Server 2012 AD DS, необходимо тщательно знать все аспекты DNS.

Поскольку раздел приложения не является частью глобального каталога, записи DNS не являются частью реплики данных глобального каталога.

Благодаря концепции программного раздела, сложность репликации снижается, и для этих областей сети потребуется важная информация о

регионе. DNS-зоны интегрируются при внедрении AD DS в Windows Server 2012.

Файлы AD оптимизируются путем их хранения в разделе приложений, что снижает трафик репликации и повышает производительность системы. Мастер DNS-сервера (настройка мастера DNS-сервера) позволяет автоматизировать процесс создания зоны с помощью пошагового мастера. Это значительно упрощает процесс создания области, особенно для Active Directory. Чтобы запустить этот мастер, щелкните правой кнопкой мыши имя сервера в диспетчере DNS и выберите его в контекстном меню.

Настройте DNS-сервер.

Зоны DNS

На серверах Windows DNS существуют зоны четырех типов:

- стандартная основная зона;
- стандартная дополнительная зона;
- зона, интегрированная с Active Directory;
- зона-заглушка.

Область DNS является частью пространства имен DNS, отвечающего за управление конкретным сервером или группой DNS-серверов. Это основной механизм делегирования полномочий DNS; использовал для его установки пределы, на которых конкретный сервер может выполнять запросы. Любой сервер, который обслуживает определенную область, считается авторитетным или ответственным за эту область; Исключение составляют зоны-заглушки.

Важно понимать, что любая часть или подразделение DNS может находиться в одной и той же области. Например, организация может разместить все пространство домена, поддоменов и поддоменов в одной зоне или разделить пространство имен на отдельные зоны. В общем, все пространства имен в Интернете могут быть представлены как единое пространство с корнями и множеством отдельных регионов.

Поскольку в базе данных активного каталога используется несколько репликаций хоста, изменения могут быть внесены в область DNS любого контроллера домена и будут повторяться на других контроллерах домена. Комбинируя DNS с Active Directory, сочетание ролей DN S и контроллера домена становится нормой.

Прямое поле зрения.

Области прямого поиска по их названию создаются для прямого поиска в базе данных DNS. То есть они преобразуют имена в IP-адреса и предоставляют информацию о ресурсах. Например, если пользователь хочет получить доступ к серверу dcl.companyabc. перейдите в ячейку и запросите ее IP-адрес непосредственно в области поиска, DNS вернет его 172.16.1.11, то есть IP-адрес этого ресурса.

Обратный поиск областей.

Области обратного поиска выполняют операцию непосредственно вместо областей прямого поиска, сопоставляя IP-адреса с общим именем. Это похоже на поиск номера телефона, когда вы не знаете имени человека,

которому вы принадлежите. Области обратного поиска обычно создаются вручную, и их не нужно запускать каждый раз. Как описано в начале этого раздела, вы также можете автоматически создать область обратного поиска при создании новой области с помощью мастера установки DNS-сервера. Как правило, области обратного поиска имеют записи PTR, которые используются для отображения соответствующих имен в ответ на запросы обратного поиска.

Для прямого просмотра клиент предоставляет полное доменное имя (FQDN), а DNS-сервер возвращает IP-адрес. Верно обратное: клиент возвращает IP-адрес, а DNS-сервер возвращает полное доменное имя.

Основные причины связаны с безопасностью. Представьте себе злоумышленника, который установил вредоносную службу для прослушивания DNS-запросов на полное доменное имя с www в сети. Когда эта служба принимает запрос, она автоматически отправляет ложный ответ клиенту с IP-адресом веб-сервера взломщика, который загружен именами червей, вирусов и троянов, прежде чем пользователь узнает, что произошло. Если вы настроите веб-браузер на поиск определенного IP-адреса, результат можно будет сравнить с запрошенным именем, и в случае расхождения он не сможет подключиться к веб-серверу.

Примером этого метода обратного поиска при разрешении имен является Windows SMTP. Этот сервис позволяет вам искать соединения с сервером. SMTP-серверы предоставляют свои собственные доменные имена при взаимодействии, и при подключении отображается адрес TCP / IP. Затем вы можете выполнить поиск в обратном направлении, чтобы убедиться, что имена соответствуют адресам.

Чтобы правильно настроить области поиска в сети, вам необходимо понять, как работает поиск. Адрес IPv4 обозначается десятичными точками с использованием четырех октетов x.y.w.z. 1Pv6-адрес аналогичен, но использует шестнадцатеричные числа и т. Д. В обоих случаях процесс обратного преобразования одинаков. DNS-сервер, получивший запрос, меняет порядок номеров на IP-адресе. Таким образом, полное доменное имя - x.y.w.z с IP-адресом z.w.y.x, и, наконец, добавляется .in-addr.arpa. Затем DNS-сервер пытается разрешить полное доменное имя z.w.u.x.in-addr.arpa как обычное полное доменное имя. Преобразование начинается с домена верхнего уровня .arpa и идет по дополнительному адресу. Назовите серверы, где каждое десятичное значение становится поддоменом пространства имен справа от него. В небольшой среде, которая включает только одну подсеть, эта подсеть может быть представлена одной зоной. В этом примере подсеть 192.168.0.0 представляет собой одну зону (рисунок 6.20). При создании области обратного поиска мастер создания новой области запрашивает имя подсети.

Основные зоны.

В традиционном DNS (не интегрированном в Active Directory) отдельный сервер служит DNS-сервером для региона, и все изменения, вносимые в этот регион, производятся там. Один DNS-сервер может

обслуживать несколько регионов и может быть первичным для одних и вторичным для других. Если область является основной, это означает, что все изменения должны быть внесены в сервер, на котором находится эталонная копия этой области.

Вторичные зоны.

Вторая зона создана для хранения и захвата исходной зоны. Однако каждая копия базы данных DNS доступна только для чтения, так как все изменения в записях производятся в исходной области. Частный DNS-сервер может содержать несколько основных и нескольких дополнительных областей. Процесс создания второй зоны аналогичен процессу создания первичных зон, описанному в предыдущем разделе, за исключением того, что зона копируется с существующего сервера.

Зоны-заглушки.

Понятие зон-заглушек можно найти только в Microsoft DNS. Эта область не содержит никакой информации о членах этого домена и служит для направления запросов для разных доменов на список определенных серверов. Поэтому в этом регионе могут присутствовать только NS, SOA и соответствующие записи.

Связующие записи - это записи, используемые для перевода IP-адреса сервера имен вместе с конкретной записью NS. Сервер с фиксированной областью для пространства имен не принадлежит этой области.

Как показано на рис., зона-заглушка служит заменителем той зоны, которая является авторитетной на другом сервере. Она позволяет серверу перенаправлять запросы в определенную зону в список серверов имен этой зоны.

Понятие записей ресурсов.

В иерархии DNS объекты идентифицируются с использованием так называемых записей ресурсов (RR). Эти записи используются для простого поиска пользователей и ресурсов в указанном домене и являются уникальными для домена, в котором они находятся. Но поскольку DNS не имеет общего пространства имен, несколько идентичных записей RR могут существовать на разных уровнях иерархии DNS.

Наличие таких уровней может зависеть от распределенной природы иерархии DNS.

Рассмотрим некоторые виды письма.

1. Первоначальный вход в зону SOA (начало авторизации). Указывает на сервер, ответственный за определенную область в базе данных DNS. То есть сервер, указанный в записях SOA, является сервером, который является основным источником информации о области и отвечает за ее обновление. Кроме того, записи SOA содержат интервал времени жизни (TTL), лицо, ответственное за работу DNS, и другую важную информацию. При настройке DNS для AD DS в Windows Server 2008/2012 запись SOA создается автоматически и заполняется значением TTL по умолчанию, именем исходного сервера и другой информацией о области. После установки эти

значения могут быть изменены в соответствии с конкретными потребностями организации.

2. Записи хоста (A, Адресные записи). Самый распространенный тип ресурса. Наиболее распространенный тип записи ресурса - это запись хоста, также известная как запись A. Эти записи содержат имя хоста и соответствующий IP-адрес. Эти записи составляют подавляющее большинство DNS, так как они используются для идентификации IP-адресов многих ресурсов в домене. Большинство записей ресурсов содержат дополнительную информацию: их время жизни (TTL) и время их создания (необязательно). Чтобы просмотреть или изменить эту информацию, выберите Вид => Дополнительно в окне консоли управления DNS.

3. Сервер Сервер (NS) записей. Укажите, какие компьютеры в базе данных DNS имеют серверы имен, то есть DNS-серверы для определенной области. Может быть одна запись SOA для каждого региона, но может быть несколько записей NS.

4. AAAA (записи адресов IPv6) связывает имя хоста с адресом протокола IPv6. Помещает IP-адрес по умолчанию в 128-битный IPv6-адрес. Этот тип записи распространен при получении IPv6.

5. CNAME (запись канонического имени) или запись канонического имени позволяет назначать мнемонические имена хосту. Мнемонические имена или псевдонимы широко используются для связи функции с хостом или для сокращения имени. По сути, эта запись перенаправляет отправленные ей запросы на запись нужного хоста A.

6. MX record (mail exchange) почтовый сервер - определяет машину, которая обрабатывает почту для этого домена.

7. Сервисные записи (Сервис - SRV) - это ресурсы, которые указывают, какие ресурсы отвечают за работу определенных сервисов. Записи SRV, указывающие на контроллер домена AD DS, идентифицируют ресурсы, такие как Глобальный каталог (GC), LDAP (протокол простого доступа к каталогам) и Kerberos. Записи SRV недавно появились в DNS, но не существовали, когда стандарт был впервые представлен. Каждая запись SRV содержит информацию о конкретных функциях, выполняемых данным ресурсом.

8. Введите PTR (указатель) или указатель записи. Обратные DNS-запросы выполняются с использованием записей ресурсов, которые называются Pointer Records (Pointer - PTR). То есть, если вам необходимо знать имя ресурса, связанного с конкретным IP-адресом, пользователь может выполнить поиск по этому IP-адресу, и DNS-сервер возвращает запись PTR с именем, связанным с этим IP-адресом.

Как правило, записи PTR находятся в областях обратного просмотра.

Другие типы записей DNS.

Вы можете создавать DNS и другие непростые типы записей, которые имеют определенную цель и имеют конкретную причину для создания. Ниже приведен полный список таких записей.

ISDN - указывает конкретное DNS-имя для номера телефона ISDN.

KEY - хранит открытый ключ, используемый для шифрования в определенном домене.

RP - указывает ответственное лицо домена.

WKS - назначает конкретную услугу (конкретную услугу).

МБ - отображает хост с реальным почтовым ящиком.

DHCP (Dynanzic Host Conjigut Rotosol Ions) - это протокол, который позволяет компьютерам динамически получать IP-адреса и другие параметры сети. Это протокол, который позволяет 11 компьютерам получать IP-адреса и другие параметры сети.

DHCP требует как сервера, так и клиента.

DHCP-сервер - это сервер, который распределяет IP-адреса и настройки для компьютеров в сети; Соответственно, он установлен на 1 р-адрес распределения и настройки сети.

DHCP-клиент - это программа, установленная на клиентских компьютерах, которые обращаются к DHCP-серверу для получения IP-адреса с соответствующими настройками. Во всех операционных системах DHCP-клиент установлен по умолчанию, например, в Windows DHCP-клиент является службой с логическим именем.

Если вы не использовали его, вы, вероятно, знаете

DHCP, тогда все компьютеры в сети должны будут вручную зарегистрировать статические IP-адреса. Это первый плюс использования DHCP. Если вы зарегистрируете фиксированные IP-адреса, проблемы неизбежно возникнут, наиболее распространенной проблемой является конфликт

IP-адреса, т.е. один адрес установлен на нескольких компьютерах одновременно.

Есть и очевидные преимущества наличия DHCP-сервера. Те же настройки, что и у шлюза, DNS-сервера и многое другое. Соответственно, если у вас нет DHCP-сервера, вы должны сделать это вручную.

«Зачем использовать DHCP,

если организация имеет в общей сложности 15 автомобилей? »Тем не менее, даже если в сети много компьютеров, вы можете сделать ад намного проще. Даже если вы экономист, помните, какой IP-адрес вы указали для каждого компьютера, устройства или устройства, и рано или поздно вам придется их менять (компьютеры устарели или повреждены) и перенастроить все эти параметры. Или, когда вы добавляете новый элемент офисного оборудования, для которого требуется IP-адрес, вы можете забыть IP-адрес или отправить сообщение об ошибке, и вам нужно будет все исправить соответствующим образом. Конечно, если в вашей сети более 5 компьютеров, это не имеет особого смысла, и в этом случае вам не нужен администратор, но если вы говорите от 50 до 100 компьютеров в вашем парке, вам нужен DHCP, чтобы подключить все компьютеры к домену. ,

Службы DNS-сервера - это новейшее введение в современную автоматизированную сетевую адресацию. Он может выполнять все функции,

такие как служба BOOTP, но может предоставлять дополнительную информацию клиентам, которые запрашивают IP-адрес10.

Сервер DHCP был освобожден с использованием трехэтапной процедуры для предоставления IP-адреса клиенту.

1. Клиент DHCP загружается и отправляет запрос DHCP на IP-адрес всех узлов локальной сети.

2. DNS-сервер в локальной сети получает запрос и готовится к нему в виде DCP-аренды этому клиенту [отправить P-адреса] [P-адреса.

3. После того как сервер DNCP определяет требуемую информацию по запросу клиента, он предоставляет клиенту дополнительный адрес аренды - IP-адрес аренды DNCP, включая маску подсети, стандартный шлюз и (возможно) IP-адрес сервера.

3.2 Защита от DoS-атак

Одной из наиболее распространенных проблем с MTA является множество прыжков, которые замедляют последовательность. Как правило, спамеров атаки затрагивают несколько адресов электронной почты. Возврат этих сообщений часто отправляется в домен, который не отправлял эти сообщения, что приводит к более медленной почте MTA, которая была исходным мусором. Это часто требует вмешательства администратора, постановки в очередь и удаления всех сообщений для этого домена. Устанавливая перенаправление на каждый домен, администраторы устанавливают число таких итераций равным нулю, а для подозрительных доменов - ноль, что позволяет устройству автоматически отключать такие сообщения. Эти функции позволяют IronPort выступать в роли «амортизатора» для серверов групповых приложений, контролируя очередь сообщений.

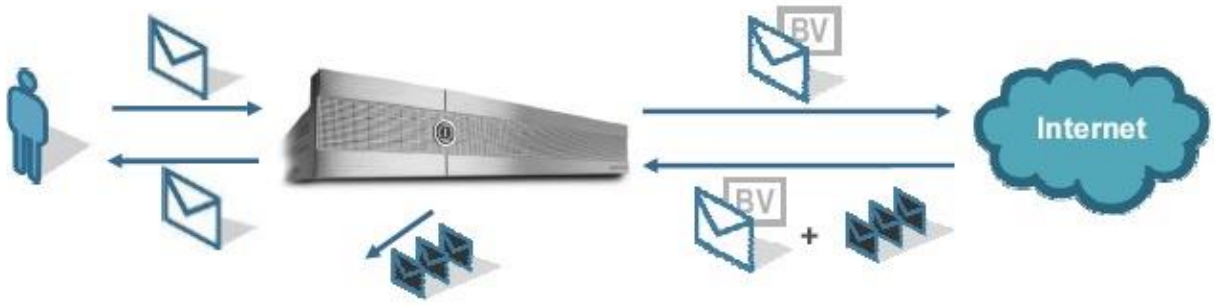

Рисунок 20 - Защита от DoS-атак

Защита от блокирования почтового трафика вышестоящими серверами.

Устройства IronPort имеют специальную технологию Virtual Gateway ™. Эта технология позволяет идентифицировать и классифицировать различные IP-адреса для исходящей почты. Его можно использовать для рассылки писем, отправленных различным организациям, на разные исходящие IP-адреса. Технология Virtual Gateway ™ - это мощный инструмент для решения проблем доставки. Если один из потоков исходящей почты не нравится и

блокируется провайдером, блокировка будет применяться только к этому IP-адресу, который вызвал блокировку, и это сообщение позволит свободный доступ к другим потокам. Эта функция полезна для провайдеров - каждому клиенту может быть назначен уникальный IP-адрес, который не влияет на производительность почты любого клиента. Эту технологию также можно использовать для разделения коммерческой почты и личной почты сотрудников. Этот подход локализует проблему с одним из потоков. Система очередей IronPort создает отдельную очередь для каждого домена получателя, для каждого виртуального шлюза. Таким образом, популярный домен получателя (например, Hotmail) может иметь отдельную очередь для каждого из виртуальных шлюзов, если один из шлюзов заблокирован, другой продолжит доставку по почте.

Виртуальные шлюзы также можно использовать для определения приоритетов экспресс-почты. Отправляя эти сообщения через частный шлюз, вы помещаете их в отдельную очередь, чтобы они не замедлялись с помощью писем с низким приоритетом. В дополнение к улучшению управления очередью и возвратом сообщений, MTA IronPort обладает отличной функцией управления подключениями. Система собирает все сообщения, отправленные на общий домен. Отправляет несколько сообщений одному соединению и открывает несколько узлов одному узлу. Типичный MTA открывает новое соединение для каждого сообщения, что увеличивает стоимость приема и отправки MTA.

IronPort - это высокопроизводительное устройство, но оно разработано в надежде, что принимающий домен не будет перегружен, что может привести к нашему занесению в черный список. Вы также можете использовать ограничение скорости для пересылки внутренней почты. Почта, отправляемая на центральный сервер Microsoft Exchange или IBM Lotus Notes, может доставляться с высокой скоростью, а почта может быть отложена для удаленных офисов для обеспечения общей стабильности системы.

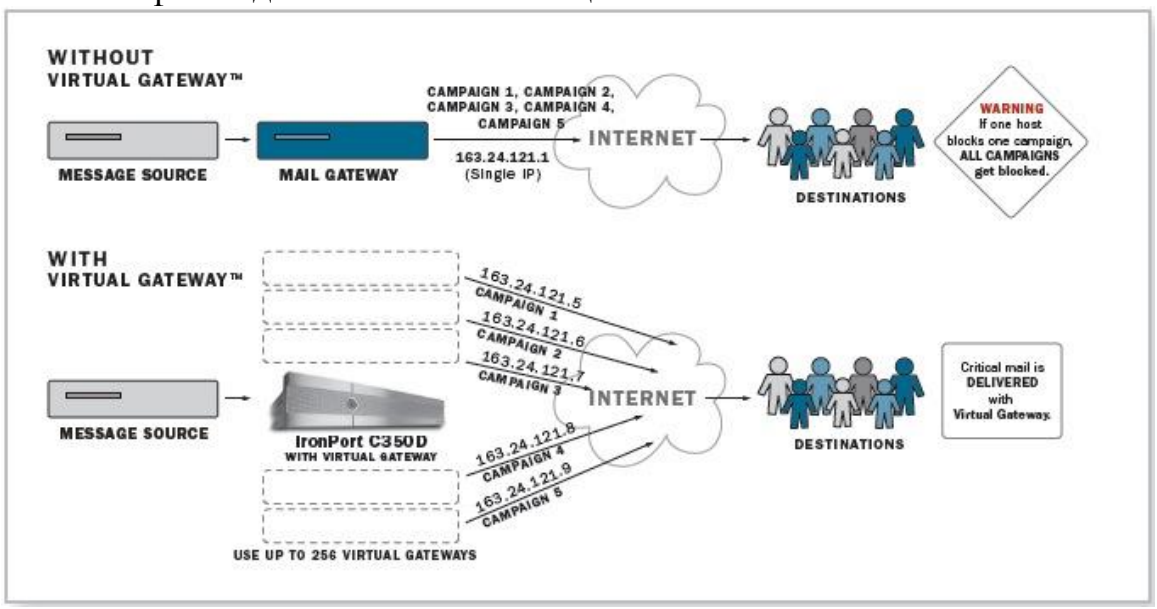

Рисунок 21 - Использование технологии Virtual Gateway™

Стабилизация скорости обмена сообщениями.

Алгоритм IronPort “Good Neighbor” вычисляет общую скорость передачи данных для всех подключений к данному домену. Когда скорость передачи данных начинает стабилизироваться, IronPort обрывает самое новое подключение, чтобы не перегружать удаленный сервер. Устройство IronPort обладает своим DNS-кэшем, что значительно повышает производительность. Этот кэш будет хранить все IP-адреса всех MX для домена-получателя и распределять подключения по разным MX в соответствии с их приоритетами.

3.3 Защита от спама и фильтрация. Репутационная фильтрация

Фильтры репутации IronPort обеспечивают первый уровень защиты благодаря оценке рисков в режиме реального времени и идентификации отправителей на основе информации из глобальной базы данных по защите от спама IronPort SenderBase®.

Авторитетная система фильтрации является первым направлением системы защиты, блокирует до 80% входящего спама на уровне связи, экономит трафик и системные ресурсы.

Устройство IronPort проверяет достоверность каждого входящего сообщения, используя запись DNS. Затем IronPort может применить уникальную политику безопасности почты к этому отправителю на основе его рейтинга (это заслуживающий доверия фильтр). Размер вложения, ограничения по типу и имени файла, схемы фильтрации спама, вирусов и контента, настройки управления потоком - все это относится к отправителям на основании их рейтинга. Таким образом, подозрительный отправитель имеет очень ограниченные возможности. Например, подозрительному отправителю может быть разрешено отправлять электронные письма не более чем на десять адресов в час для полной проверки на спам, вирусы и ключевые слова. Наоборот, надежный отправитель имеет большие преимущества - 1000 получателей в час, большое количество вложений и любого типа, шифрование TLS. Администраторы настраивают разные политики только один раз (с помощью веб-интерфейса), а затем отслеживают, как система классифицирует отправителей.

Управление мессенджерами через DNS. Многие коммерческие системы, доступные сегодня, предлагают «замедление», ограничивая количество соединений на хост. Спамеры легко добавляются к этому методу, отправляя несколько сообщений каждому получателю или одно сообщение нескольким получателям. IronPort может ограничивать количество маршрутов в час. Это очень эффективное решение, когда дело доходит до репутации. Отправитель больше похож на спамера, он работает с нами медленно.

Явные спамеры могут быть быстро идентифицированы и заблокированы. Письма от проверенных отправителей могут быть доставлены без проверки на спам или вирусы. Эти два класса отправителей обычно

составляют 80 процентов входящей почты. Оставшиеся 20 процентов почтового трафика («серая зона») ограничены скоростью приема и подлежат фильтрации содержимого с помощью встроенного антиспам-сканера. Отнимающие много времени спам-фильтры используются только при необходимости. Ограничение скорости - эффективный инструмент для защиты от спамеров и DoS-атак.

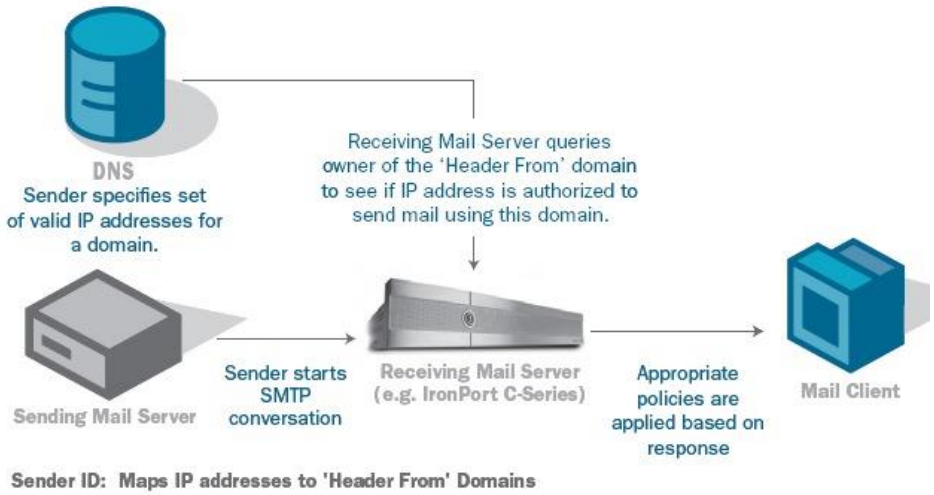

Рисунок 22 - Работа репутационного фильтра

SenderBase® - первая и самая большая в отрасли сеть для отслеживания почтового и веб-трафика. SenderBase контролирует множество сетевых настроек для каждого IP-адреса, который отправляет почту в Интернет. Эти параметры включают в себя общее количество сообщений, отправленных на этот IP-адрес, продолжительность его отправки, его местоположение, был ли он занесен в черный список, правильные настройки DNS, возможность отправителя получать почту и многое другое. включен. SenderBase собирает данные из примерно 100 000 различных сетей по всему миру. На эти сети приходится более 25 процентов мирового почтового и веб-трафика. SenderBase - единственная служба управления трафиком, которая собирает данные из разных источников и отслеживает более 120 различных параметров для каждого отправителя. SenderBase использует алгоритм, анализирует объективные параметры уровня сетевого уровня и имеет «рейтинг репутации» (рейтинг отправителя) от -10 до +10. Этот рейтинг будет доступен для устройства в режиме реального времени, когда вы получите сообщение от любого отправителя. Многие политики могут быть связаны с рейтингом отправителя.

В круглосуточном центре операций IronPort Threat (TOC) работают многие многоязычные специалисты и статистики, которые анализируют и управляют данными в SenderBase. Команда TOC разработала качественный процессор данных, который обрабатывает и измеряет данные из различных источников для точной и точной интерпретации. Эта команда гарантирует, что данные в SenderBase являются точными и точными, и администраторы

могут полагаться на данные SenderBase для автоматической классификации почты, не устраняя время и затраты на добавление черного списка и времени в список.

Рисунок 23 – TOC

Антиспамовая фильтрация.

IronPort Anti-Spam основан на инновационном подходе к идентификации почтовых угроз - уникальной CASE-системе (Contextual Adaptive Scanning System), разработанной IronPort, которая действует как внутренний уровень защиты от спама с минимальными административными затратами и наиболее точным обнаружением спама.

Основным преимуществом этой технологии является высокая эффективность борьбы с «графическим» спамом. Для этого устройства IronPort анализируют входящие почтовые сообщения по четырем группам параметров:

- идентификационные данные отправителя;
- адресная информация (ссылки, телефонные номера и почтовые адресов.

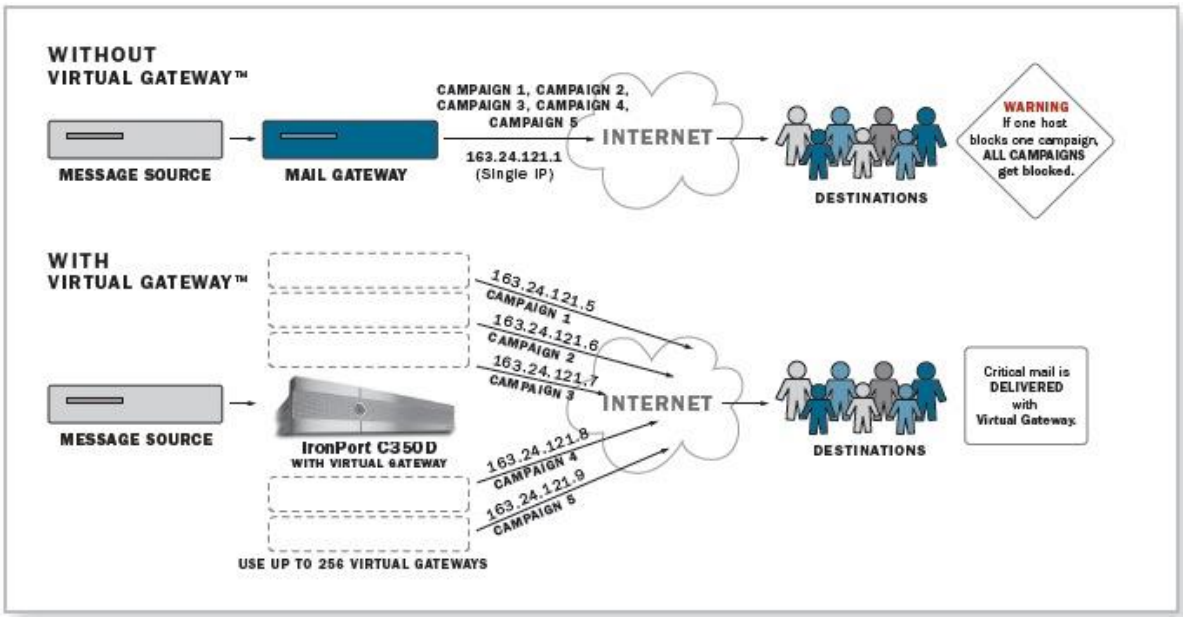

Рисунок 24 - Использование технологии Virtual Gateway

DNS (*Domain Name System*) – это система доменных имён, которая позволяет по доменному имени узнать IP адрес хоста и наоборот.

Запустите диспетчер сервера *(Server Manager)* на сервере Windows Server 2012 с полным графическим интерфейсом.

Перейдите в раздел *Dashboard (Инструменты)* и щелкните на ссылке *Add Roles and Features (Добавить роли и компоненты)*.

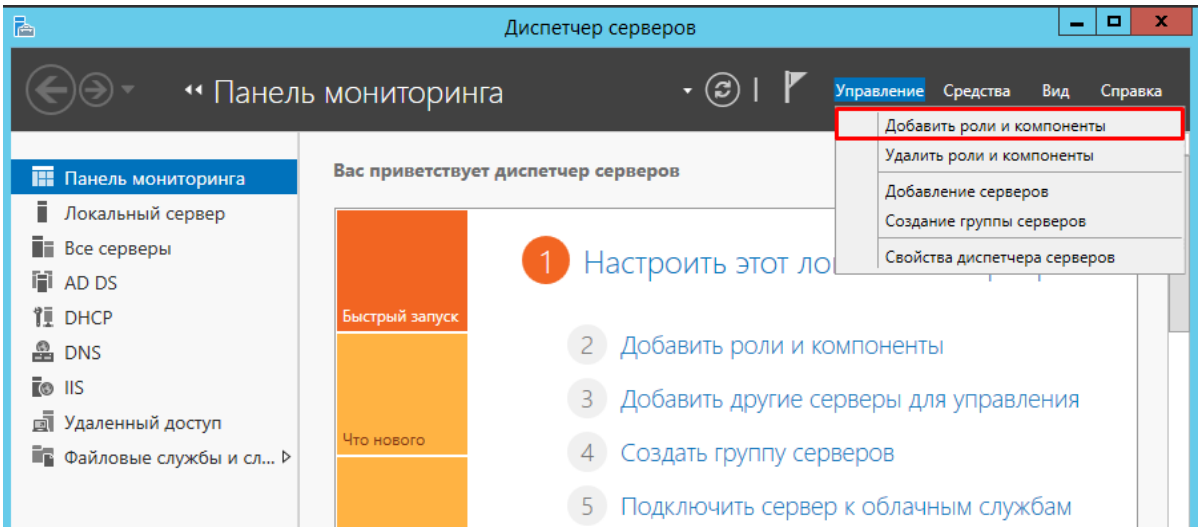

Рисунок 24 - Панель мониторинга

На странице *Before You Begin (Прежде чем приступить к работе)* щелкните на кнопке *Next (Далее)*.

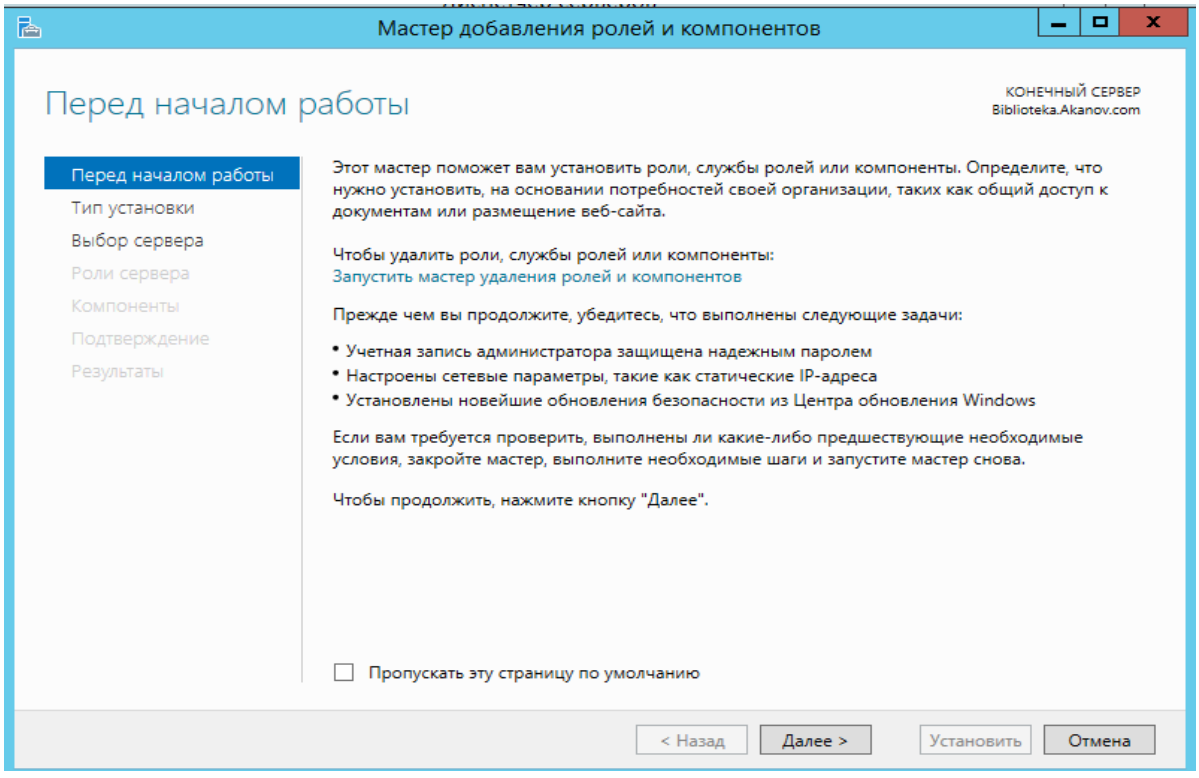

Рисунок 25 - Мастер добавления ролей и компонентов (начало)

Оставьте выбранным вариант Role-Based or Feature-Based lnstallation (Установка на основе роли или компонента) и щелкните на кнопке Next.

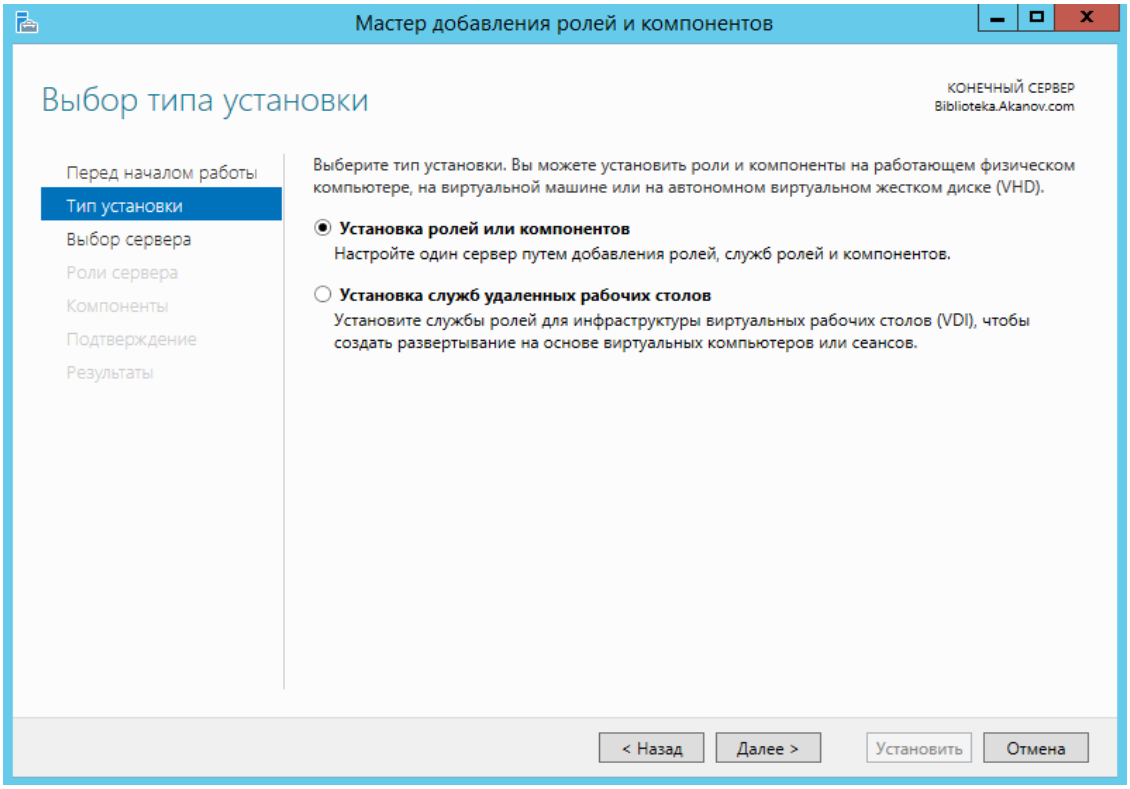

Рисунок 26 - Мастер добавления ролей и компонентов (выбор типа установки)

Выберите в серверном пуле сервер, на который нужно добавить роль DNS, и щелкните на кнопке Next.

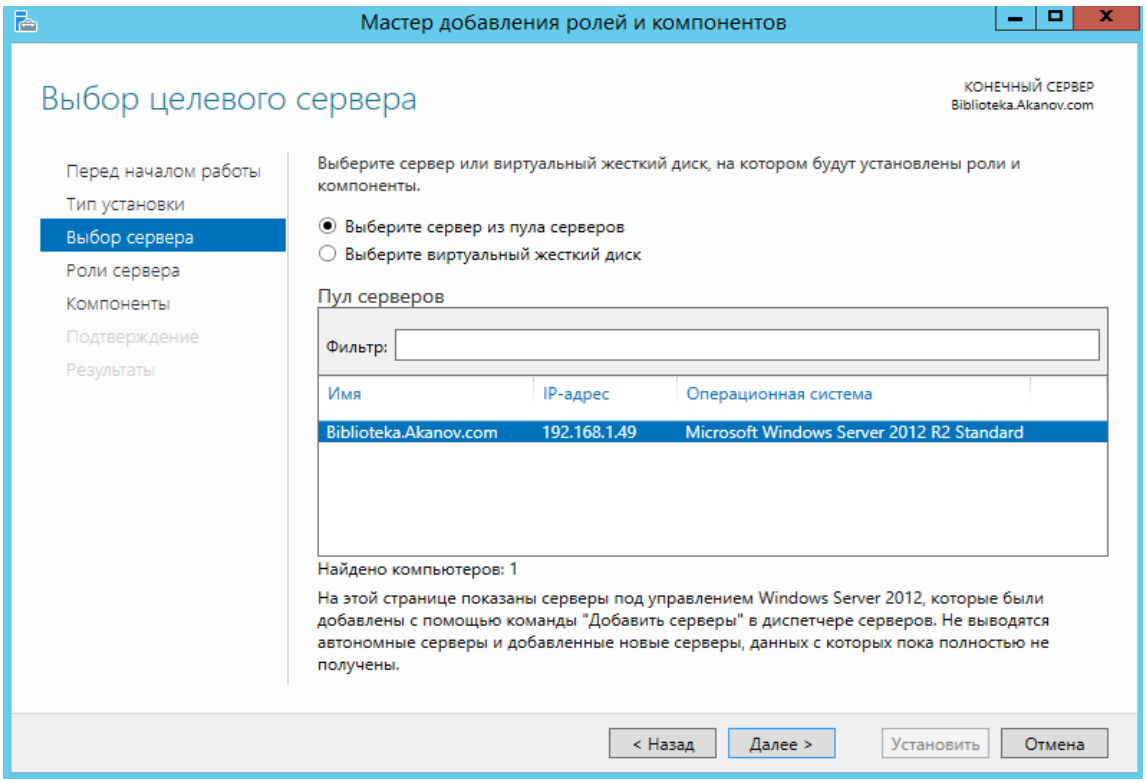

Рисунок 27 - Мастер добавления ролей и компонентов (выбор целевого сервера)

Примечание: При отметке флажка DNS Server Role мастер выполнит проверку, что целевой сервер готов для выполнения роли DNS. Например, если для сервера не выделен статический IP-адрес, появится предупреждающее сообщение.

На странице Features (Компоненты) щелкните на кнопке Next.

На странице lntroduction to DNS Server (Вводные сведения о DNS-сервере) щелкните на кнопке Next.

На странице Confirmation (Подтверждение) щелкните на кнопке lnstall (Установить), чтобы запустить установку роли DNS.

Щелкните на кнопке Close (Закрыть) , чтобы завершить работу мастера.

Перейдите в раздел DNS. Появится список серверов в серверном пуле, на которых установлена роль DNS.

Щелкните правой кнопкой мыши на нужном сервере DNS и выберите в контекстном меню пункт DNS Manager (Диспетчер DNS).

Выберите имя сервера DNS, на котором нужно выполнить настройку.

В меню *Action (Действие)* выберите пункт *Configure a DNS Server (Настройка DNS сервера).*

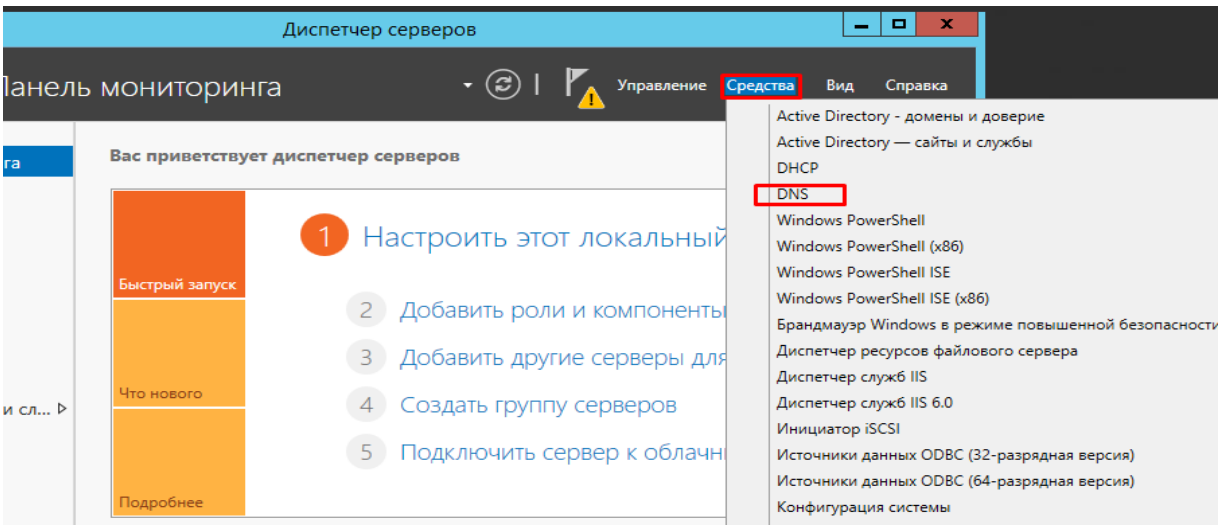

Рисунок 28 - Вход в диспетчер DNS

Зоны прямого просмотра.

Зоны прямого просмотра (forward lookup zone), как не трудно догадаться по их названию, создаются для выполнения прямого поиска в базе данных DNS. То есть они выполняют преобразование имен в IP-адреса и предоставляют информацию о ресурсах. Например, если пользователь захочет обратиться к серверу dcl.companyabc . сот и запросит его IP-адрес в зоне прямого просмотра, DNS возвратит ему значение 172.16.1.11 , т.е. IP-адрес данного ресурса.

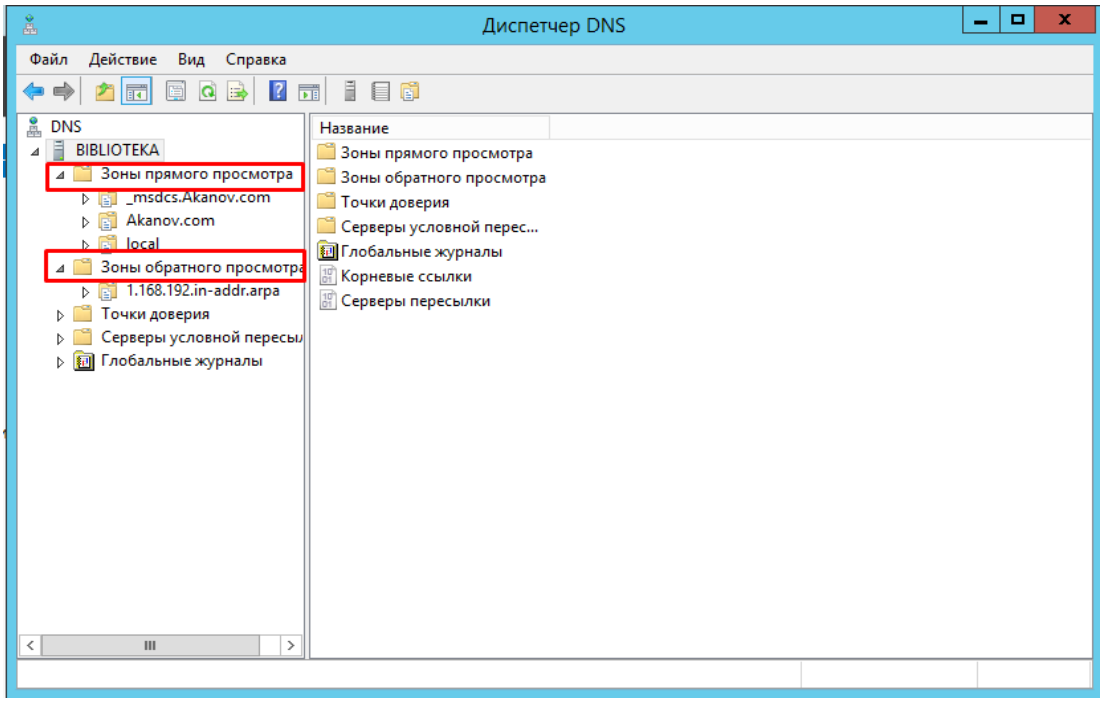

Рисунок 29 - Диспетчер DNS

Зоны обратного просмотра.

Зоны обратного просмотра (reverse lookup zone) выполняют операцию, прямо противоположную той, что выполняют зоны прямого просмотра -

сопоставление IP-адресов с обычным именем. Эта похоже на поиск телефонного номера, когда не известно имя того, кому он принадлежит. Зоны обратного просмотра обычно создаются вручную и вовсе не обязательно присутствуют вкаждой реализации. При создании новой зоны с помощью мастера настройки сервера DNS, как было описано ранее в главе, может быть автоматически создана и зона обратного просмотра. Как правило, зоны обратного просмотра содержат записи PTR, которые служат для указания на соответствующие имена в ответ на запросы обратного поиска.

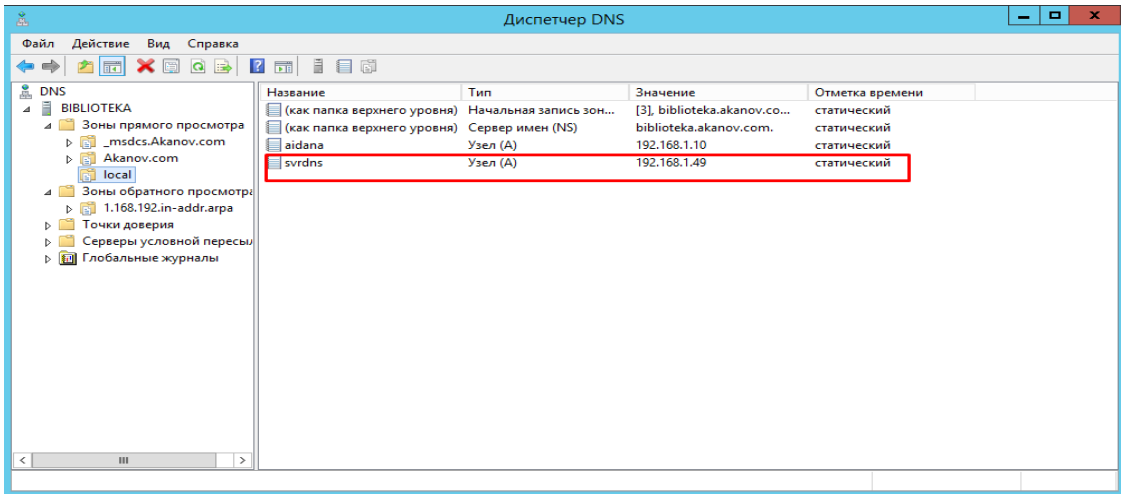

Рисунок 30 - Диспетчер DNS

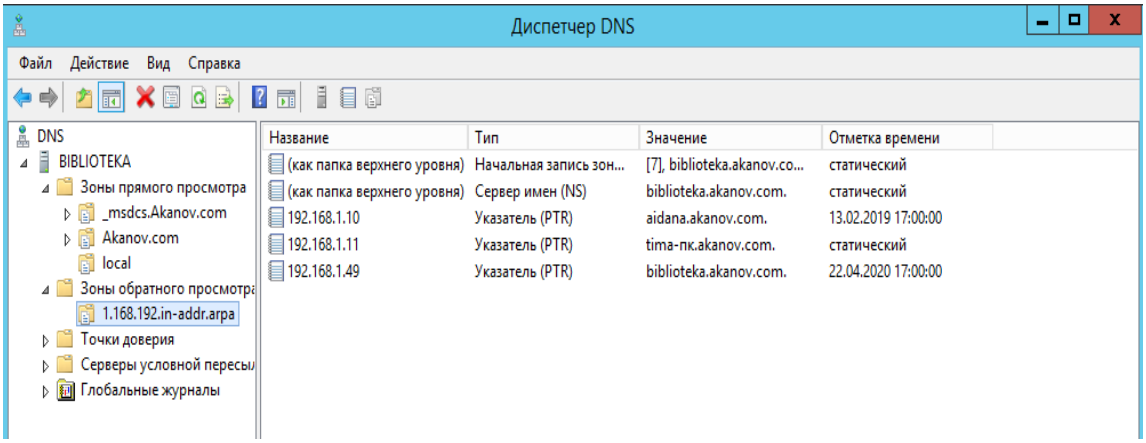

Рисунок 31 - Диспетчер DNS

Зоны прямого просмотра

DHCP (англ. *Dynamic Host Configuration Protocol* — протокол динамической настройки узла) — сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому *серверу DHCP* и получает от него нужные параметры.

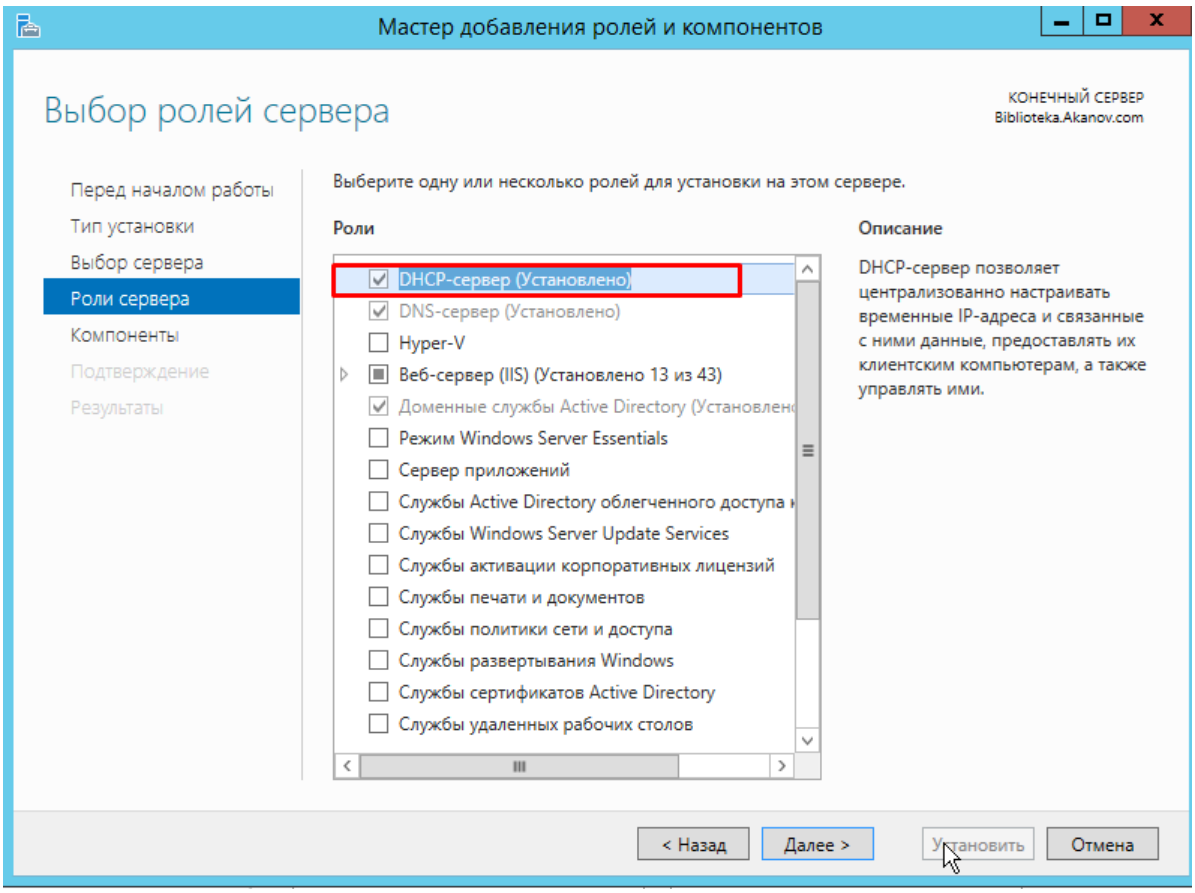

Рисунок 32 - Мастер добавления ролей и компонентов (выбор ролей сервера)

Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

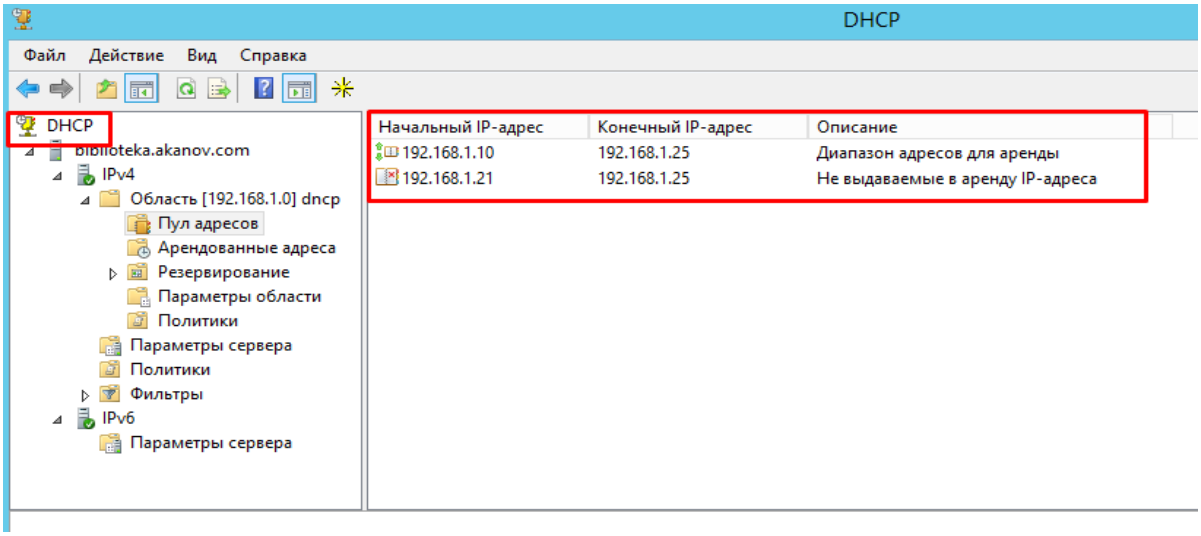

Рисунок 33 - Диспетчер DHCP

На следующем шаге выбирете роль “Веб-сервер (IIS)”. В открывшемся окне нажмите “Добавить компоненты”. Веб-сервер (IIS) содержит консоли для управления службой SMTP.

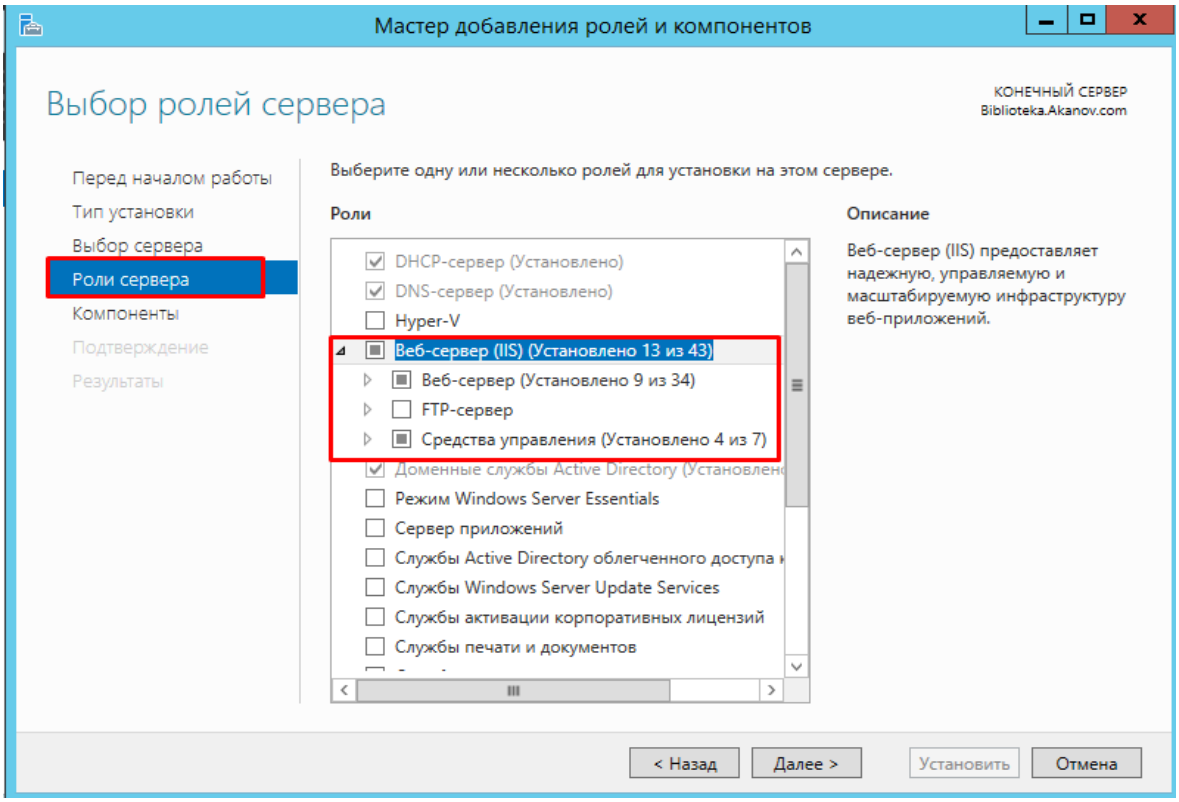

Рисунок 34 - Мастер добавления ролей и компонентов

Далее в списке компонентов выберете “SMTP-сервер”. В открывшемся окне нажмите “Добавить компоненты”.

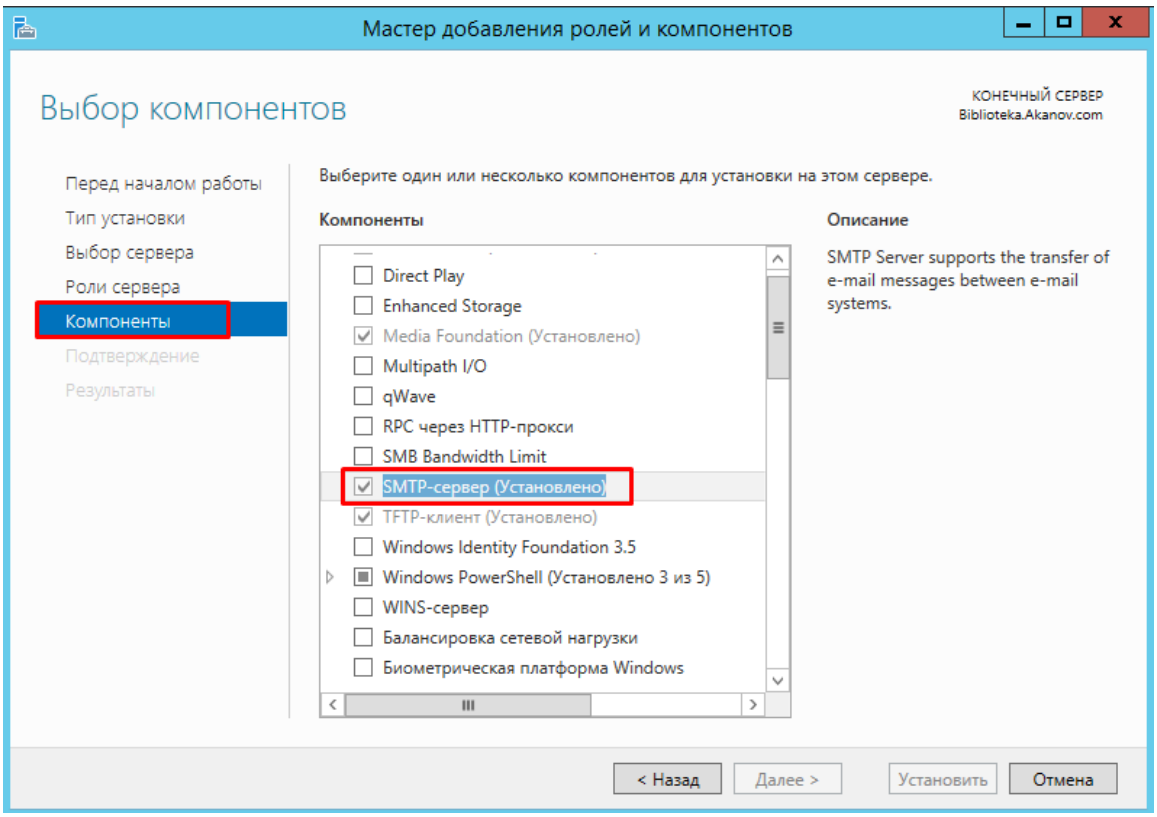

Рисунок 35 - Добавления ролей SMTP server

Настройка SMPT сервера. Управлять SMTP сервером можно через Internet Information Services (IIS) Manager 6. Чтобы открыть IIS, перейдите в диспетчер серверов и в меню в правом верхнем углу выберете раздел “Средства” -> “Диспетчер служб IIS 6.0”.

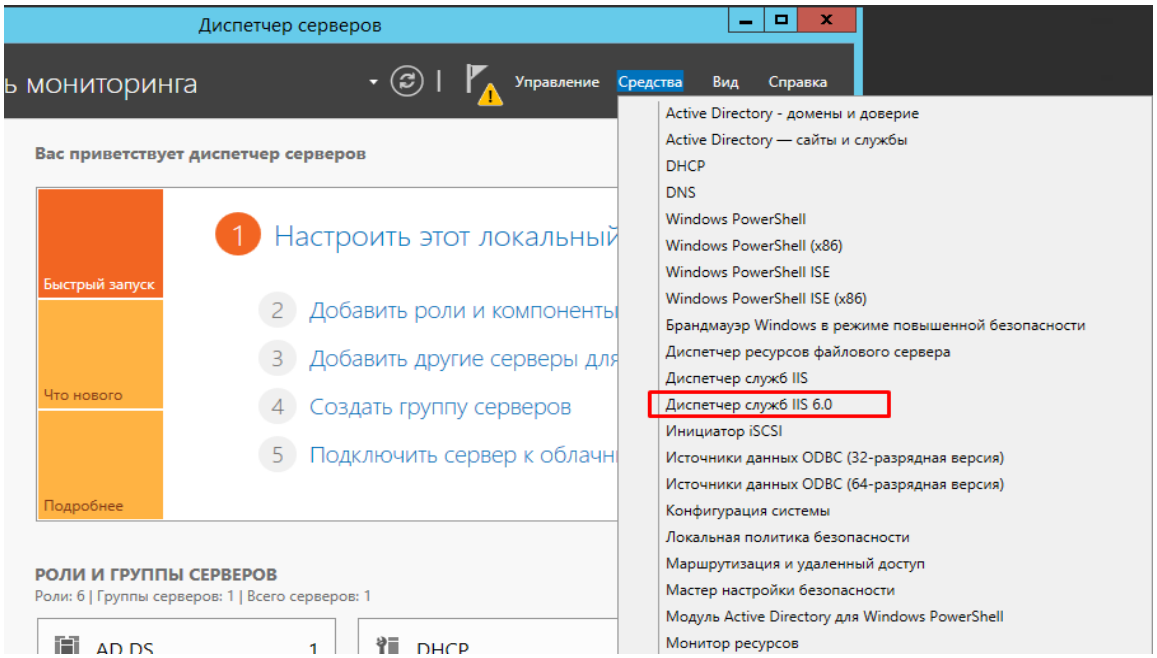

Рисунок 36 - Диспетчер служб IIS 6.0

Разверните ветку с именем сервера, выберете SMTP Virtual Server и откройте его свойства.

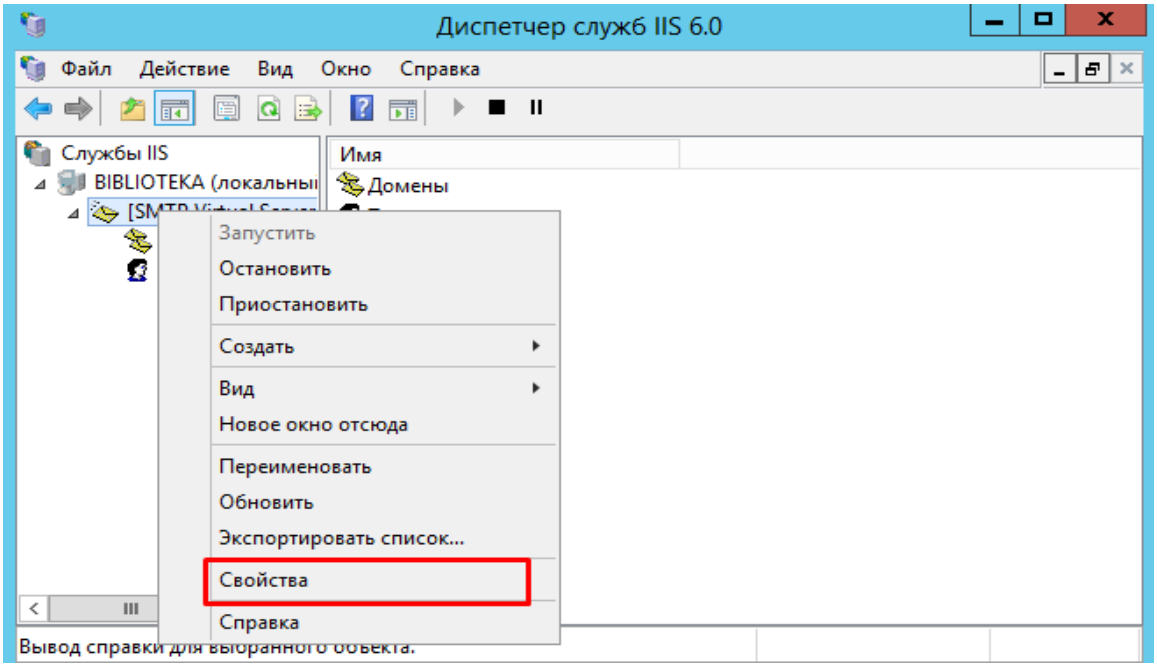

Рисунок 37 - Свойства служб IIS 6.0

На вкладке “Общие” выберете ваш IP-адресс, на котором должен отвечать SMTP сервер и включите ведение журнала, для сохранения информации обо всех отправленных письмах

.

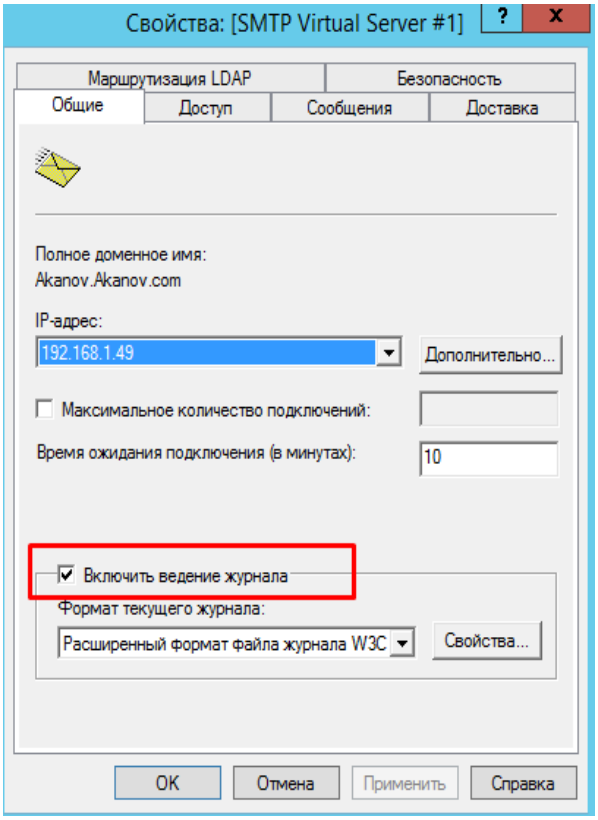

Рисунок 38 - Свойства SMTP Virtual server

На вкладке “Доступ” в раздел “Управление доступом” нажмите кнопку “Проверка подлинности”. В открывшемся окне отметьте галочкой пункт “Анонимный доступ” для того, чтобы все пользователи сервера и приложения могли использовать SMTP-сервер.

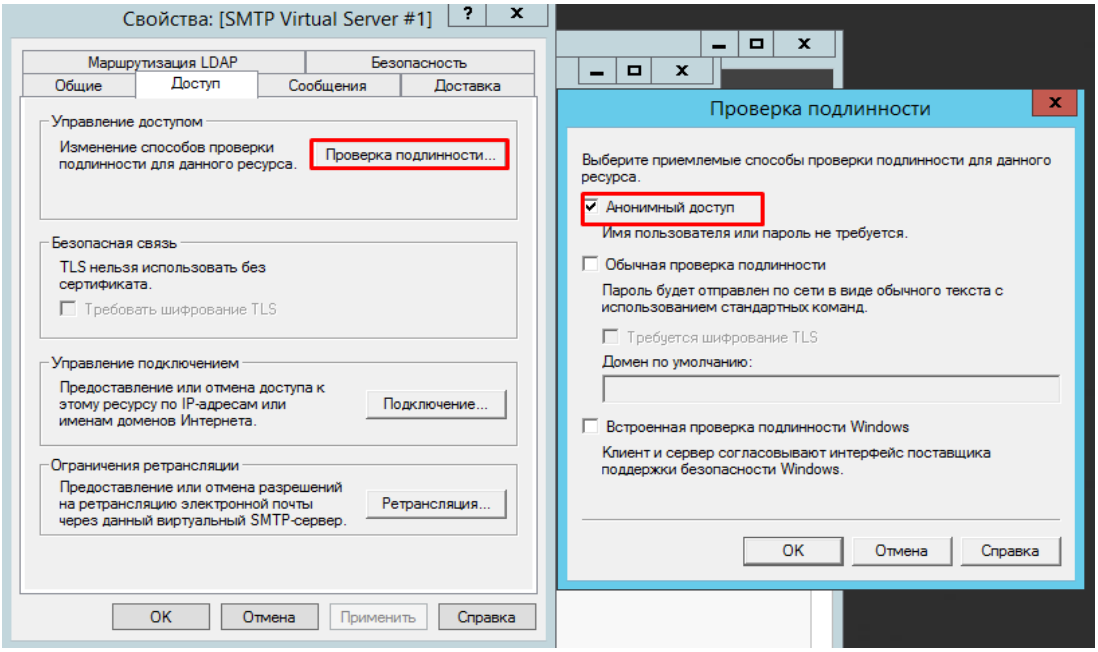

Рисунок 39 - Свойства SMTP Virtual server анонимный доступ

Далее в разделе “Управление подключением” нажмите кнопку “Подключение”. В открывшемся окне разрешите доступ к SMTP-серверу только определенным компьютерам, добавив их в список и выбрав тип подключения “Только компьютеры из списка ниже”.

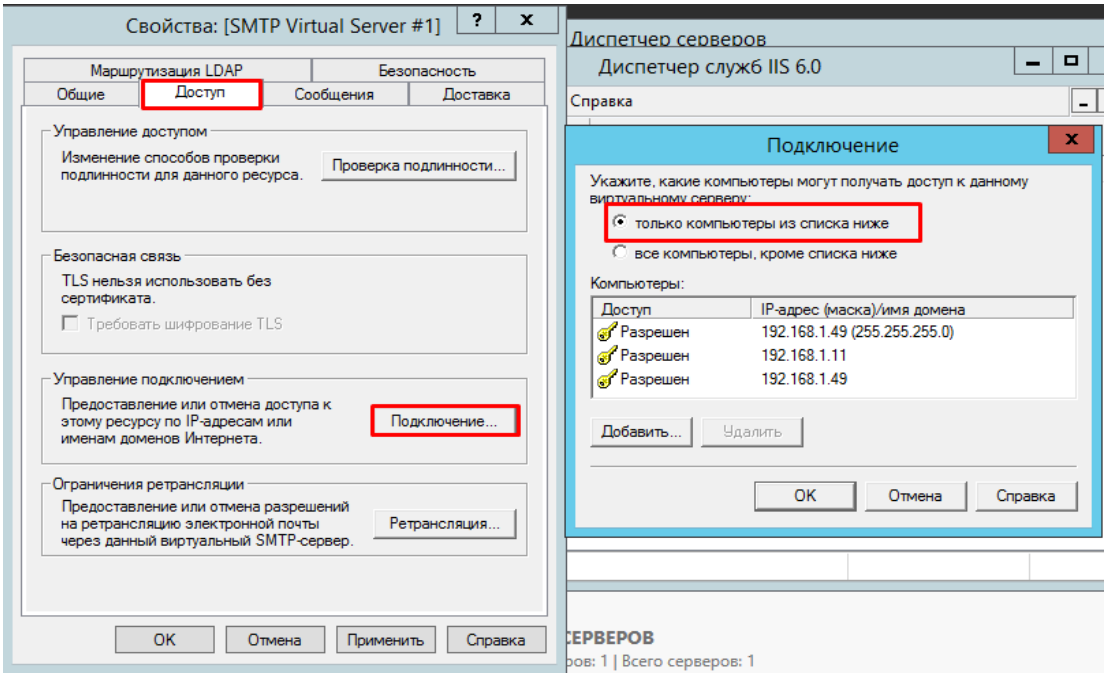

Рисунок 40 - Свойства SMTP Virtual server подключение ip-адреса

Далее, на вкладке “Доставка” нажмите кнопку “Дополнительно”. В открывшемся окне в поле “Полное доменное имя” введите ваше доменное имя или IP-адрес.

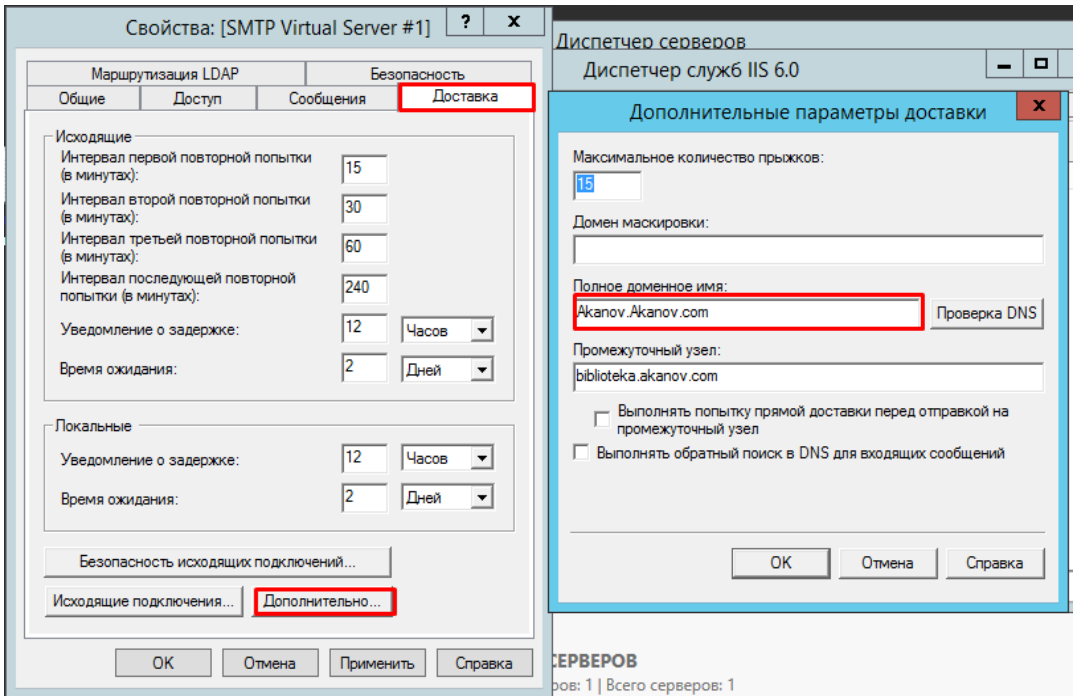

Рисунок 41 -Свойства SMTP Virtual server дополнительные параметры

При проверке DNS имя домена должно быть допустимым.

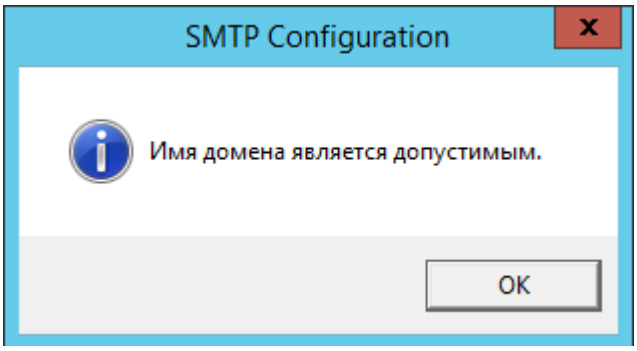

Рисунок 42 - Проверка DNS имени

Сохраняем все внесенные изменения.

Автозапуск службы SMTPSVC.

Служба SMTP-сервера должна запускаться автоматически при включении сервера, для этого откройте командной строку и выполните следующие команды:

set-service smtpsvc -StartupType Automatic

Запустите службу:

start-service smtpsvc

Убедитесь, что служба SMTPSVC запущена:

get-service smtpsvc

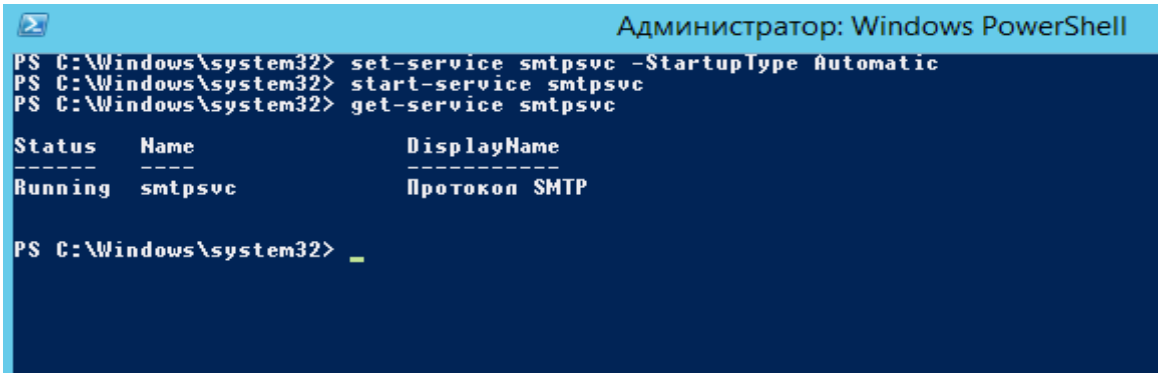

Рисунок 44 - Консоль PowerShell

Тестирование SMTP сервера.

Для проверки корректности работы создайте любой текстовый документ с расширением txt (например, на рабочем столе), и внесите следующие строки, указав от кого вы отправляете письмо и кому:

- From:server@example.org
- To:test@gmail.com
- Subject:test
- Some text

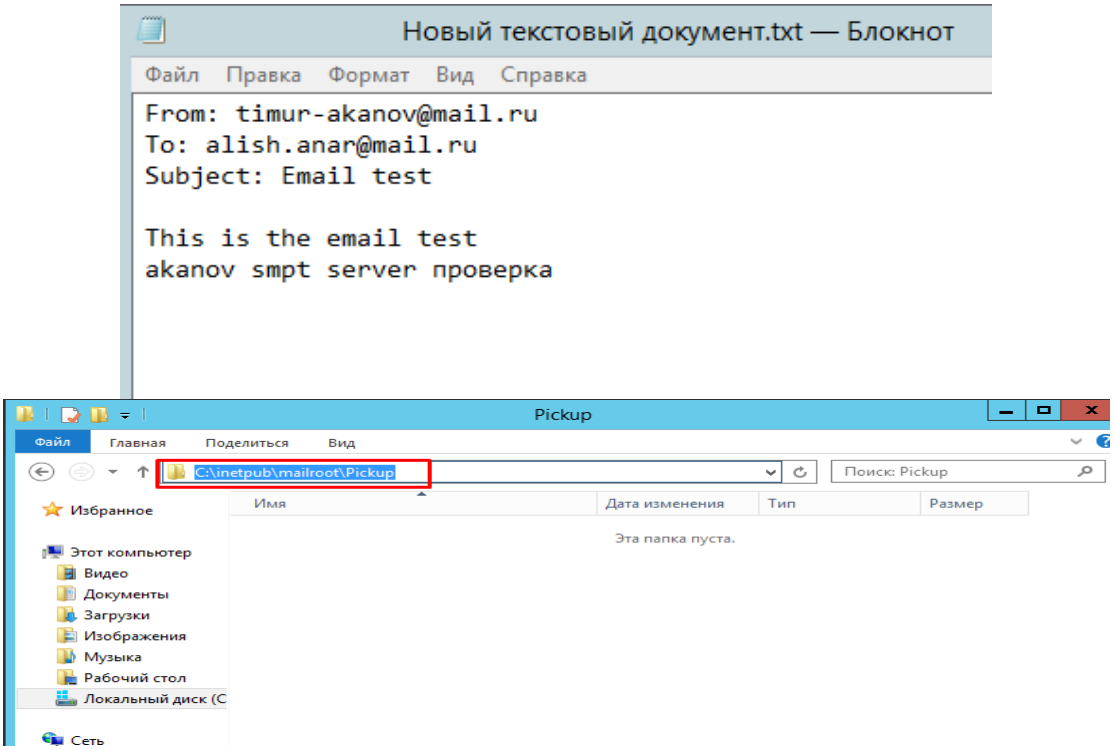

Рисунок 44 - Отправка почти через SMTP server

Далее перенесите созданный файл в директорию C:\inetpub\mailroot\Pickup. Файл исчезнет спустя короткий промежуток времени. Проверьте полученное письмо.

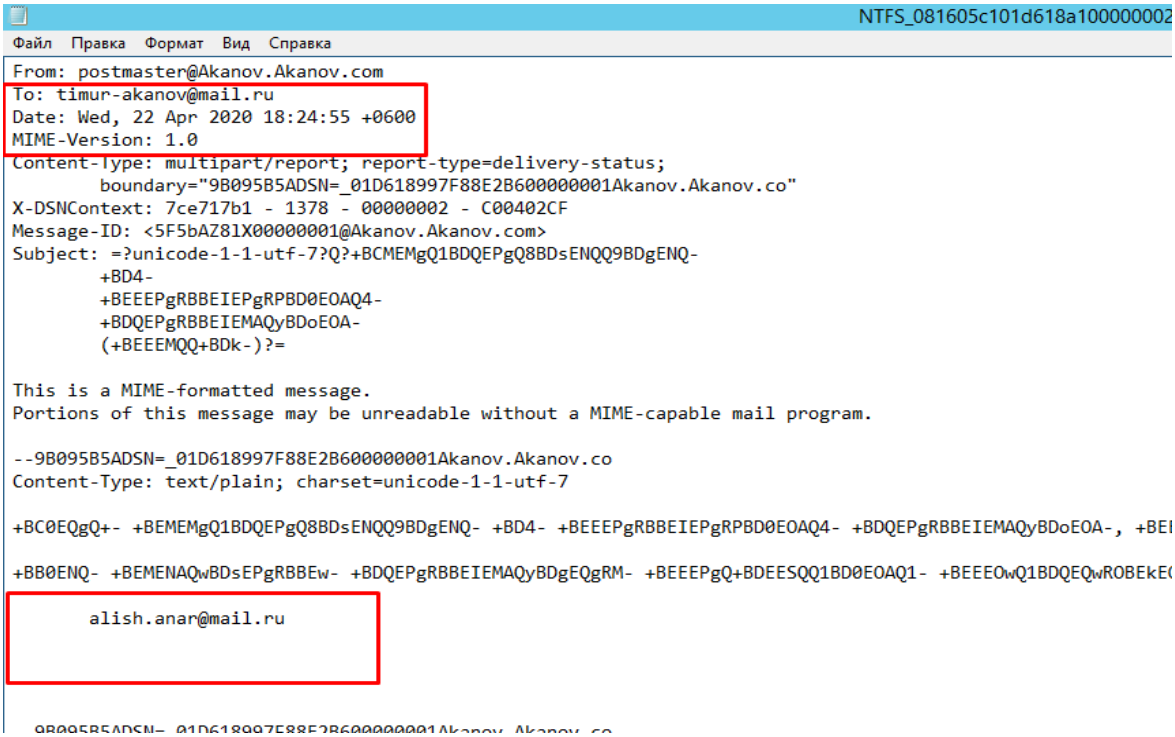

Рисунок 45 - Проверка подлинности отправки почты

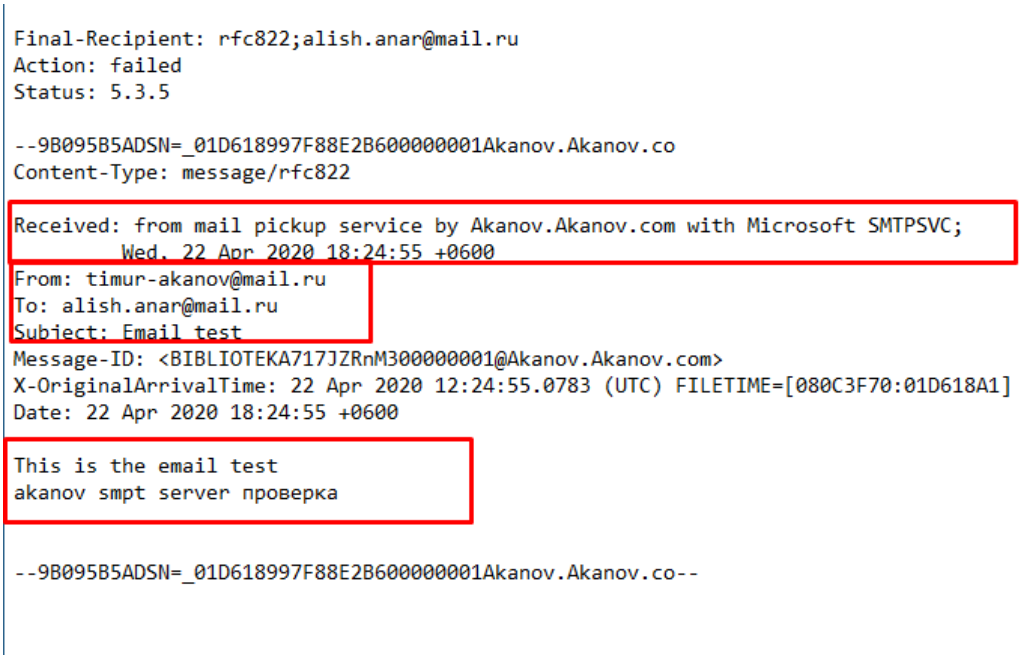

Рисунок 46 - Файл отправителя и получателя

Simple Mail Transfer Protocol (SMTP) – это протокол, используемый для передачи электронной почты в сети Интернет. Как правило, локальный SMTP-сервер будет расположен в зоне DMZ, таким образом, почта, отправленная удаленными SMTP-серверами, пройдет через межсетевой экран для достижения локального сервера. Локальные пользователи будут использовать программное обеспечение клиента e-mail для того, чтобы получить электронную почту с локального SMTP-сервера. Протокол SMTP также

используется при отправке клиентами электронной почты, SMTP ALG может использоваться для мониторига SMTP-трафика между клиентами и серверами.

Основные функции SMTP ALG:

-email rate limiting можно назначить максимально допустимую скорость передачи e-mail сообщений. Данный показатель рассчитывается на основе IP-адреса источника, другими словами, это не общий показатель, представляющий интерес, а показатель, зависящий от определенного источника email. Данная функция является очень полезной, так как обеспечивает защиту от клиентов или серверов, зараженных вирусом, отправляющих большое количество вредоносных сообщений;

-email size limiting можно назначить максимально допустимый размер e-mail сообщений. С помощью данной функции можно подсчитать общее количество байт для одного сообщения, к которому относятся: размер заголовка, размер содержимого, размер любого вложения после шифрования;

-email address blacklisting можно внести в «черный список» адреса отправителя или получателя электронной почты для того, чтобы заблокировать сообщения с данными адресами. «Черный список» применяется после «белого списка», таким образом, если адрес соответствует записи в «белом списке», проверка на наличие его в «черном списке» не выполняется;

-email address whitelisting можно внести в «белый список» адреса отправителя или получателя электронной почты для того, чтобы разрешить прохождение через ALG независимо от того, занесен ли адрес в «черный список» или письмо отмечено как «спам»;

-verify MIME type можно проверить содержание прикрепленного файла на соответствие с указанным расширением;

-block/Allow filetype предварительно определенные расширения файлов из списка могут быть заблокированы или разрешены как вложения, в список могут быть добавлены новые расширения файлов;

-anti-Virus scanning антивирусная подсистема NetDefendOS может выполнить сканирование вложения email для выявления вредоносного кода. Подозрительные файлы могут быть удалены или просто занесены в журнал.

Порядок SMTP-фильтрации

SMTP-фильтрация выполняется в порядке, аналогичном порядку выполняемому HTTP ALG за исключением добавления фильтрации спама:

1. «Белый список».
2. «Черный список».
3. Фильтрация спама (если включено).
4. Антивирусное сканирование (если включено).

Как описано выше, если адрес находится в «белом списке», он не будет заблокирован, даже если он также находится в «черном списке». Фильтрация спама (если функция включена) применяется к адресам из «белого списка», но пакеты с адресами e-mail, отмеченными как «Спам», не будут отклонены, а только зарегистрированы. Антивирусное сканирование (если функция

включена) применяется даже в тех случаях, если адрес e-mail находится в «белом списке.

Порядок обработки SMTP ALG.

В записях, сделанных в белых и черных списках можно использовать метод подстановки *(wildcarding)* для того, чтобы иметь одну запись вместо большого количества потенциальных адресов электронной почты. Подстановочный символ «*» можно использовать для представления любой последовательности символов.

Например:

- запись адреса **@some_domain.com* может использоваться для определения всех возможных адресов электронной почты для *some_domain.com* ;

- если подстановка (wildcarding) используется в «черном списке» для блокировки всех адресов для определенной компании под именем my_company, то в черный список следует добавить запись *@my_company.com ;

- если необходимо разрешить передачу сообщений только для одного отдела под именем my_department в my_company, то в «белый список» добавляется запись в виде my_department@my_company.com.

SMTP ALG и ZoneDefense.

SMTP используется как клиентами, которым необходимо отправить электронную почту, так и почтовыми серверами, которые передают сообщения на другие почтовые серверы.

Совместное использование ZoneDefense и SMTP ALG обеспечивает блокировку локальных клиентов, которые занимаются распространением вирусов, прикрепляя их к исходящим сообщениям. Не рекомендуется использовать технологию ZoneDefense для блокировки сообщений, передаваемых на SMTP-сервер, так как при этом будут заблокированы все входящие сообщения с заблокированного почтового сервера.

Например, если удаленный пользователь отправляет сообщение, зараженное вирусом, используя широко известную почтовую службу, блокировка отправляющего сервера с помощью ZoneDefense заблокирует все последующие сообщения от той же службы, отправленные любому локальному получателю. Поэтому рекомендуется использовать технологию ZoneDefense совместно с SMTP ALG для блокировки локальных клиентов e-mail.

Для того чтобы выполнить блокировку, администратор устанавливает сетевой диапазон ZoneDefense, содержащий всех локальных SMTP-клиентов. При попытке клиента отправить сообщение, зараженное вирусом, вирус будет заблокирован и ZoneDefense изолирует хост.

Отмена блокировки некоторых хостов и серверов может быть настроена вручную путем добавления их в список ZoneDefense Exclude.

POP3 – это протокол передачи сообщений, который отличается от SMTP-протокола тем, что передает сообщение напрямую от сервера на программное обеспечение клиента, используемого пользователем.

Основные функции POP3 ALG:

1. Block clients from sending USER and PASS command. Блокировка соединений между клиентом и сервером, отправляющим имя пользователя/пароль в виде текста, который можно легко прочитать (некоторые серверы могут поддерживать только этот метод).

2. Hide User. Данная функция предупреждает POP3-сервер, что имя пользователя не существует. Это позволяет пользователям подбирать различные имена, пока не будет найдено корректное имя.

3. Allow Unknown Commands. Можно разрешить или запретить нестандартные команды POP3, не распознанные объектом ALG.

4. Fail Mode. Можно разрешить или запретить прохождение файлов с нарушенной целостностью, обнаруженных при сканировании.

5. Verify MIME type. Можно выполнить проверку содержимого прикрепленного файла на соответствие указанному расширению.

6. Block/Allow type. Предварительно определенные расширения файлов могут быть дополнительно заблокированы или разрешены, а новые расширения могут быть добавлены в список.

7. Anti-Virus Scanning. Подсистема антивирусного сканирования NetDefendOS может дополнительно просканировать вложения электронной почты для обнаружения вредоносного кода. Подозрительные файлы могут быть отброшены или просто зарегистрированы.

Задание - необходимо заблокировать почтовые домены mail.ru, yandex.ru, google.ru для почтовых клиентов lan-сети. Отдельно необходимо заблокировать почтовый ящик baduser на любом почтовом домене .kz.

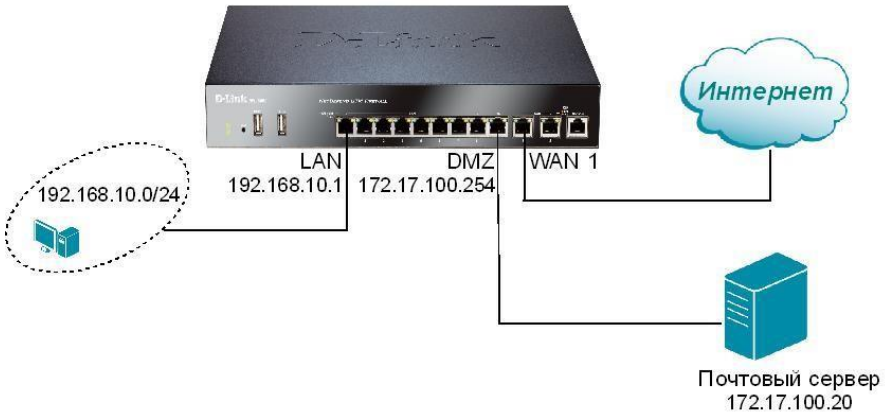

Рисунок 47 - Порты межсетевого экрана

Подаем питание на межсетевой экран. Соединяем сетевым кабелем компьютер и межсетевой экран (LAN-порт) .

Интерфейс межсетевого экрана NetDefend и интерфейс рабочей станции должны быть в одной и той же сети для успешной коммуникации между ними.

Зададим сетевые настройки:

Для ОС Microsoft Windows XP: Пуск → Настройка → Сетевые подключения → Подключение по локальной сети → Свойства → Протокол Интернета TCP/IP → Свойства → Использовать следующий IP-адрес

Для ОС Microsoft Windows Vista/ Windows 7: Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера → Подключение по локальной сети → Свойства → Протокол Интернета TCP/IPv4 → Свойства → Использовать следующий IP-адрес

Введите параметры:

IP-адрес	192.168.10.2
Маска	255.255.255.0
Основно	192.168.10.1

Для получения доступа к Web-интерфейсу, используя заводские настройки по умолчанию, запустите Web-браузер на рабочей станции (рекомендуется последняя версия Internet Explorer или Firefox) и наберите адрес - , https://192.168.10.1.

При успешной установке соединения с NetDefendOS, появится диалоговое окно аутентификации пользователя.

Рисунок 48 - Вход в web-интерфейс

Введите имя пользователя и пароль, затем нажмите кнопку Login.

Имя пользователя по умолчанию – admin, пароль по умолчанию – admin.

Если учетные данные пользователя корректные, выполняется переход на главную страницу Web-интерфейса .

Зайдите *Interfaces ->Ethernet*.

Выберите **wan1** и уберите галочку с поля **Enable DHCP Client. ОК.**

Зайдите *Objects -> Address book ->InterfaceAddresses*:

Отредактируйте IP-адреса WAN1, LAN и DMZ:

Значение **lan_ip** **192.168.10.1**

Значение	**lannet**	**192.168.10.0/24**
Значение	**wan1_ip**	**192.168.110.1**
Значение	**wan1 net**	**192.168.110.0/24**
Значение	**dmz**	**172.17.100.20**
Значение	**dmz net**	**172.17.100.0/24**

Создадим объект «IP-адрес почтового сервера в dmz-зоне».

Зайдите в меню *Objects→Address Book→Add→IP4 Address.* Введите следующие параметры:

Таблица 9 - Ввод параметров в web-интерфейс

Name	email_server
Address	172.17.100.20
Настройка ALG	
Создайте SMTP ALG. Зайдите в меню *Objects→ALG→Add→SMTP ALG*.	
Введите:следующие параметры на вкладке *General*:	
Name	smtp_alg
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient.*	
Введите следующие параметры:	
Sender/Recipient to	Sender
Classify the email	Blacklist
Email	*@mail.ru
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient.*	
Введите следующие параметры:	
Sender/Recipient to	Sender
Classify the email	Blacklist
Email	*@yandex.ru
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient*	
Введите следующие параметры:	
Sender/Recipient to	Sender
Classify the email	Blacklist
Email	*@google.ru
Во вкладке *Whitelist/Black list* добавьте новый *Email Sender/Recipient*,	
Введите следующие параметры:	
Sender/Recipient to	Sender
Classify the email	Blacklist
Email	baduser@*.ru

Продолжение таблицы 9

Создайте POP3 ALG. Зайдите в меню *Objects→ALG→Add→POP3 ALG*.	
Введите следующие параметры во вкладке *General*:	
Name	pop3_alg
Block clients from sending USER and PASS command	Поставьте галочку
Allow unknown commands	Уберите галочку
Создание SMTP-сервиса	
Создадим сервис smtp-inbound (если его нет в разделе *Service*).	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service с параметрами:	
Name	smtp-inbound
Type	TCP (выберите из списка)
Destination	25
ALG	smtp_alg (выберите из списка ранее созданный
Создание POP3-сервиса	
Зайдите в меню *Objects→Services*, добавьте TCP/UDP Service со	
Name	pop3
Type	TCP (выберите из списка)
Destination	110
ALG	pop3_alg (выберите из списка ранее созданный
Настройка IP Rule	
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule для SAT*General*:	
Введите параметры во вкладке	
Name	SAT-smtp
Action	SAT
Service	smtp-inbound
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip (настраиваем для внешнего интерфейса)
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP Address	email_server (внутренний IP-адрес почтового

Продолжение таблицы 9

Зайдите в меню *Rules→IP Rules*. Добавьте новое второе IP Rule для SAT.	
Введите параметры во вкладке *General*:	
Name	Allow-smtp
Action	Allow
Service	smtp-inbound
Source Interface	wan1
Source Network	all-nets
Destination Interface	core
Destination Network	wan1_ip
Зайдите в меню *Rules→IP Rules*. Добавьте новое IP Rule, введите параметры	
Name	NAT-pop3
Action	NAT
Service	pop3
Source Interface	lan
Source Network	lannet
Destination Interface	dmz
Destination Network	email_server
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

Отправьте почтовому клиенту, защищенному межсетевым экраном, письмо с заблокированных почтовых доменов и с незаблокированных почтовых доменов, а также от имени baduser - baduser@ya.ru

ksuser@mail.ru ksuser@yandex.ru

ksuser@google.ru ksuser@jmail.com.

3.4 Фильтрация спама при помощи DNSBL

Нежелательные сообщения, часто упоминаемые как «спам», стали причиной раздражения пользователей, а также проблемой безопасности в сети Интернет. Нежелательные сообщения, разосланные в огромных количествах группами лиц, известных как «спамеры», могут расходовать ресурсы, содержать вредоносные программы, а также пытаться направить пользователя на Web-страницы, использующие уязвимые места браузера.

Неотъемлемой частью NetDefendOS SMTP ALG является модуль *фильтрации спама*, обеспечивающий фильтрацию входящих сообщений на основании источника. Это может существенно снизить нагрузку на почтовые ящики пользователей, находящихся за межсетевым экраном. NetDefendOS предлагает два способа обработки спама:

Отбрасывание сообщений с большой вероятностью содержания спама. Разрешение на прохождение сообщений email с небольшой вероятностью содержания спама.

Разрешение прохождения сообщений email с небольшой вероятностью содержания спама.

Система NetDefendOS применяет фильтрацию спама для сообщений, проходящих через межсетевой экран с удаленного SMTP-сервера на локальный SMTP-сервер с которого позднее локальные клиенты загрузят сообщения электронной почты. Как правило, локальный защищенный SMTP-сервер будет установлен в зоне DMZ.

Ряд доверенных организаций поддерживает общедоступную базу данных IP-адресов SMTP-серверов, рассылающих спам, запрос на которые может быть выполнен через Интернет. Эти списки известны как базы данных *DNS Black List* (DNSBL), эту информацию можно получить с помощью стандартизированного метода запросов, поддерживаемого системой NetDefendOS.

Ниже показаны все используемые компоненты фильтрация спама с помощью DNSBL.

Рисунок 48 - Схема фильтрация спама с помощью DNSBL

Фильтрация спама с помощью DNSBL

При настройке функции фильтрации спама, IP-адрес сервера-отправителя сообщения может быть отправлен на один или более DNSBL-серверов, для поиска IP-адреса в спам базах DNSBL.

Сервер отправляет ответ, что IP-адрес либо не находится в списке, либо внесен в список. В последнем случае, когда IP-адрес находится в списке, DSNBL-сервер указывает, что возможно сообщение электронной почты является спамом. Кроме того, как правило, может предоставлять информацию, известную как запись *TXT*, представляющую собой текстовое пояснение к списку.

Администратор может настроить SMTP ALG для обращения к нескольким DNSBL-серверам в целях составления мнения об адресе источника сообщения e-mail. Когда приходит новое сообщение, серверы

опрашиваются для выявления вероятности того, является ли сообщение спамом, основанной на адресе источника.

Администратор NetDefendOS назначает весовое значение больше нуля для каждого настроенного сервера, таким образом, взвешенная сумма (weighted sum) может быть вычислена на основе всех ответов.

Администратор может настроить одно из следующих действий, основанных на вычисленной сумме:

1. Dropped (Отбрасывание пакетов). Если сумма больше или равна предварительно определенному значению *Drop threshold,* то сообщение рассматривается как спам и будет отброшено или отправлено в специальный почтовый ящик. Если сообщение отклонено, то администратор отправляет сообщение об ошибке на SMTP-сервер отправитель.

2. Flagged as SPAM (Отметка «Спам»). Если сумма больше или равна предварительно определенному значению *SPAM threshold,* то сообщение рассматривается как возможный спам и будет перенаправлено получателю с уведомляющим вложенным текстом.

Пример вычисления значения порога. Предположим, что настроено три DNSBL-сервера: dnsbl1, dnsbl2 и dnsbl3. Им назначаются весовые значения **3**, **2** и **2** соответственно. Установленное значение порога спама – **5**.

Если *dnsbl1* и *dnsbl2* считают, что сообщение является спамом, а *dnsbl3* так не считает, в результате получаем итоговую сумму **3+2+0=5.** Так как итоговая сумма **5** равна (или больше) значению порога, то сообщение email рассматривается как спам.

Если установленное значение *Drop threshold* – **7**, то всем трем DNSBL-серверам необходимо ответить, чтобы на основании вычисленной суммы (**3+2+2=7**) отбросить сообщение.

Если вычисленная сумма больше или равна значению *Drop threshold,* то сообщение не будет перенаправлено назначенному получателю. Вместо этого, администратор может выбрать один из двух альтернативных вариантов для отброшенных сообщений:

Можно указать определенный адрес электронной почты для всех отброшенных сообщений. Если это выполнено, то любые сообщения *TXT,* отправленные DNSBL-серверами, которые идентифицировали сообщение как спам, могут быть добавлены системой NetDefendOS в заголовок перенаправленного сообщения.

Если нет адреса получателя отброшенных сообщений, то они удаляются системой NetDefendOS. Администратор может указать, что сообщение об ошибке отправлено обратно на адрес отправителя наряду с *TXT* сообщениями от DNSBL-серверов, определивших, что сообщение является спамом.

Для того чтобы выполнить настройку фильтрацию спама с помощью DNSBL в SMTP ALG, выполните следующие шаги:

Определите, какие DNSBL-серверы будут использоваться. Сервер может быть один или их может быть несколько. Несколько серверов могут

действовать в качестве дублеров друг друга, а также для подтверждения статуса отправителя.

Определите весовое значение для каждого сервера, который определит важность значения во время принятия решения, является ли сообщение спамом, при расчете взвешенной суммы.

Определите пороги для спама. Если взвешенная сумма больше или равна значению порога, то сообщение рассматривается как спам.

Определены два порога:

- порог Spam – Порог для сообщений, маркированных как спам;
- порог Drop – Порог для отбрасывания сообщений.

Значение Порога Spam должно быть меньше значения Порога Drop. Если значения порогов одинаковые применяется только Порог Drop.

Определите текстовую маркировку в качестве префикса в поле Тема сообщения, рассматриваемого как спам.

Дополнительно определите адрес email, на который будут отправляться все отброшенные сообщения.

Задание: Необходимо проверить входящие потовые сообщений на спам.

Добавим новый SMTP ALG

Зайдите в меню Objects→ALG→Add→SMTP ALG.

Таблица 10 - Ввод параметров в web-интерфейс

Во вкладке *General* введите следующие параметры:	
Name	SMTP-inbound
Email Rate	200
Email Size	5120
Fail Mode	Deny
Во вкладке *Anti-spam*:	
Check emails for mismatching SMTP command "From"	Поставьте галочку и выберите *...and block them.*
DNSBL Anti-Spam	Поставьте галочку напротив *Enable*.
Spam Threshold	3
Drop Threshold	5
Spam Tag	*** SPAM ***
Cache Size	0
Cache Timeout	600
Для *DNS Blacklists* введите спам-сервера и значения веса для них, после	
sbl.spamhaus.org	Weight Value 1
virbl.dnsbl.bit.nl	Weight Value 1
bl.spamcop.netorg	Weight Value 1
list.dsbl.org	Weight Value 1
zen.spamhaus.org	Weight Value 1

Таблица 11 - Ввод Настройка IP Rule

Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	email_spam
Action	SAT
Service	smtp-inbound (содержит SMTP ALG)
Source Interface	wan1
Destination	core
Source Network	all-nets
Destination	wan1_ip
Введите параметры во вкладке *SAT*:	
Translate the	Destination IP Address
To New IP	email_server
Зайдите в меню *Rules→IP Rules→Add→IP Rule.* Во вкладке *General* введите следующие параметры:	
Name	email_spam2
Action	Allow
Service	smtp-inbound
Source Interface	wan1
Destination	core
Source Network	all-nets
Destination	wan1_ip
Зайдите в меню *Configuration* и выберите *Save and Activate*.	

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Основной целью данного дипломного проекта является проектирование программно-аппаратного комплекса для обеспечения безопасности объекта. Актуальность этой темы заключается в том, что на данный момент информация является ценным ресурсом, с которым необходимо правильно взаимодействовать, и если мы допустим вероятность потери данных, это оценивается в огромный материальный ущерб.

Это исследование может быть использовано для реализации корпоративной сети почтового сервера . Благодаря этому исследованию, обеспечение безопасности внутренних и внешних пространств объекта, прилегающей территории, людей, материальных и интеллектуальных ценностей будет контролироваться круглосуточно и отслеживаться событиями в реальном времени и анализом данных.

Обеспечение безопасности труда и отдыха способствует сохранению жизни и здоровья человека за счет снижения травматизма и заболеваемости.

Вопросы безопасной жизнедеятельности человека необходимо решать на всех стадиях жизненного цикла, будь то разработка, эксперимент или применение разработанной методики на практике.

Работа с вычислительной техникой по вредности относится к безопасным (риск смерти на человека в год составляет менее 0.0001). Тяжесть труда у работника вычислительной техники также минимальна, так как уровень психической нагрузки по этому роду деятельности предусматривает энергозатраты 2000...2400 ккал в сутки.

Однако сотрудник при работе с вычислительной техникой подвергается воздействию комплекса неблагоприятных факторов, обусловленных характером производственного процесса условий труда:

- повышенная интенсивность работы и ее монотонность;
- специфический характер зрительной работы;
- тепловыделение от оборудования;
- воздействие шума;
- воздействие ионизирующих и неионизирующих излучений, вредных
- неудовлетворительные условия световой среды в помещении и освещения на рабочем месте.

Анализ условий труда и мероприятия по защите от воздействия вредных производственных факторов.

Анализ условий труда.

При исследовании и настройке программного обеспечения сотруднику приходится долго взаимодействовать с компьютерным оборудованием. Рабочая зона - это зона временного или постоянного присутствия работника. В связи с тем, что работник должен долго находиться в сидячем положении, должны быть предусмотрены меры максимального комфорта, которые позволят работать комфортно и без вредных воздействий. Эти меры должны включать: компьютерное оборудование и мебель должны быть расположены оптимально, достаточное рабочее пространство, которое позволит работнику выполнять все необходимые действия и движения, работник должен получать необходимое количество световых лучей, чтобы минимизировать нагрузку на зрение. Существует несколько видов освещения, естественное и искусственное. [1].

Естественное освещение - освещение, которое проникает через световые проемы и является дневным светом. Этот тип освещения меняется в зависимости от природных условий, времени суток и времени года.

Искусственное освещение - освещение, при котором естественное освещение не задействовано и может использоваться ночью и при недостаточном естественном освещении.

Использование искусственного и естественного освещения одновременно называется комбинированным освещением.

Правильность выбора освещения и освещения в виде ламп и светильников, а также правильное расположение обеспечат не вызывающее

привыкания, значение 40 кд / м ^ 2 отражения бликов на рабочей станции и рабочей поверхности.

Для искусственного освящения следует использовать люминесцентные лампы белого света. Металлогалогенные лампы мощностью до 250 Вт могут использоваться в производственных условиях и административных общественных помещениях.

4.1 Характеристики рабочего помещения.

Рабочее помещение, в котором работники проводят свое исследование рассчитан на три рабочих места. Располагается на 1 этаже жилого здания. Визуализированная модель помещения представлена на Рисунке 48.

Характеристики помещения: длина L = 10 метра, ширина B = 5 метров, высота H = 3 метра. Помещение было построено и оборудовано согласно санитарным требованиям от 01.12.2019 года, т.е. площадь одного рабочего места 4,5 метра в квадрате, а монитор должен находиться на расстоянии 60см от глаз. Рабочее пространство работника удовлетворяет требованиям и составляет 50 м^2.

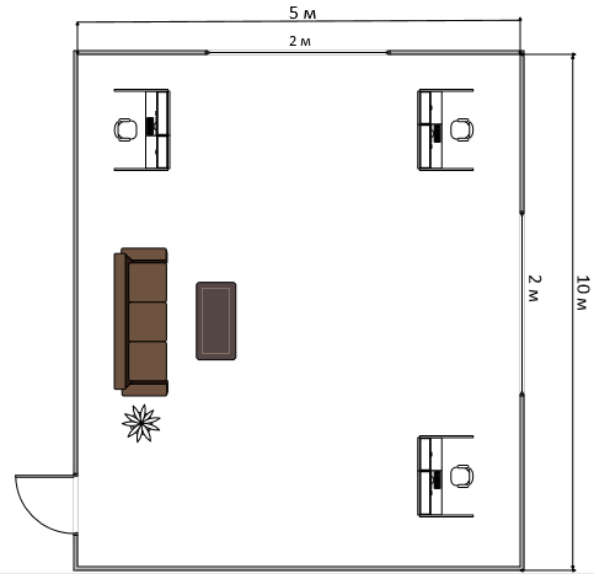

Рисунок 49 - Рабочее помещение

Используемое оборудование и его характеристики

Ноутбук Lenovo ideopad E5-575G. Технические характеристики устройства:

- Intel(R) Core i7 6498DU (CPU 2.60 GHz);
- AMD Radeon graphics;
- ОЗУ 8 ГБ;
- HDD 1 ТБ;
- электропитание: 220-250В, 50Гц, 400 Вт;
- габариты(мм): 270 - 414 – 32,5.

Модем: 4-х портовый с коммутатором 10/100 Мбит/с.

Стул: высота 0,6 м.

Стол: высота – 0,8 м, длина – 4 м, ширина – 1 м.

4.2 Расчет естественного освещения.

Один из главных показателей, который должен находить на заданном уровне, это освещение. Качество освещения важно для создания удобства при работе. Хороший уровень освещения необходим для комфортной работы и исключения зрительного напряжения, которое в следствии может привести к ухудшению здоровья и сказаться на качестве работы. Согласно нормам освещенности (СНиП 11-4-79) и отраслевым нормам, работа инженера относится к четвертому разряду зрительной работы. Важно проводить расчеты по освещению, они необходимы для определения площади световых проёмов естественного освещения и характеристики искусственного освещения. Формула (1) для расчета площади световых проемов при естественном освещении:

$$S = \frac{(S_n * e_n * K_n * h_0 * K_{зо})}{(100 * t_0 * r_1)} \quad (4.1)$$

где S_n – площадь помещения, м^2;

e_n – нормированное значение КЕО, %;

K_n – коэффициент запаса;

h_0 – световая характеристика окон (6,5 - 29);

$K_{зо}$ – коэффициент затемнения окон зданиями стоящими напротив (1,0-1,7);

r_1 – коэффициент повышение КЕО за счет отраженного света от поверхности помещения (1,05 - 1,7);

t_0 - общий коэффициент светопропускания равен от 0,1-0,8.

Полагаясь на данные характеристики, длина помещения равна 5 метров, а ширина равно 4 метра, можно найти площадь пола по следующей формуле:

$$S_n = L * B \quad (4.2)$$

Для данного рабочего пространства площадь световых проемов естественного бокового освещения определяется формулой (1), необходимы следующие значения:

где $e_n = 1{,}5$ %;

$K_n = 2$;

$h_0 = 21$;

$K_{зо} = 1{,}2$;

$r_1 = 1{,}5$;

$t_0 = 0{,}8$.

Теперь необходимо подставить значение данных коэффициентов в формулу (0,1) и вычислить площадь световых проемов:

$$S = \frac{50 * 1{,}5 * 2 * 21 * 1{,}2}{100 * 0{,}8 * 1{,}5} = 31{,}5 \text{ м}^2$$

Рассчитав площадь оконного пространства, значение вышло 31.5 $м^2$, из чего следует вывод что необходимо искусственное освещение так как окна площадью 2 $м^2$ недостаточно для создания комфортных условий освещения.

4.3 Расчет искусственного освещения.

Основываясь на норму СНиП 11-4-79 для четвертого класса зрительных работ освещенность помещения должно быть не менее 200 Лк. Номинальная освещенность рабочего места определяется формулой:

$$E = \frac{Ф_{св} * n * N * 1}{s * К_з * Z} \quad (4.3)$$

где, $Ф_{св}$ – световой поток от ламп, Лк;
N – количество светильников;
$К_з$ – коэффициент, учитывающий запыленность светильников;
n – коэффициент использования светильников;
s – площадь помещения, $м^2$;
z – коэффициент неравномерности освещения.

Основываясь на норму СНиП 11-4-79 для типа ламп, который будут использоваться $К_з = 1{,}4{:}\ 1{,}5$ при нормальной эксплуатации светильников; z = 1,1:1,2 при оптимальном их размещении. В данном случае коэффициент n полностью зависит от светильников и их типа, коэффициенты отражения светового потока от потолка - p_2, от пола p_3, от стен p_1, зависят от размера помещения, учитывающих величиной I, где I это индекс помещения. [2]

$$I = \frac{(A * B)}{h_c * (A + B)} \quad (4.4)$$

где A, B - параметры помещения, м;
h_c - высота светильников над рабочей поверхностью.
Расчёт высоты светильников над рабочей поверхностью выводится по формуле:

$$h_c = H_{помещения} - H_{свеса} - H_{р.п.} \quad (4.5)$$

где $H_{свеса}$ = 0,4 - высота свеса ламп, м;

$H_{р.п.}$ = 0,8 - расстояние рабочей поверхности над полом, м;

$H_{помещения} = 3$ - высота помещения, м.

Основываясь на формулу (0.5) определяется высота светильников над рабочей поверхностью:

$$h_{расч} = 3 - 0{,}4 - 0{,}8 = 1{,}8 \text{ м}$$

Зная что параметры помещения равны 4м × 5м и высота светильников над рабочей поверхностью $h_c = 1{,}8$м, по формуле (4):

$$I = \frac{(5 * 10)}{2 * (5 + 10)} = 0{,}5$$

Основываясь на таблицу (0.1) определяется коэффициент использования светового потока n, учитывая, что коэффициенты p_1 = 30%, $p_2 = 50\%$, $p_3 = 10\%$.

Таблица 12 - Значения коэффициента использования светового потока

Коэффициент I	0,5	1	2	3	4
Коэффициент использования светового X потока, h	0,22	0,36	0,48	0,54	0,59

Коэффициент n = 0,3 для рабочего места. От лампы типа ДРЛ-80 световой поток равняется 3800 Лк, в совокупности от 2 ламп световой поток будет равняться 7600 Лк. Основываясь на все вычисления и данные можно определить номинальную освещенность рабочего места по формуле (0.3). [5]

$$E = \frac{7600 \cdot 0{,}3 \cdot 3}{20 \cdot 1{,}4 \cdot 1{,}2} = 203{,}5 (Лк)$$

Значение, полученное в ходе расчётов, соответствует нормальным условиям освещенности и создается комфортную для работы обстановку.

4.4 Определение расчета кратности воздухообмена

Кратность воздухообмена — санитарный показатель состояния воздушной массы в помещении. От этого параметра зависит безопасность и комфорт людей. Допустимые значения регулирует государство — в строительных нормах и правилах (СНиП), сводах правил (СП), санитарных правилах и нормах (СанПиН) и ГОСТах. Кратность воздушного обмена показывает, сколько раз в течение часа воздух заменялся на новый.

Есть 2 типа воздухообмена: естественный и искусствен-ный. Естественный способ обмена заключается в движении воздушных масс за счет разницы давления. Из точек с большим давлением — в места с меньшим. Искусственный воздухообмен подразумевает работу вентиляторов, кондиционеров и других электрических устройств.

Формула кратности воздухообмена выглядит так[3]:

$$\mathbf{N = Q / V} \qquad (4.6)$$

где, N или n — кратность (раз в час);

Q - нужное количество свежего воздуха в час, м³/ч;

V - объем помещения, м³; если у комнаты сложная форма, объем нужно определять вместе со специалистами.

Естественное замещение воздуха ограничивается 3-4-кратным показателем, поэтому его движение иногда приходится усиливать механической вентиляцией.

Вентиляционные системы работают по 2 схемам: вытесняют старый воздух новым или перемешивают обе эти массы.

Для систем, работающих только на удаление воздуха, основная формула кратности выглядит следующим образом: [4]

$$\mathbf{N = V\ у.\ в. / V\ пом}, \qquad (4.7)$$

где, V у. в. — объем удаляемого воздуха, м³/ч;

V пом — объем помещения, м³.

В удаляемый объем следует включать тепловые выделения и летучие вредные вещества.

Для приточной и вытяжной вентиляции рассчитывают также отдельные показатели кратности.

К примеру, для приточной системы его определяют так[7]:

$$\mathbf{N_{пр} = L\ пр / V\ пом}, \qquad (4.8)$$

где, L пр — производительность приточной системы, м³/ч;

V пом — объем помещения, м³.

На одного сотрудника следует отводить 60 м³/ч, а на временного посетителя — 20 м³/ч. Удельная кратность выступает как информативный показатель при условии, что размеры помещения приближаются к стандартным.

В офисах и административных учреждениях требуется больше свежего воздуха, чем в индивидуальном жилье. Причина этому — большое количество офисной техники, напряженная умственная деятельность и стандарты обслуживания клиентов.

Новый воздух должен эффективно удалять испарения. Стоит уделить внимание увлажнению и очистке воздуха, его охлаждению или прогреву перед подачей в помещения.

В рабочей комнате на 1 сотрудника нужно не меньше 20 м³/ч. В конференц-залах столько же отводят на каждого посетителя. Интенсивный воздухообмен следует обеспечивать в умывальных и санитарных комнатах — до 15 обновлений воздуха в час.

Возьмем для примера помещение высотой 3,5 м и площадью 60 м², где работает 15 человек. Считаем, что воздух загрязняется только от роста концентрации углекислого газа из-за дыхания.

Сначала находим объем помещения: V = 2 м × 10 м² = 20 м³.

Учитываем, что 1 среднестатистический человек выделяет 22,6 л углекислого газа в час[8].

Получаем, что вредные выделения можно рассчитать формулой

В = 22,6 × n, где n соответствует количеству людей в помещении.

В = 22,6 л/ч × 15 = 339 л/ч

Для помещений максимально допустимая концентрация углекислого газа равняется 1/1000, или же 0,1 %. Переведем это в 1 л/м³. В чистом воздухе углекислого газа есть около 0,035 %. Переводим в 0,35 л/м³.

Рассчитаем по формуле 10.6, сколько свежего воздуха понадобится для всех 15 человек:

Q = 339 л/ч : 1 л/м³ – 0,35 л/м³ = 339 л/ч : 0,65 л/м³ = 521,5 м³/ч. Кубические метры в данном случае перешли в числитель, а часы — напротив, в знаменатель.

Определяем кратность воздухообмена (формула 7):

N = 521,5 м³/ч : 210 м³ = 2,48 раз в час. Выходит, при сменяемости воздуха на уровне 2,48 раз в час концентрация углекислого газа останется в пределах нормы.

Найдем теперь удельную кратность воздухозамещения на 1 человека и на 1 м². Объем помещения при этом должен быть не меньше 210 м³, а высота потолка — от 3,5 м.

521,5 м³/ч : 15 чел. = 34,7 м³/ч на 1 человека

521,5 м³/ч : 60 м² = 8,7 м³/ч на 1 м² площади

Таким образом, в помещении **удельная кратность воздухозамещения** на 1 человека 34,7 м³/ч, при том, что в рабочей комнате на 1 сотрудника необходимо не меньше 20 м³/ч.

Вывод: в данном разделе моего дипломного проекта я рассмотрел и рассчитал световые показатели для условий труда. Эти показатели одни из важнейших при организации работы, должны всегда соответствовать рамкам стандартов и нормы, поскольку это будет способствовать созданию благоприятных условий для работника и не будет мешать работе затормаживая ее. Основываясь на расчёты, могу сказать, что, для того чтобы осветить комнату площадью 50 м2 абсолютно не хватает естественного

освещения, предоставляемого с окна размером 2 метра в длину и 2 в ширину. Для удобной работы необходимо комбинированное освещение, в которое включено как естественное, так и искусственное освещение. Полагаясь на расчёты полученные в ходе выполнения этого раздела должно использоваться 2 лампы в моем случае это ДРЛ-80 3800 Лк. Если необходимые условия буду соблюдены, то работник может проводить все необходимые работы и исследование в ночное время.

Для этого необходимо было ввести в действие меры по улучшению условий труда: сокращение продолжительности воздействия шума и нервно-эмоциональной нагрузки. После введения мероприятий категория тяжести труда повышается с пятого на второй уровень. Коэффициент производительности был увеличен с 38 в относительных единицах до 77, производительность рабочей силы составил 20,5%.

5 Расчет рисков информационной безопасности

5.1 Анализ рисков информационной безопасности

Риск информационной безопасности - это вероятность раскрытия или потери в результате информационных атак или утечки данных в организации. Учитывая описанные выше риски, связанные с использованием электронной почты, организациям необходимо принять соответствующие меры для защиты от них.

Подход к защите должен быть всесторонним и комплексным — необходимо сочетать организационные меры с использованием соответствующих технических средств.

К организационным мерам относятся разработка и внедрение в компании политики использования электронной почты.

Технические средства должны обеспечить выполнение данной политики как за счет мониторинга почтового трафика, так и за счет адекватного реагирования на нарушения.

Идентификация факторов рисков - включает в себя идентификацию и ранжирование рисков

Количественная оценка риска - включает в себя определение и уточнение значения количественных показателей вероятности возникновения угрожающих событий.

Планирование реагирования на риски - включает в себя определение степени реагирования: избежание, передача, минимизация, принятие

Мониторинг и контроль рисков - действия по контролю и управлению необходимо осуществлять на протяжении всего проекта. Наступление непредвиденного рискового случая на заключительных стадиях угрожает большими потерями, чем на начальных стадиях. В ходе мониторинга пересматриваются значения уже идентифицированных рисков и иногда идентифицируются новые.

Система контроля содержимого электронной почты

Политики использования электронной почты реализуется посредством программно-технических средств - системы контроля содержимого электронной почты.

Системы контроля содержимого электронной почты — это комплекс технических средств и программного обеспечения, способное анализировать содержание письма по различным компонентам и структуре в целях реализации политики использования электронной почты.

Спектр возможностей всех категорий систем контроля содержимого электронной почты достаточно широк и существенно меняется в зависимости от производителя. Однако ко всем системам предъявляются наиболее общие требования, которые позволяют решать задачи, связанные с контролем почтового трафика.

К наиболее общим требованиям относятся:

Текстовый анализ электронной почты (анализ ключевых слов и выражений с помощью встроенных словарей). Данная возможность позволяет обнаружить и своевременно предотвратить утечку конфиденциальной информации, установить наличие непристойного или запрещенного содержания, остановить рассылку спама, а также передачу других материалов, запрещенных политикой безопасности.

Контроль отправителей и получателей сообщений электронной почты. Данная возможность позволяет фильтровать почтовый трафик, тем самым реализуя некоторые функции межсетевого экрана в почтовой системе.

Разбор электронных писем на составляющие их компоненты (MIME-заголовки, тело письма, прикрепленные файлы и т.п.), устранение "опасных" вложений и последующий сбор компонентов письма воедино.

Блокировка или задержка сообщений большого размера до того момента, когда канал связи будет менее всего загружен (например, в нерабочее время). Циркуляция в почтовой сети компании таких сообщений может привести к перегрузке сети, а блокировка или отложенная доставка позволит этого избежать.

Распознавание графических, видео и звуковых файлов. Как правило, такие файлы имеют большой размер, и их циркуляция может привести к потере производительности сетевых ресурсов. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы компании.

Обработка сжатых/архивных файлов. Это дает возможность проверять сжатые файлы на содержание в них запрещенных материалов.

Распознавание исполняемых файлов. Как правило, такие файлы имеют большой размер и редко имеют отношение к коммерческой деятельности компании. Кроме того, исполняемые файлы являются основным источником заражения вирусами, передаваемыми с электронной почтой. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы компании и избежать заражения системы.

Контроль и блокирование спама. Циркуляция спама приводит к перегрузке сети и потере рабочего времени сотрудников. Функция контроля и блокирования спама позволяет сберечь сетевые ресурсы и предотвратить снижение эффективности работы компании.

Способность определять число вложений в сообщениях электронной почты. Пересылка электронного письма с большим количеством вложений может привести к перегрузке сети, поэтому контроль за соблюдением определенных политикой информационной безопасности ограничений на количество вложений обеспечивает сохранение ресурсов корпоративной сети.

Контроль и блокирование программ-закладок (cookies), вредоносного мобильного кода (Java, ActiveX, JavaScript, VBScript и т.д.), а также файлов, осуществляющих автоматическую рассылку (так называемые "Automatic Mail-to"). Эти виды вложений являются крайне опасными и приводят к утечке информации из корпоративной сети.

Категоризация ресурсов почтовой системы компании ("административный", "отдел кадров", "финансы" и т.д.) и разграничение доступа сотрудников компании к различным категориям ресурсов сети (в т.ч. и в зависимости от времени суток).

Реализация различных вариантов реагирования, в том числе: удаление или временная блокировка сообщения; задержка сообщения и помещение его в карантин для последующего анализа; "лечение" зараженного вирусом файла; уведомление администратора безопасности или любого другого адресата о нарушении политики безопасности и т.п.

Ведение полнофункционального архива электронной почты, способного обеспечить хранение в режиме on-line большого количества электронной почты с высоким уровнем доступности данных. На основании хранящейся в архиве информации, возможно проводить дальнейший анализ почтового потока компании, корректировать работу системы, осуществлять анализ инцидентов, связанный с злоупотреблением сотрудниками компании почтовым сервисом и т.п.

На Рис. 50 представлена последовательность работы типичной системы контроля содержимого электронной почты. Схема обработки сообщения, как правило, включает в себя следующие этапы:

- рекурсивная декомпозиция электронного письма;
- анализ содержимого электронного письма;
- "категоризация" электронного письма (отнесение к определенной категории);
- действие над письмом по результатам присвоения категории.

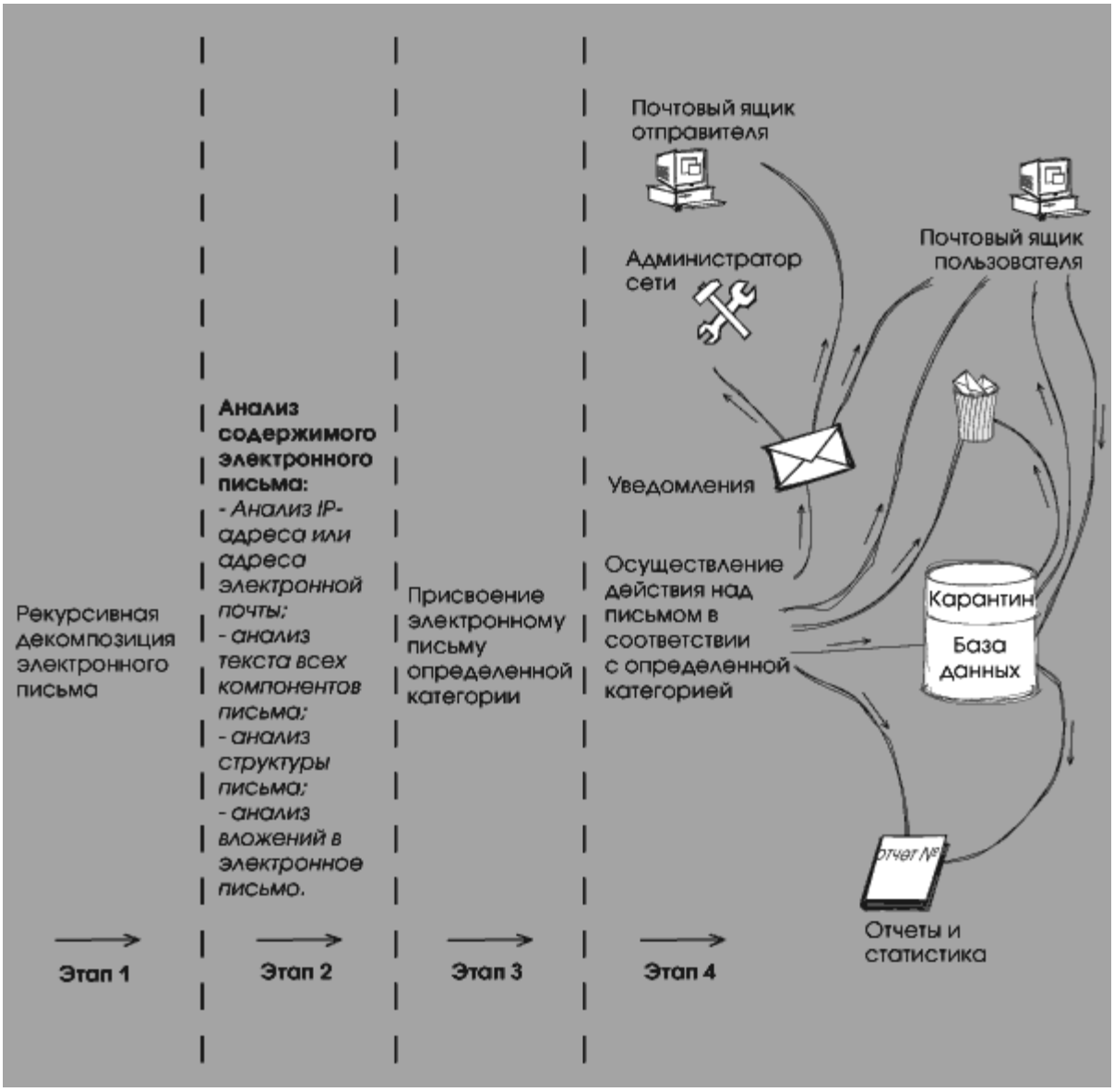

Рисунок 50 - Схема обработки сообщения системой контроля содержимого электронной почты

5.2 Метод оценки рисков по двум параметрам

Метод оценки по двум рискам включает в себя оценку вероятности возникновения угрозы и оценку возможного ущерба. Риск по данной методике определяется формулой ниже:

$$R = V * U \qquad (5.1)$$

где , R – риск;
V – вероятность;
U – ущерб.

Данный метод включает в себя три этапа:

а) первоначальный расчет рисков;

б) определение мер для неприемлемых рисков;

в) повторный расчет.

Первоначальный расчет рисков начинается с определения вероятности возникновения угрозы и возможного ущерба.

Для определения вероятности возникновения угрозы необходимо воспользоваться таблицей 9, где описано значение вероятности возникновения угрозы для расчета и его соотношение во времени.

Таблица 9 - Шкала вероятности возникновения угроз

Значение	Описание
0 - очень низкий	раз в 5 лет
1 – низкий	раз в 3 года
2 – средний	раз в год
3 – высокий	несколько раз в год
4 - очень высокий	пару раз в месяц

Для определения возможного ущерба необходимо воспользоваться таблицей 10, где описано значение ущерба для расчета .

Таблица 10 - Таблица рисков

Код	Угрозы	Уязвимость	Максимальный уровень риска	Категория риска	Остаточная мера риска
1 Microsoft Outlook 2016 Standard					
aa	Перехват данных	Возможность подмены IP-адреса источника и ресурса	6	уменьшение	4
ab	Отказ в обслуживании	Переполнения буфера обмена	6	уменьшение	4
ac	Внедрение вредоносных ПО	Отсутствие регулярных проверок и обновлении, антивирусной защиты	4	уменьшение	2
2 Рабочие компьютеры					
aad	Нарушение конфиденциальности информации	Подмену содержимого сообщение в электронной почте.	4	уменьшение	2
aae	Искажение данных	Незнание и/или несоблюдение установленных правил при работе с электронной почтой и изменение данных	6	уменьшение	4

aaf	Несанкционированное получение доступа к электронной почте через ПК сотрудника	Отсутствие проверки данных, предоставленных пользователем	3	уменьшение	3
3 Почтовый сервер					
aag	Несанкционированное получение доступа к управлению почтовом сервером	Неправильное распределение	4	уменьшение	2
aah	Отказ оборудования	Изъяны планов непрерывности	6	уменьшение	4
aak	Внедрение серверных расширений	Отсутствие проверки данных, предоставленных пользователем.	3	уменьшение	3

5.3 Метод оценивания рисков программой Coras

В данной работе применяется такой метод оценивания рисков как Coras.

В данной методологии информационные системы представлены как сложный комплекс с учётом человеческого фактора, а не только на основе используемых технологий.

Программное обеспечение использует язык UML (сокр. от англ. Unified Modeling Language – унифицированный язык моделирования) – язык графического описания для объектного моделирования в области разработки программного обеспечения.

UML является языком широкого профиля, это открытый стандарт, использующий графические обозначения для создания абстрактной модели системы, называемой UML - моделью. UML был создан в основном для определения, визуализации, проектирования и документирования программных систем

Таблица 11 - Использующиеся элементы при оценивании рисков

Вид	Название на английском языке	Название на русском
	Asset	Ценность, информация, подлежащая защите
	Threat Human Deliberate	Угроза преднамеренная, связанная с человеческим фактором воздействия
	Threat Scenario	Сценарий угрозы
	Vulnerability	Уязвимость
	Risk	Риск
	Treatment	Противодействие угрозе

Первым делом произведем описание присутствующих в организации основных активов, на которые может распространятся действие программно-аппаретного комплекса дипломного проекта. Выполним построение диаграмм в программе Coras.

На рисунке 51 показаны активы, и потоки данных, которые протекают между этими активами. Относительно проекта выделено основных актива,

это «Почтовый сервер» и «Microsoft Outlook». Потоки между данными активами протекают через Маршрутизатор. Говоря о простых примеров потоков данных можно отметить работу пользователя над какими-либо электронными документами, которые представляют некоторую ценность для организации. После описания перечня активов, можно приступать к рассмотрению списка пар угроза + уязвимость, которые могут возникать для выбранных активов.

Рисунок 52, 53 - уязвимость описывает пары угроз и уязвимостей, а также к каким активам, по какому сценарию и кем реализуются данные пары. Графическое представления данной диаграммы позволяет более наглядно понять, насколько важен процесс анализа угроз и уязвимостей в электронной почте.

После описания пар угроз и уязвимостей, можно перейти к построению диаграммы рисков, возникающих в организации относительно выбранных активов. Рисунок 54 как раз и отображает данную диаграмму, описывая основные риски, активы к которым они относятся, а также источники возникновения данных рисков.

Процесс работы с диаграммной рисков на этом не заканчивается, поскольку относительно выбранных методик расчетов, требуется произвести расчеты. Как видно из рисунка 55 каждому риску выставляется определенный числовой показатель, сопровождаемый параметром приемлемости риска для организации.

Когда произведен первичный расчет рисков в организации, можно переходить к процессу выбора мер по обработке риска. Рисунок 56 отображает диаграмму расчет риска основывался на методе по двум параметрам. Результаты расчетов позволяют наглядно увидеть текущее состояние информационной системы. Были приняты дополнительные меры защиты, направленные на снижение ранее рассчитанных рисков. После определения системы защиты информации, необходимой для снижения рисков, риски были пересчитаны таким же образом. В результате пересчета рисков с учетом внедренных систем информационной безопасности они были снижены до приемлемого уровня. Эти методы расчета риска действительно полезны и позволяют увидеть текущее состояние информационной системы с точки зрения информационной безопасности.

Активы на которые влияют данные риски показаны ниже

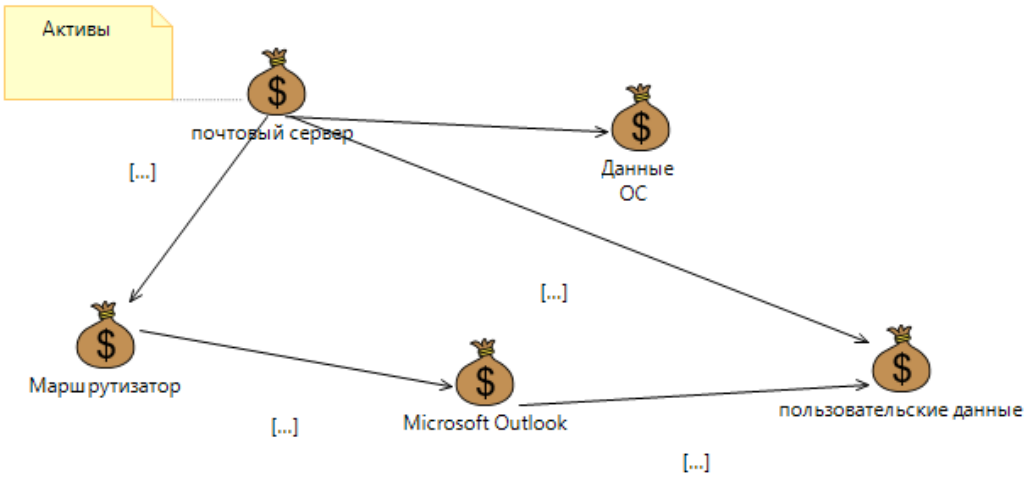

Рисунок 51 – Активы на которые влияют уязвимости

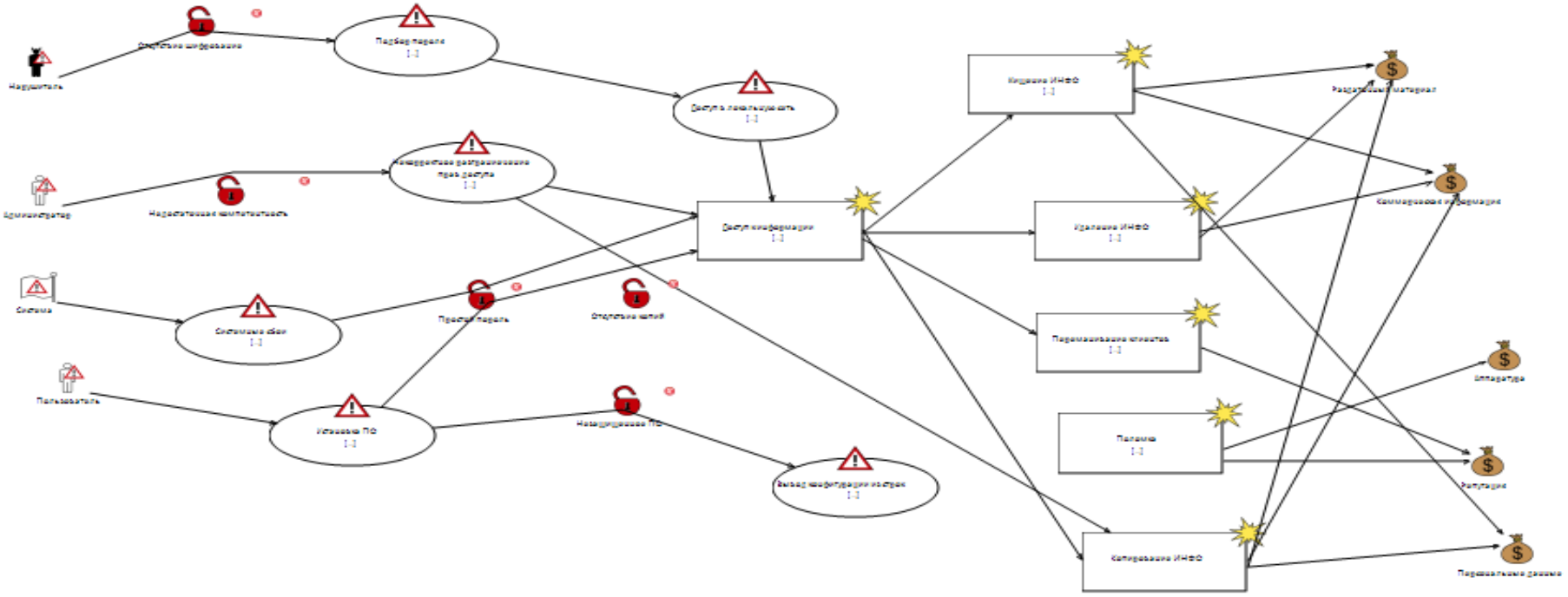

Рисунок 52 - Модель угроз

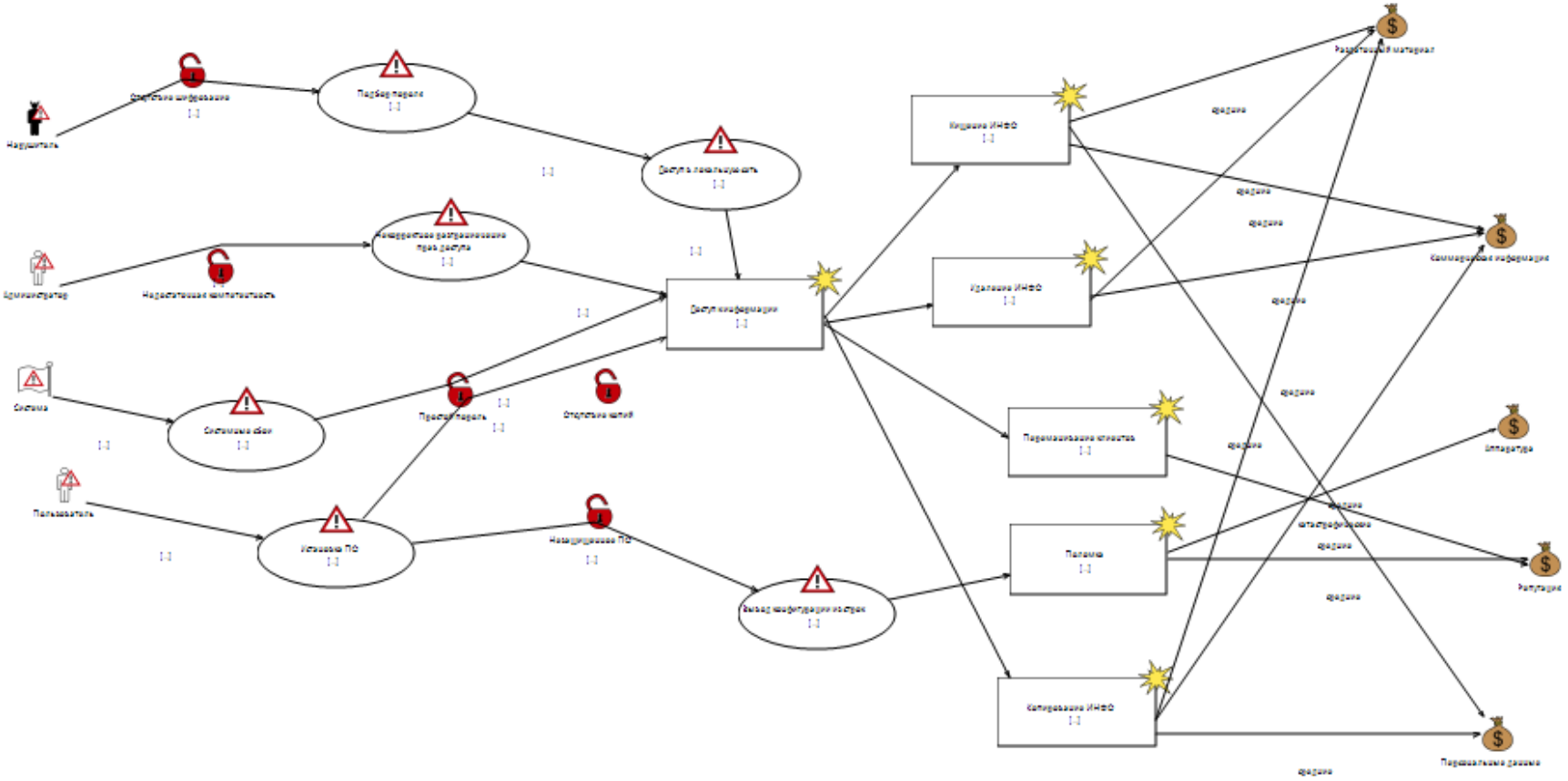

Рисунок 53 - Модель угроз с вероятностными характеристиками

Генерируем диаграмму рисков (щелкаем правой кнопкой мыши по вкладке Угрозы и выбираем Generate risk diagram). Полученная диаграмма представлена на рис.54.

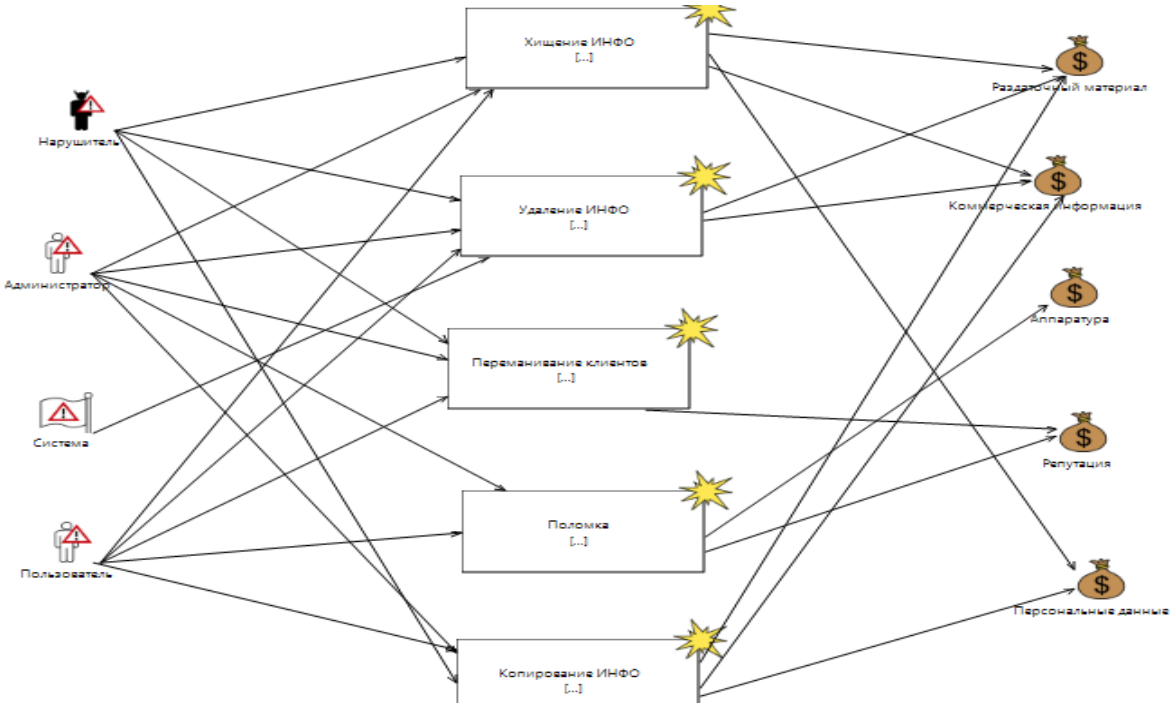

Рисунок 54 – Диаграмма рисков

Теперь по каждому риску для каждого актива определяем последствия в случае осуществления этого риска (рис.55).

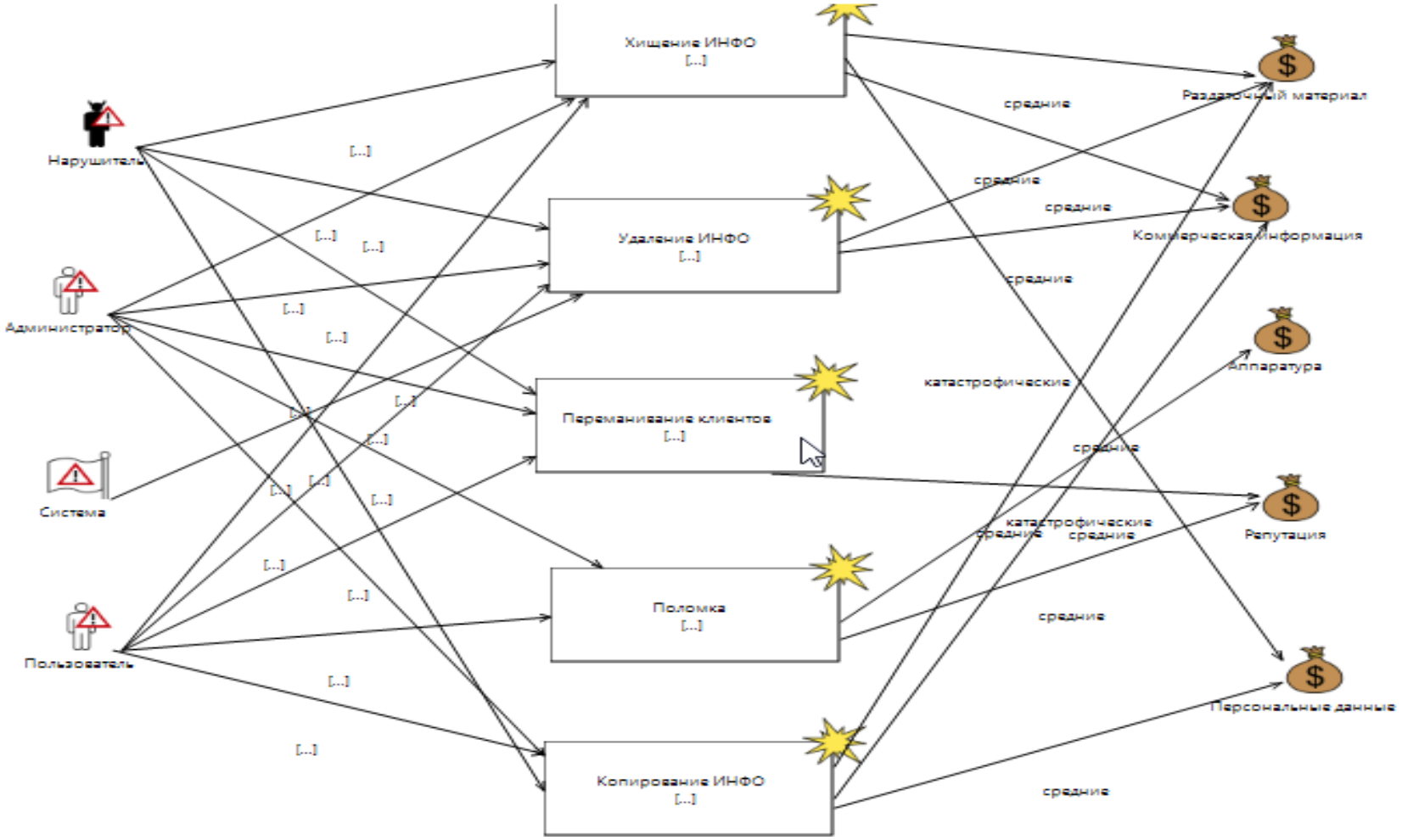

Рисунок 55 – Диаграмма рисков с характеристикой последствий осуществления угрозы

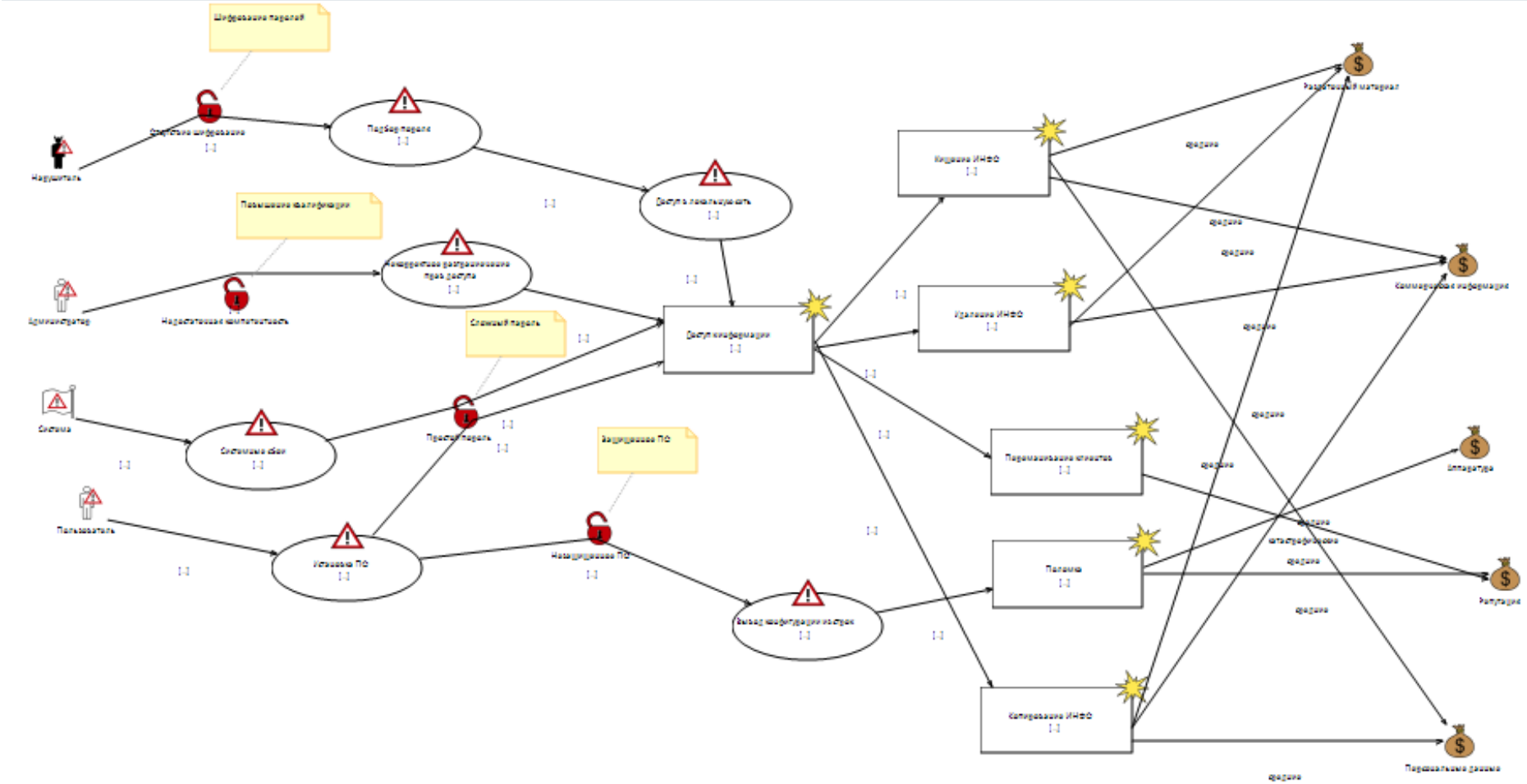

Рисунок 56 – Диаграмма угроз после добавления противодействий

Вывод: по итогам данной главы были проведены расчеты оценки рисков по двум параметрам, которые включает в себя три этапа, Первый этап - первоначальный расчет рисков возникающих в электронной почте . Второй этап - определение мер для неприемлемых рисков . Третий этап повторный расчет рисков. Были рассмотрены основные угрозы и уязвимости выбранных активов. После было выявлено высокий уровень рисков, в связи с этим приняли решение об использовании защитных мер. По итогам был произведен перерасчет рисков.

В результате первичной оценки среднее значение уровня рисков было 6, при проведении переоценки с применением защитных мер значение уровня рисков снизилось в 2 раза и стали приемлемыми для активов.

На второй части был произведен анализ рисков с помощью программы CORAS и были построены UML диаграммы, начиная с идентификации активов рисков, модели угроз и уязвимостей, заканчивая внедрением противодействий .

Заключение

Вопросы обеспечения эффективной защиты объектов, рассматриваемые в данной дипломной работе, способствуют формированию базовой (фундаментальной) теоретической и практической подготовки в области интегрированных систем безопасности. Изучение основных терминов, определений и принципов организации интегрированных комплексных систем безопасности позволяет решить следующие задачи проектирования и анализа функционирования интегрированных систем безопасности:

- выбор варианта защиты объекта с использованием комплекса технических средств защиты в соответствии с требованиями технической безопасности объекта;
- реализация основных этапов проектирования интегрированных систем безопасности с использованием основных принципов разработанной концепции безопасности;
- разработка структурной схемы интегрированной комплексной системы безопасности на основе данных о ее системах контроля доступа, пожарной сигнализации и телевизионной безопасности;
- синтез отдельных компонентов интегрированных систем безопасности на основе готовых унифицированных функциональных блоков, расчет их основных параметров и характеристик;
- выполнение оптимизации структуры интегрированной системы безопасности с использованием методов оценки эффективности ее функционирования.

Выполнение этих задач развивает способность собирать, обрабатывать, анализировать и систематизировать научно-техническую информацию, выбирать перспективные методы решения профессиональных задач на основе современного развития оптико-электронных и телевизионных систем безопасности.

Коллективное решение задач проектирования оптоэлектронных устройств и систем безопасности предполагает активное приобретение навыков правильной формулировки основных требований к параметрам элементов оптоэлектронных систем безопасности, их сборки, наладки, контроля и испытаний, а также безопасности. Система в целом, основанная на анализе требований клиентов и обследовании объектов.

Список литературы

1 В. Олифер, Н. Олифер "Компьютерные сети. Принципы, технологии, протоколы.

2 Уильям Станек "Microsoft Windows Server 2012. Справочник администратора.

3 Крейг Хант, "TCP/IP — Сетевое администрирование.

4 Международный стандарт ISO 27001:2013 «Информационные технологии – Методы защиты - Системы менеджмента информационной безопасности – Требования».

5 Международный стандарт ISO 27002:2013 Информационные технологии - Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью.

6 Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. - Москва: Наука, 2018. - 532 с.

7 Бабаш А. В. Информационная безопасность (+ CD-ROM) / А.В. Бабаш Е.К., Баранова Ю.Н., Мельников. - М.: КноРус, 2019. - 136 с.

8 Васильков А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2020. - 368 с.

9 Гафнер В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2019. - 336 с.

10 Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2019. - 240 с.

11 Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2019. - 176 с.

12 Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников , 2019. - 536 с.

13 Международный стандарт ISO 27001:2013 «Информационные технологии – Методы защиты - Системы менеджмента информационной безопасности – Требования».

14 Международный стандарт ISO 27002:2013 Информационные технологии - Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью.