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 | старший преподаватель Дмитриева Маргарита | 17.02.2020 – 09.05.2020 | |

| | | | |
|---|---|---|---|
| безопасности | Валерьевна | | |
| 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 ,<br>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 | |

Дата выдачи задания «7»_____ноября_____2019г.

Заведующий кафедрой _____ (Бердибаев Рат Шындалиевич)
(подпись) (ФИО)

Научный руководитель проекта _____ (Шайкулова Актоты Алиевна)
(подпись) (ФИО)

Задание принял к исполнению студент _____ (Аканов Тимур Ерикович)
(подпись) (ФИО)

## Аннотация

В дипломном проекте была создана виртуальная корпоративной сеть, с для передачи электронной почты. Показан практический способ реализации информационной безопасности при помощи настройки виртуального маршрутизатора PFSENSE. Была использована виртуальная машина VmWarePRo , для настройки Windows server 2012 , созданы две операционной системы Windows 7 для передачи писем клиентам.

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. Windows серверін 2012 конфигурациялау үшін VmWarePRo виртуалды машинасы қолданылды, клиенттерге хат жіберу үшін екі Windows 7 операциялық жүйесі құрылды.

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. A VmWarePRo virtual machine was used to configure Windows server 2012, two Windows 7 operating systems were created for sending letters to clients.

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

Корпоративная почта имеет много угроз, создают серьезные риски, связанные с ее использованием. Например, недоступность корпоративной почты, когда пользователи начинают использовать корпоративную почту для отправки спама, простота использования могут привести к утечке информации, распространению вируса, отправке документов и так далее.

Таким образом, достоинство корпоративной почты оказалось под угрозой, так как корпоративная почта содержит различные «риски» приложения, в том числе вирусы, вредоносные программы, трояны и т. д. стал удобным инструментом для распространения.

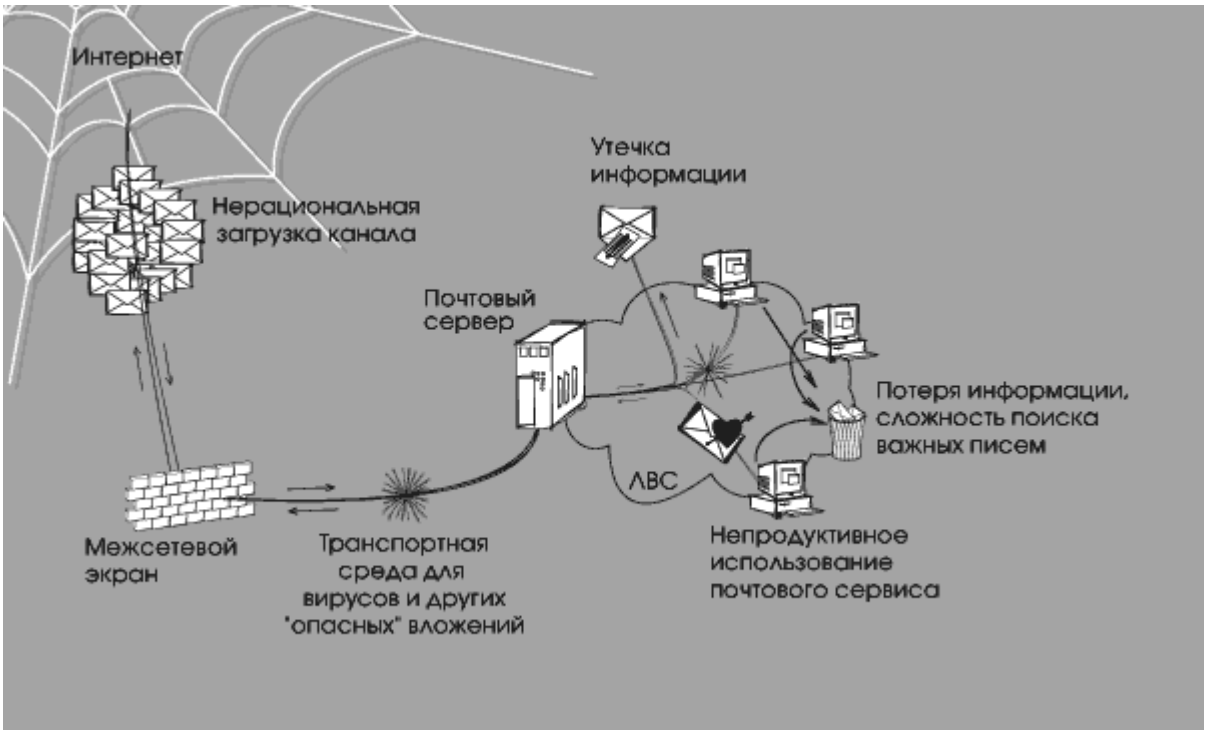



Рисунок 1- Влияние различных факторов на почтовую систему

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.

Спам ведет к блокировке спам-трафика. Как правило, это включает в себя различные услуги, товары и так далее. письма, содержащие

повторяющиеся письма. Такие корпоративные письма включает к «группе риска» по распространению вируса. Большое количество нежелательнных почты загружает каналы, «нежелательные», для удаления нежелательной писем требуется время, и вы с вероятностью случайно не уведете нужные сообщения.

Например реклама, не предназначено для закрытия почтовой системы организации, но приводит к негативным последствиям. Использование списков список рассылки, включающий всех пользователей одной и той же сети и прием рекламных сообщений для этих пользователей, и угрожает организации снижением производительности ее сетевого оборудования.

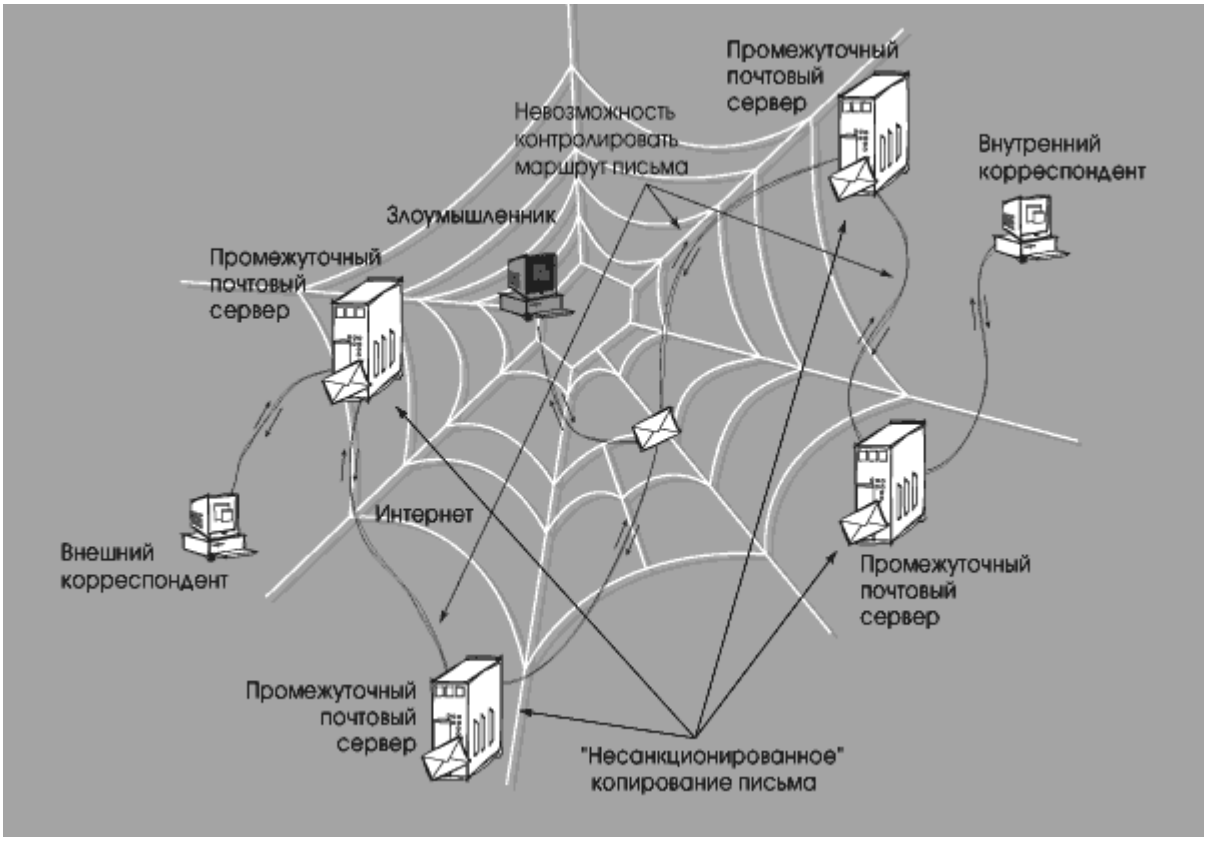



Рисунок 2 - Проблемы, связанные с отправкой электронной почты

Все функции, и простота копирования корпоративной почты и невозможность контролировать это действие позволяют сотруднику предоставлять корпоративную информацию третьим лицам, как внутри, так и за ее пределами компании.

Такая информация о компании (письма, соглашений, о планируемых транзакциях компании и т. д.). Пароли, оборудования данных, 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 .

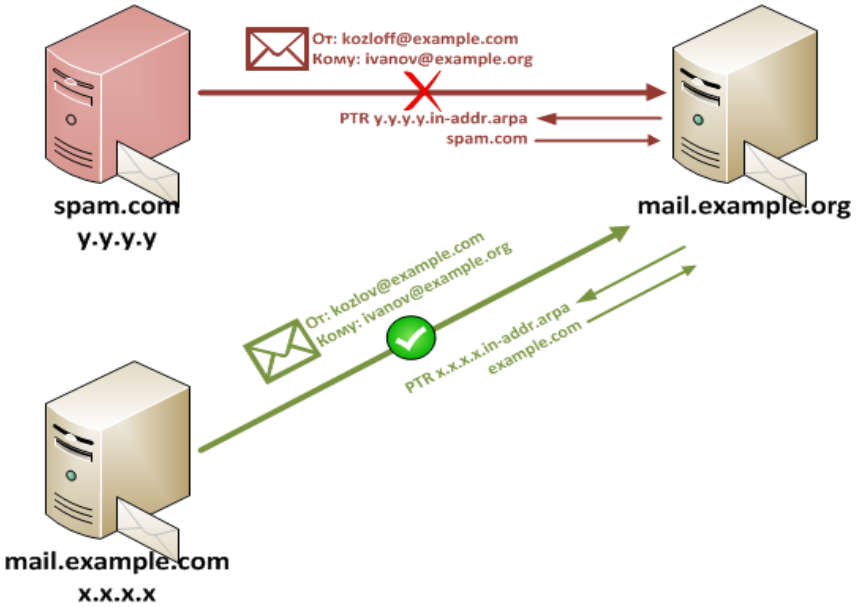



Рисунок 3 - Allow spam server

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).

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.

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.

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.

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 Электронная почта - протоколы SMTP, POP3, IMAP4

Корпоративная почта является информационных ресурсов, одним из популярных средств 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 ip-адресам;
- отправлять письма сразу двум получателям;
- отправить полученное письмо на другой ip-адрес;
- используйте имена вместо адресов ;
- 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.

Протокол POP3 – это почтовый протокой для использование приема электронной почты с удаленного сервера на локальный компьютер и использовать для собрание писем на ваш ПК и читать их. При использование протокола POP3 после подключение к вашей учетной записи сообщение загружается локально и удаляется с сервера электронной почты.

Протокол IMAP – это протокол получение писем электронной почты, используется для доступа к ней на удаленный web-сервере от локального ПК. IMAP работает на двух портах:

- port 143 – это незашифрованный порт по умолчанию;
- port 993 – его используют для безопасности подключение.

Протокол SMTP – это протокол отправки электронной почты через интернет. SMTP работает на трех портах:

- port 25 – это незашифрованный port;
- port 2525 – он открыт на всех серверах, если порт 25 фильтруется вы отправите не зашифрованное письмо с помощью SMTP;
- port 465 – его используют для безопасной передачи письма.

## 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.

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

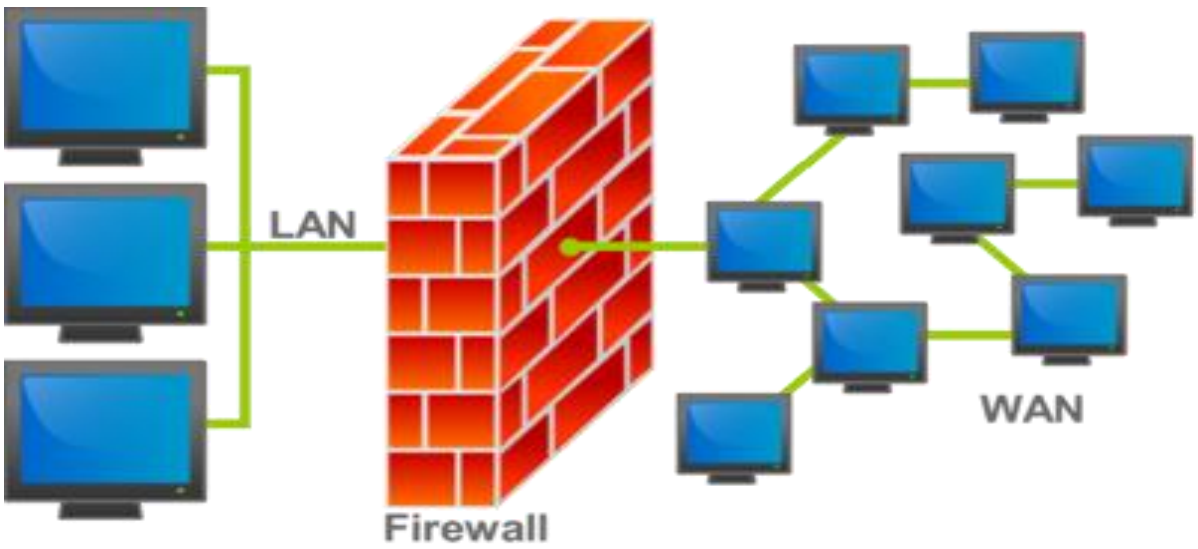



Рисунок 4 - Firewall сетевого периметра

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 - это протокол управления передачей;

IP- это межсетевой протокол.

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

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.

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.

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 5 – Производительность firewall D-Link NetDefend


Рисунок 6 - Обзор производительности DFL-260E и DFL-860E


Рисунок 7 - Обзор производительности 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.

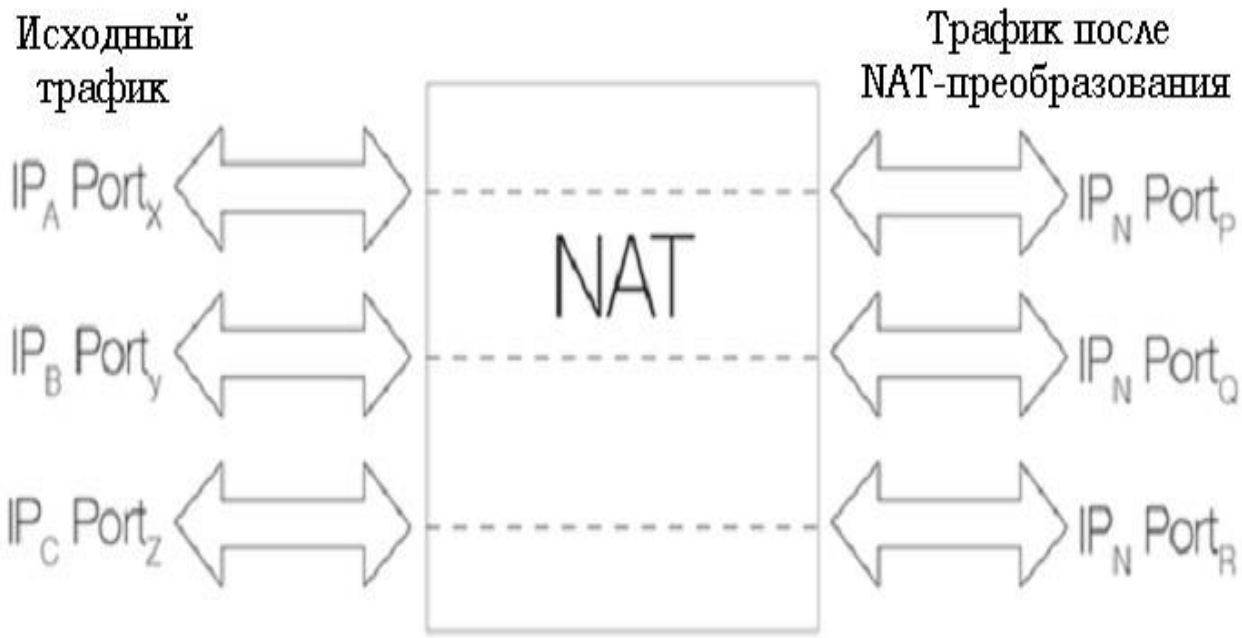



Рисунок 8 - Диаграмма NAT

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.

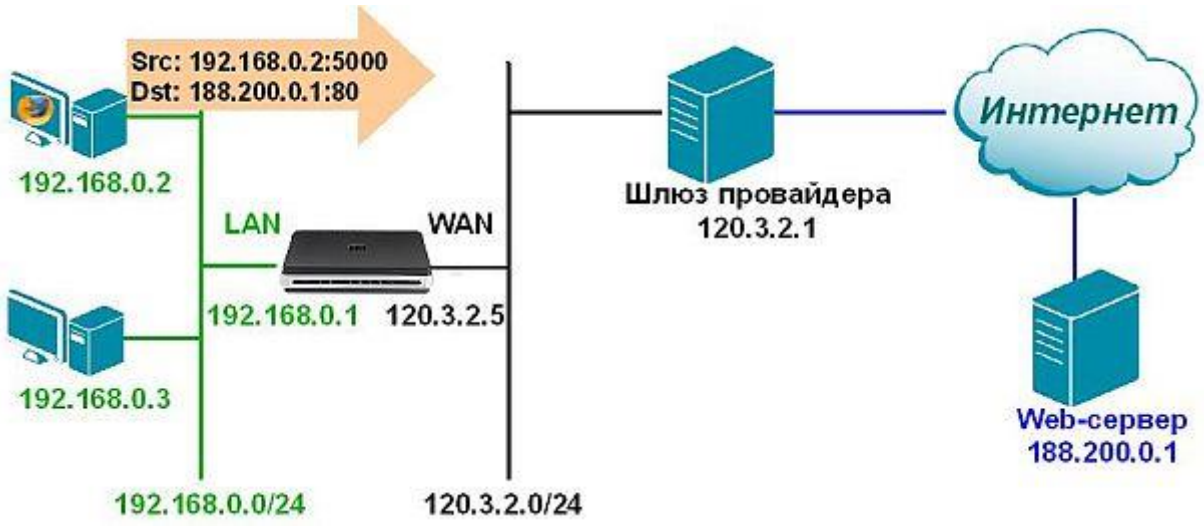



Рисунок 9 - Запись в таблице соединений

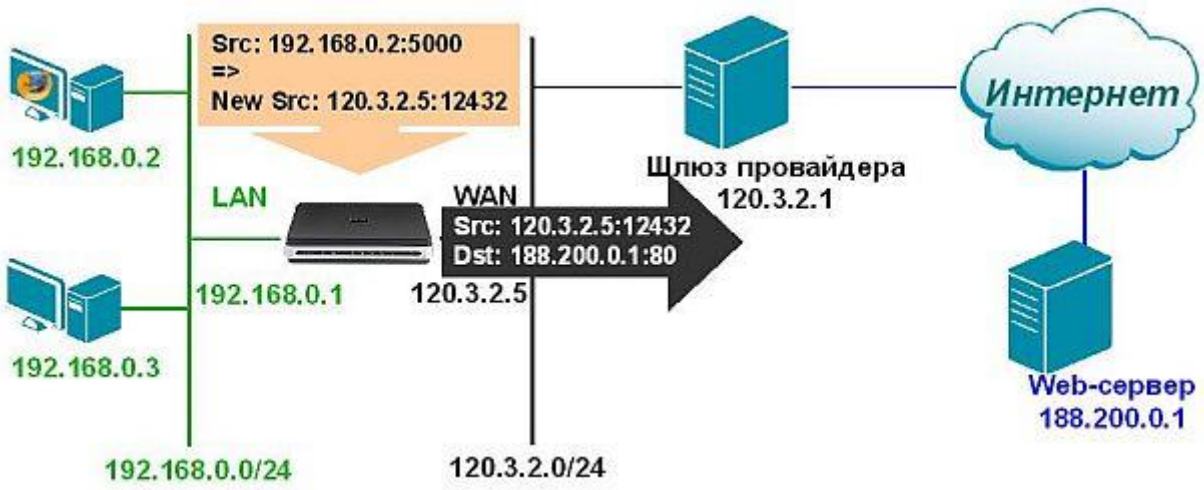



Рисунок 10 - Преобразование адресов при использовании функции NAT

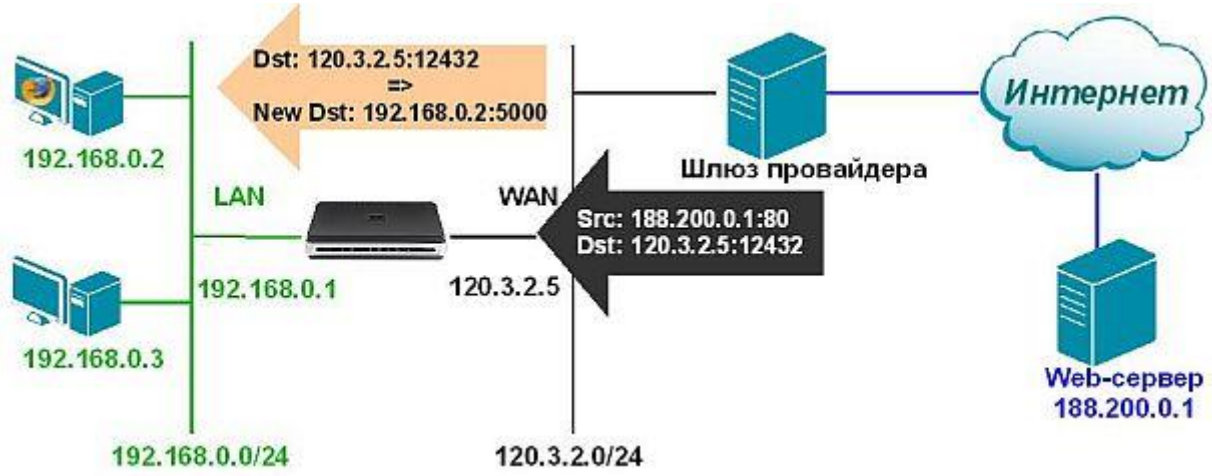



Рисунок 11 - Преобразование адресов при использовании функции NAT

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.

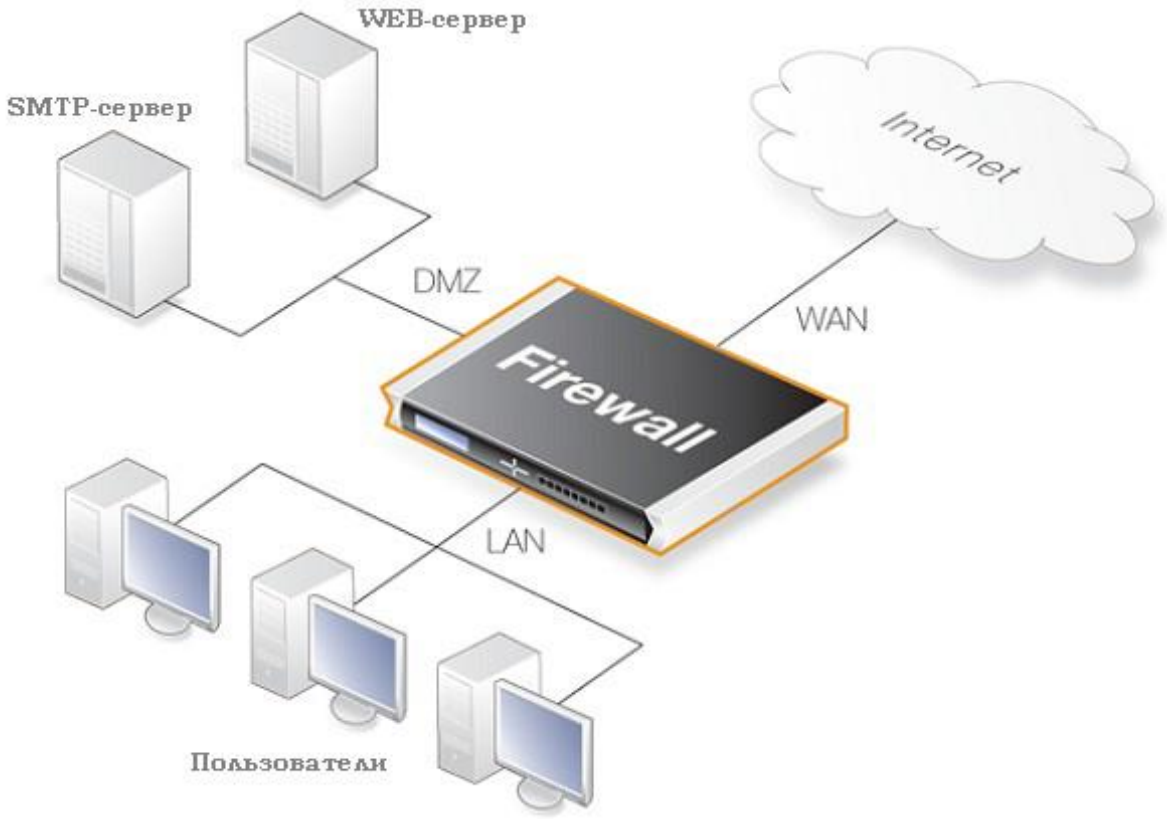



Рисунок 12 - Схема серверами в зоне DMZ

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).

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.

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

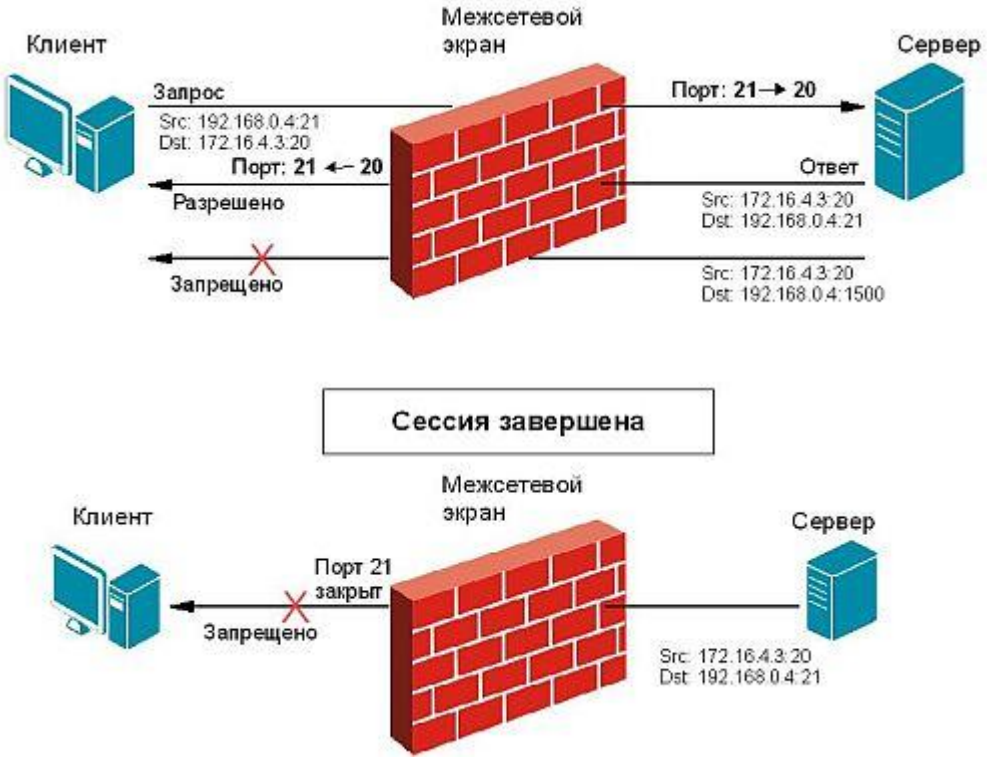



Рисунок 13 - Пример механизма Stateful Inspection с FTP-протоколом

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.

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.

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.

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

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 и реализация защиты от спама

### 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 2012. DNS используется роль домен служб AD.

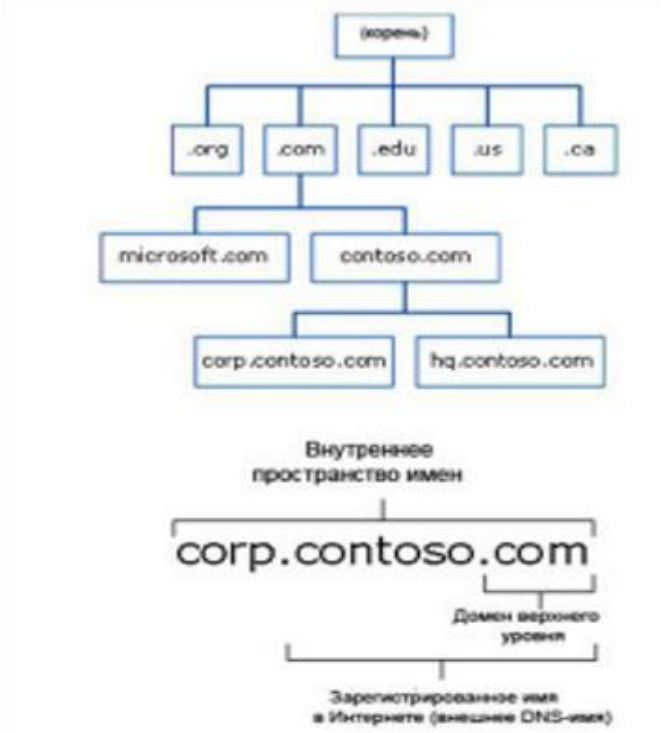



Рисунок 14 – Организация имен DNS

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.

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.

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

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.

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.

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.

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.

3. Сервер (NS) записей. Указывает, какие пк в данных DNS имеют серверы имен, то есть DNS-серверы для определенной диапазона. Одна запись 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.

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 компьютеров ? » 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.

Перейдите в раздел Добавить роли и компоненты.

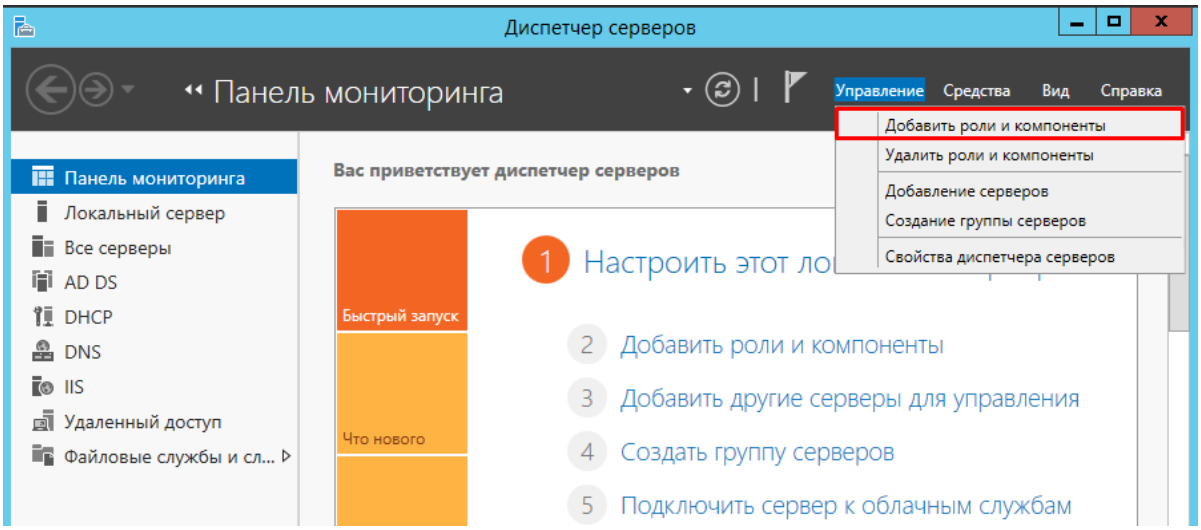



Рисунок 15 - Панель мониторинга

На странице Мастер добавление ролей и компонентов щелкните на кнопке Далее.

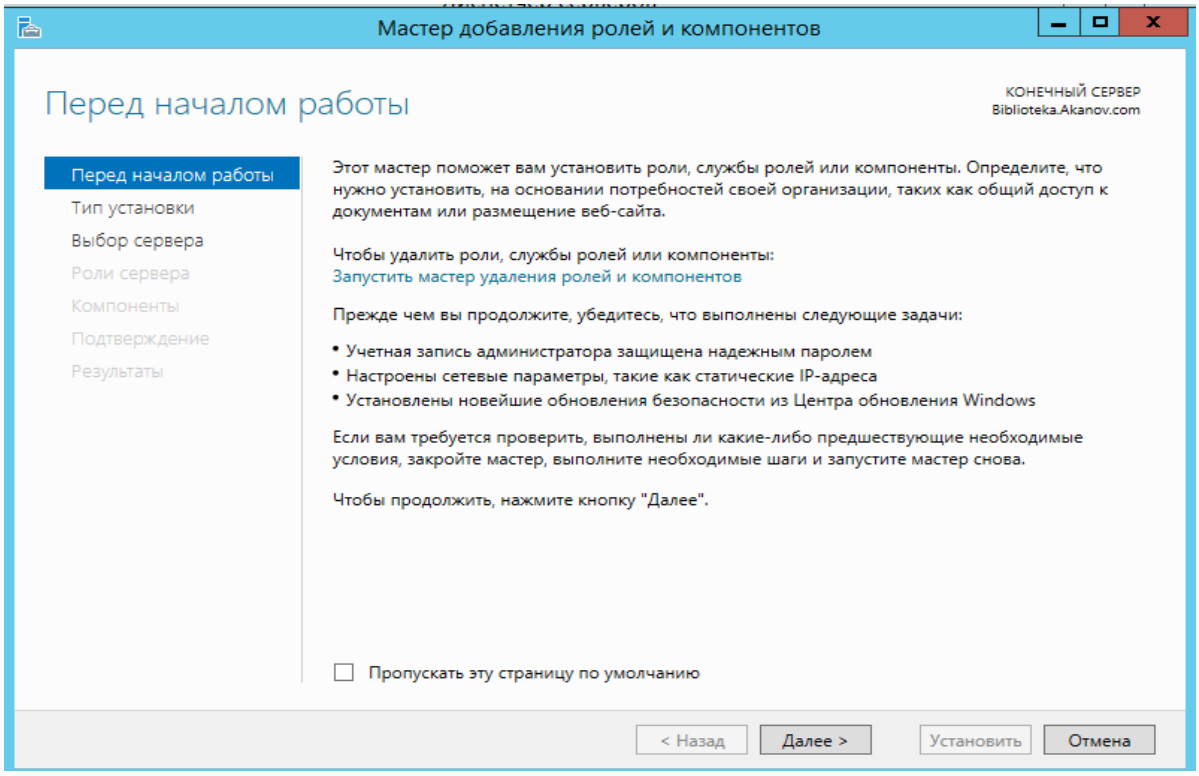



Рисунок 16 - Роли и компоненты DNS

Выберите вариант Установка на основе роли или компонента и щелкните на кнопке Далее.

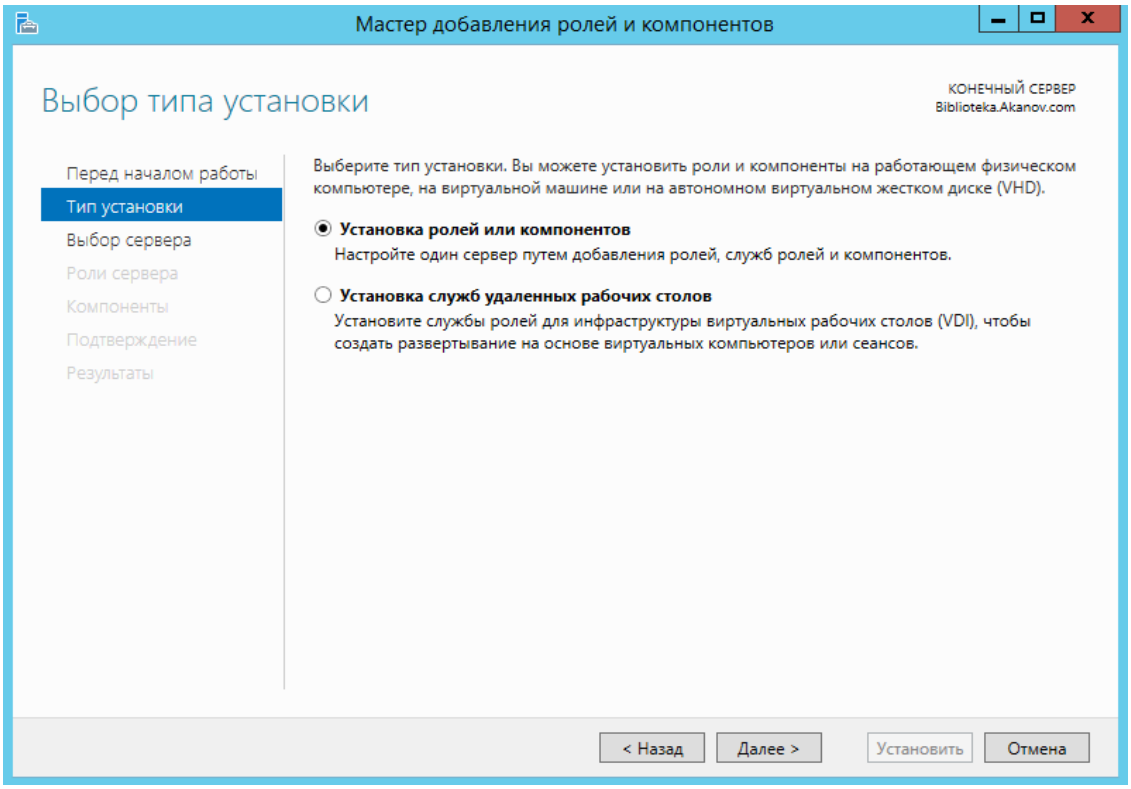



Рисунок 17 – Мастер выбора типа установки компонентов

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

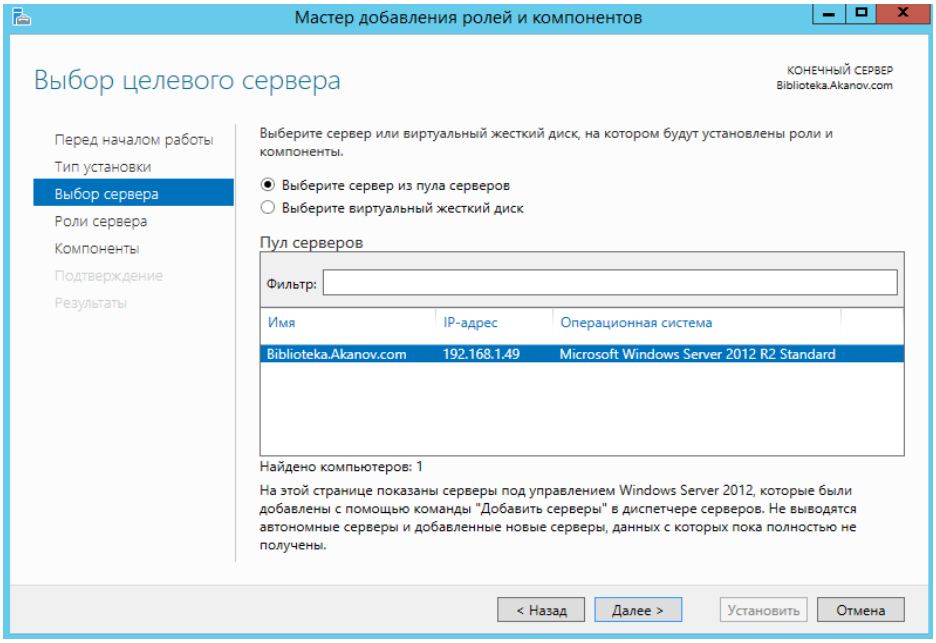



Рисунок 18 - Мастер добавления ролей и компонентов (выбор целевого сервера)

Выберите имя сервера, на котором нужно выполнить настройки DNS. В меню выберите пункт настройка DNS сервера.

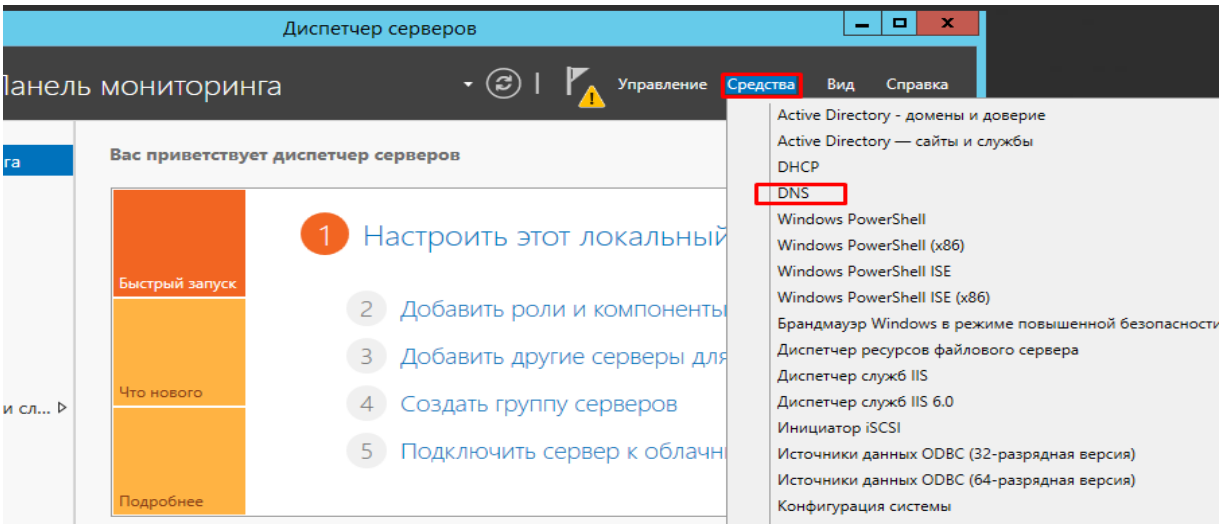



Рисунок 19 - Вход в диспетчер DNS

Зоны прямого просмотра.

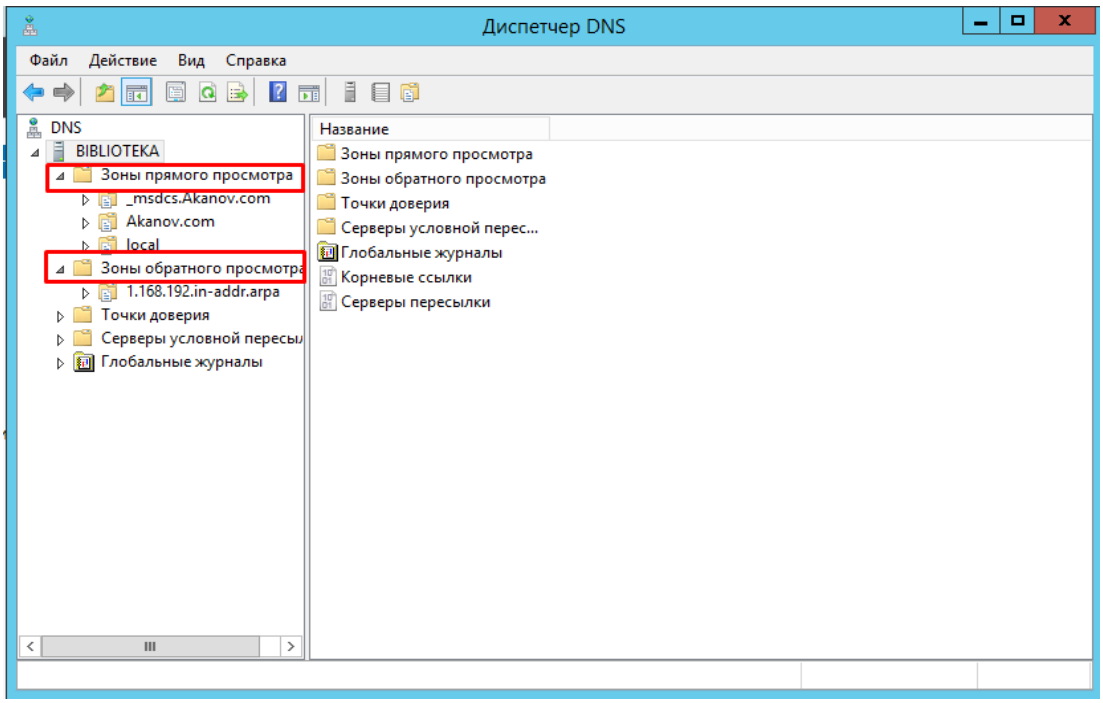



Рисунок 20 - Диспетчер DNS

Зоны обратного просмотра.

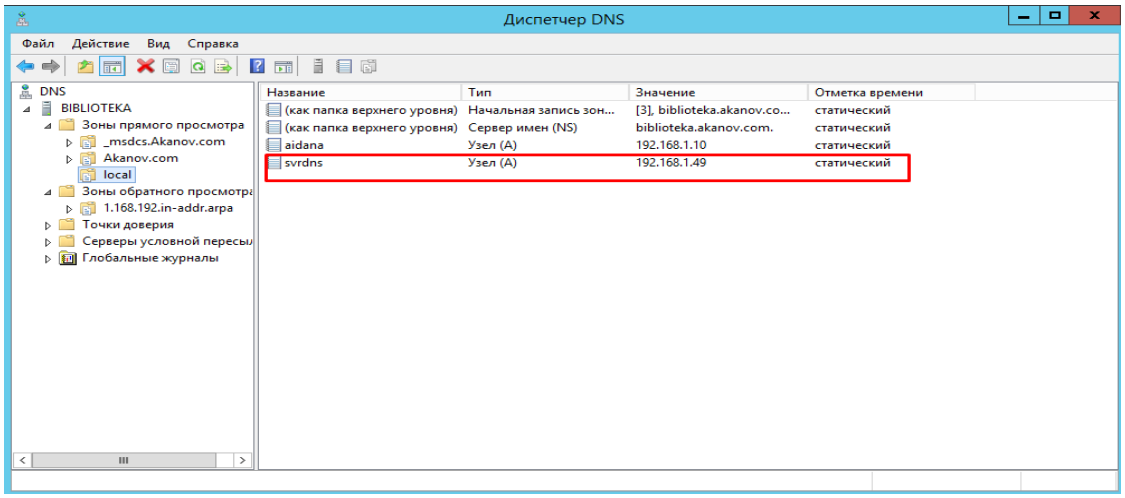



Рисунок 21 - Диспетчер DNS

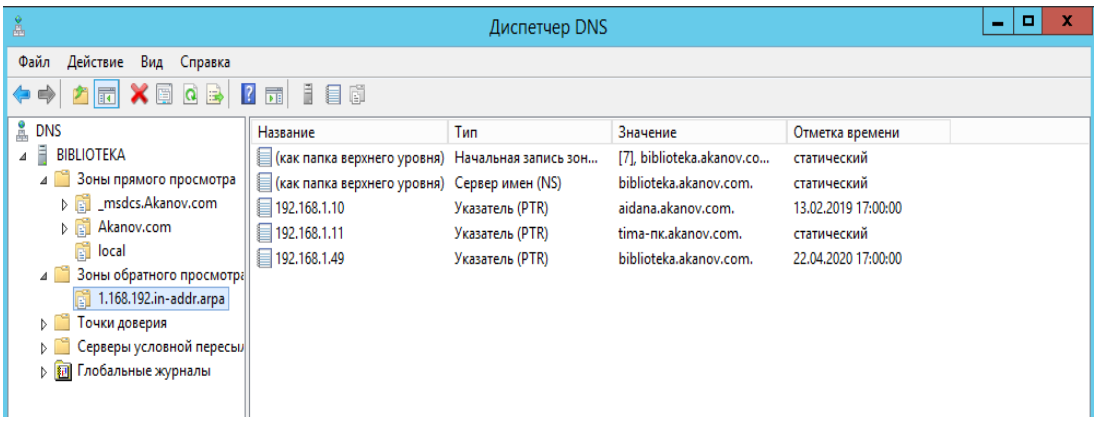



Рисунок 22 - Диспетчер DNS

Зоны прямого просмотра.

Настройка DHCP сервера на Windows server 2012 для определение зоны пола адресов.

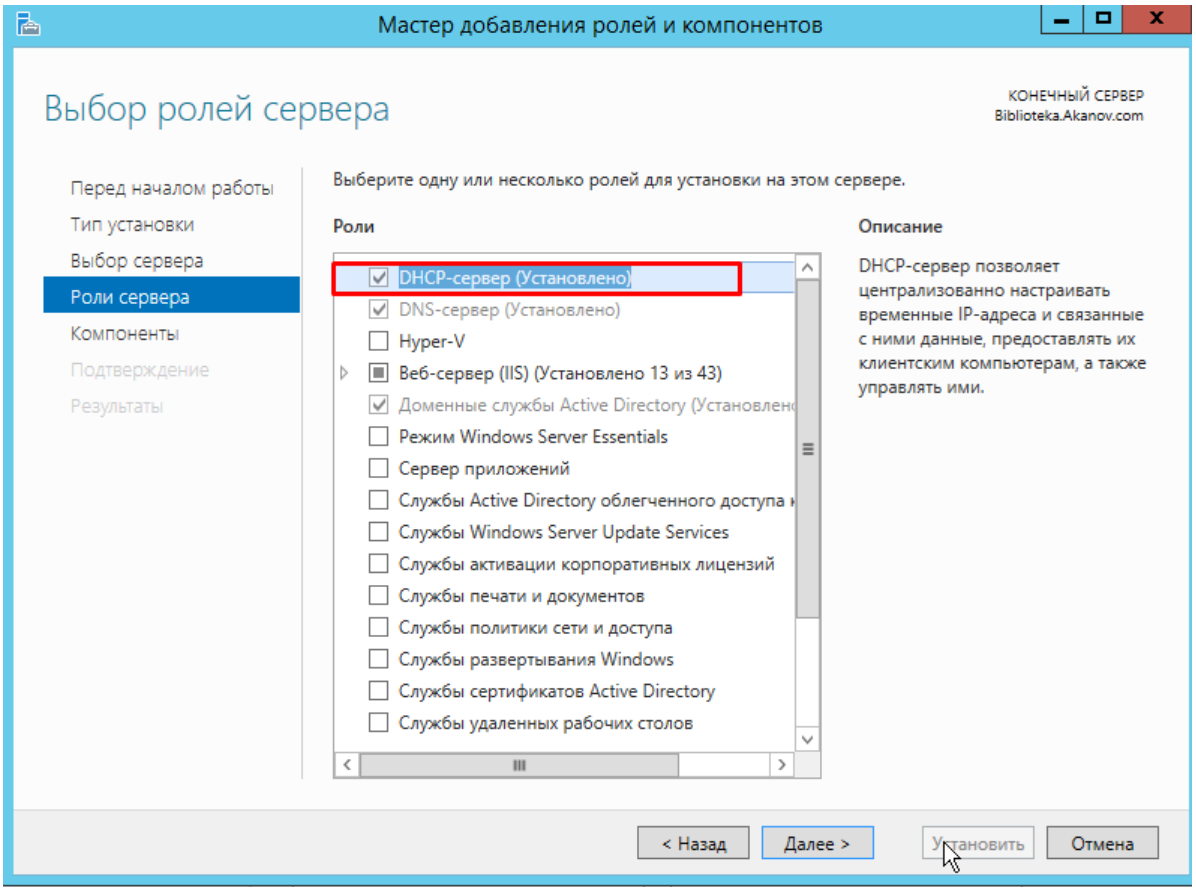



Рисунок 23 - Мастер добавления ролей и компонентов (выбор ролей сервера)

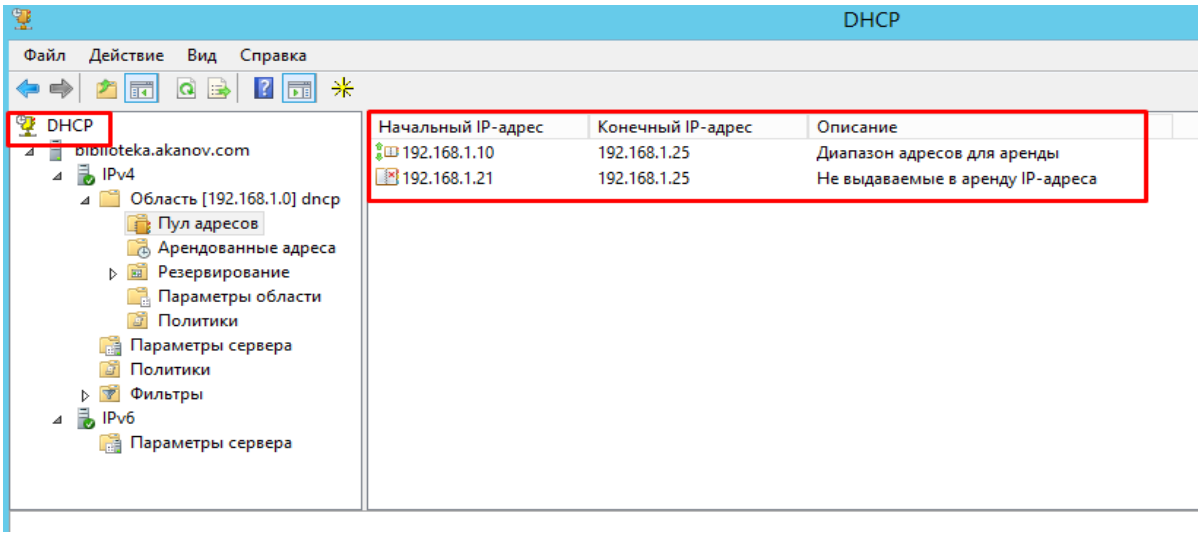



Рисунок 24 - Диспетчер DHCP

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

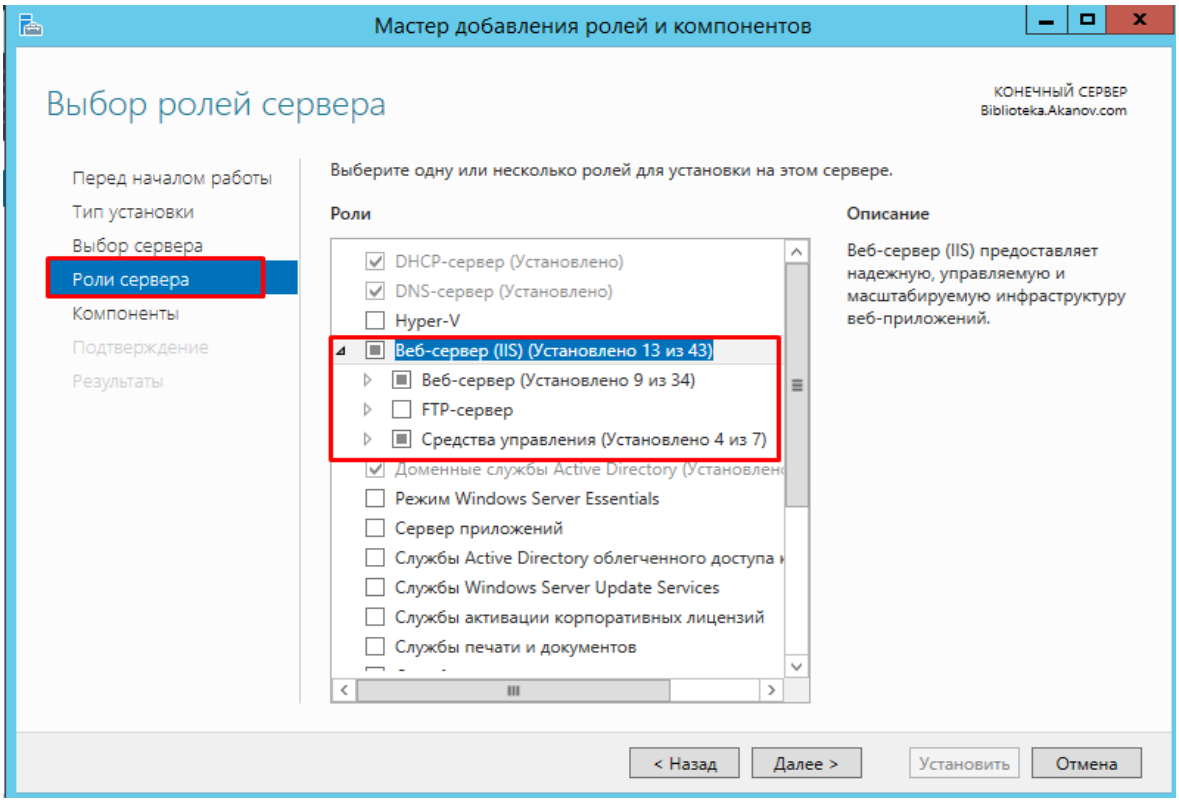



Рисунок 25 – Мастер ролей и компонентов DHCP

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

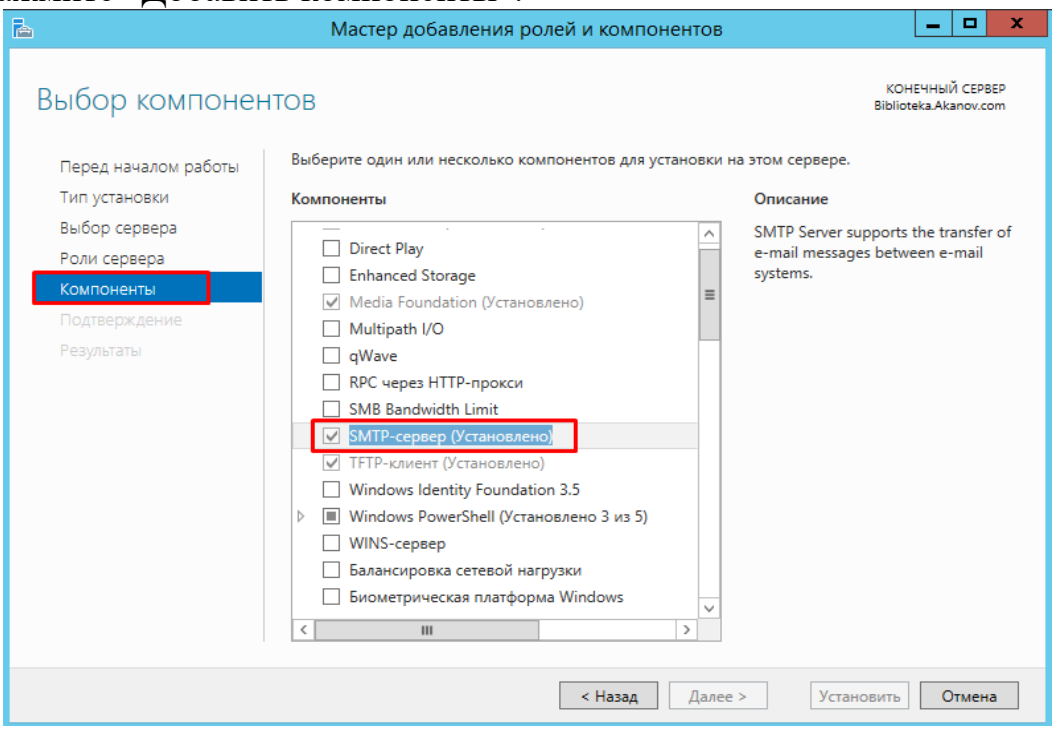



Рисунок 26 - Добавления ролей SMTP server

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”.

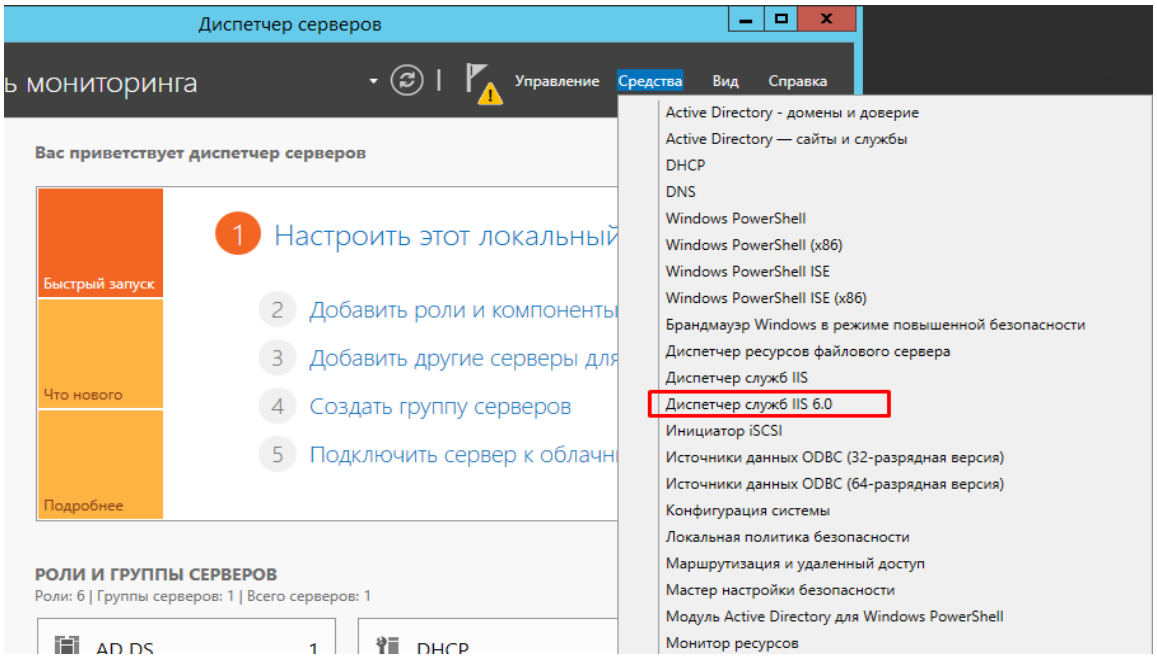



Рисунок 27 - Диспетчер служб IIS 6.0

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

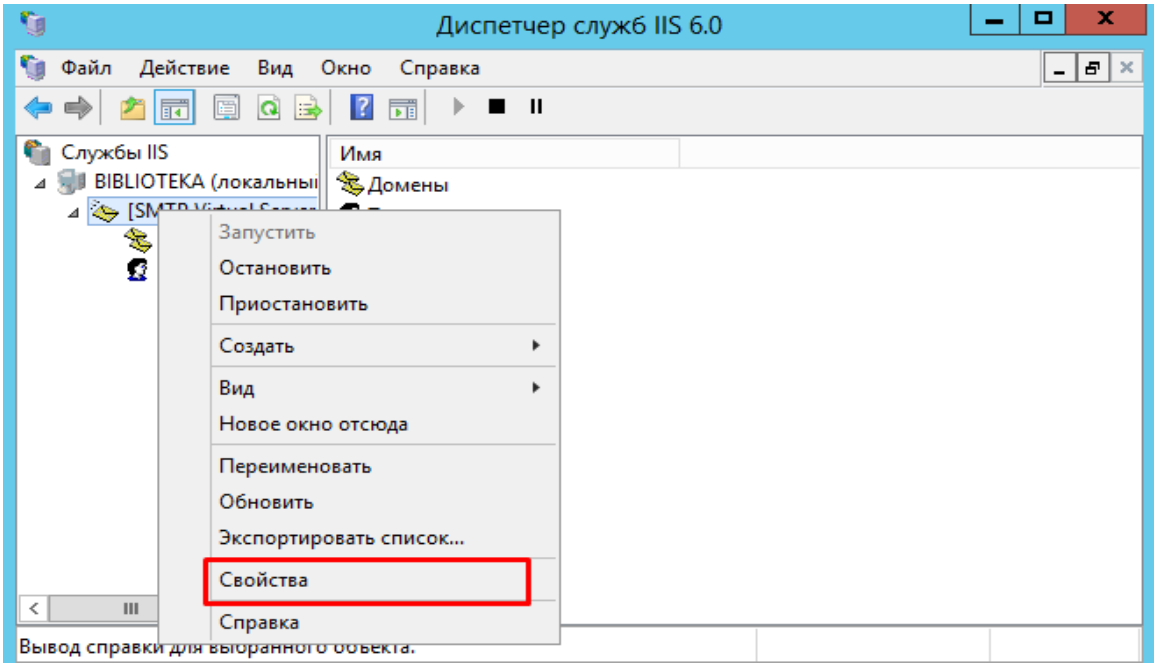



Рисунок 28 - Свойства служб IIS 6.0

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

.

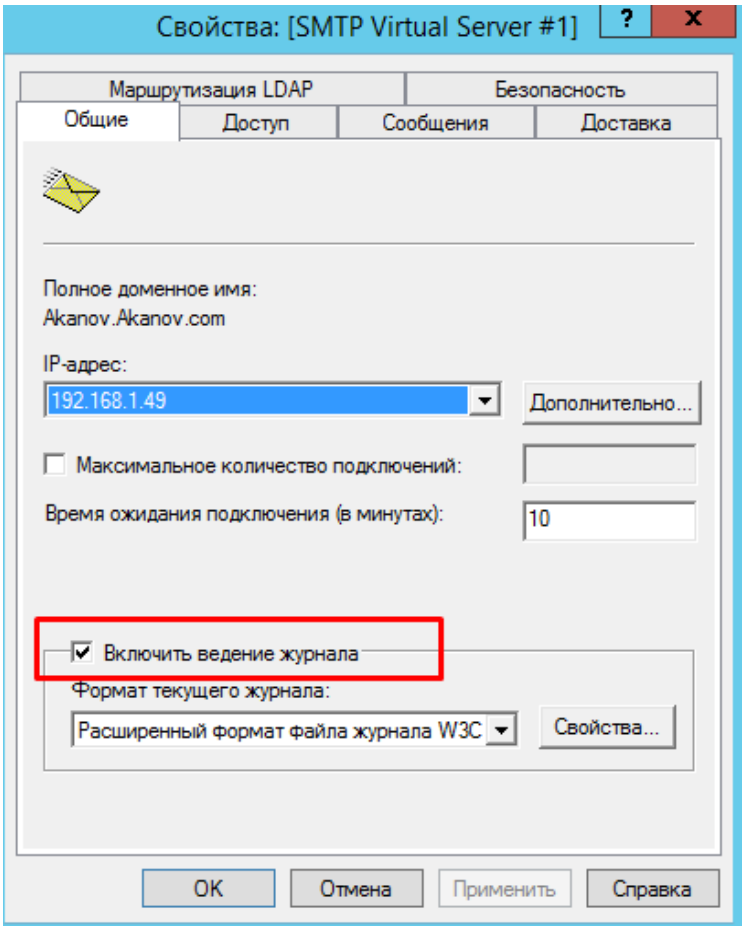



Рисунок 29 - Свойства SMTP Virtual server

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.

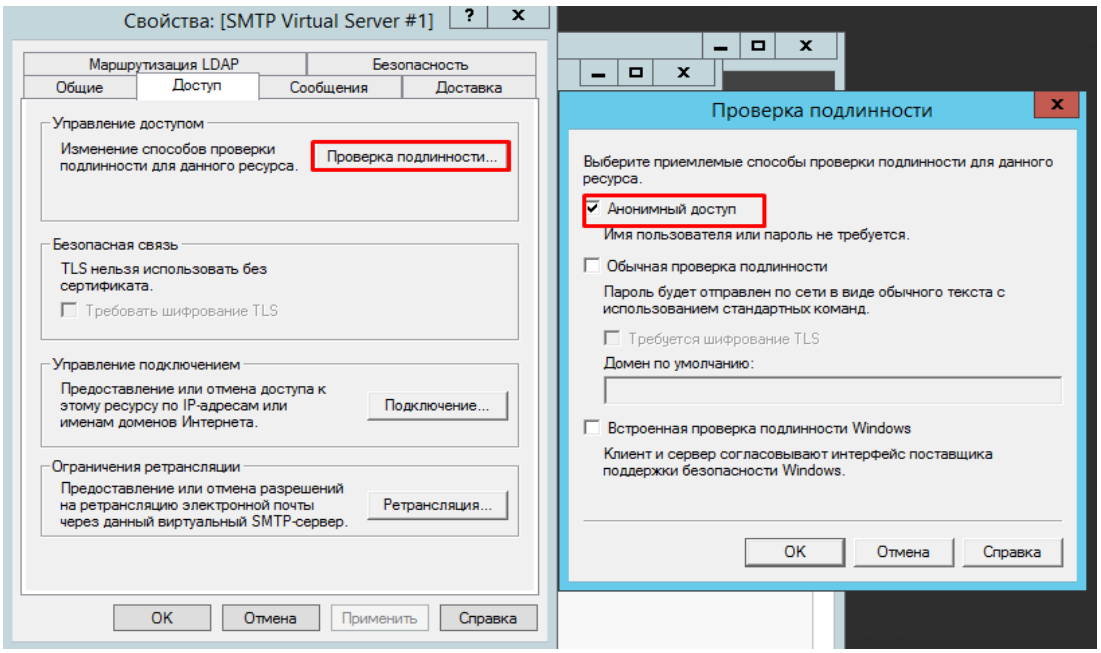



Рисунок 30 - Свойства SMTP Virtual server анонимный доступ

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”.

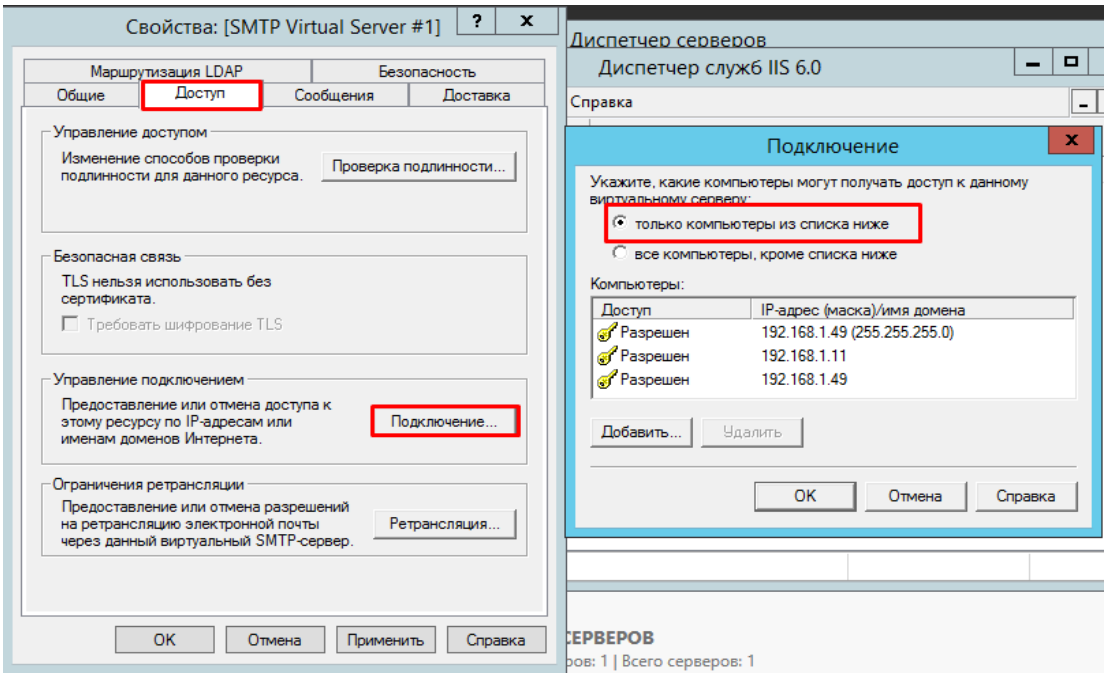



Рисунок 31 - Свойства SMTP Virtual server подключение ip-адреса

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

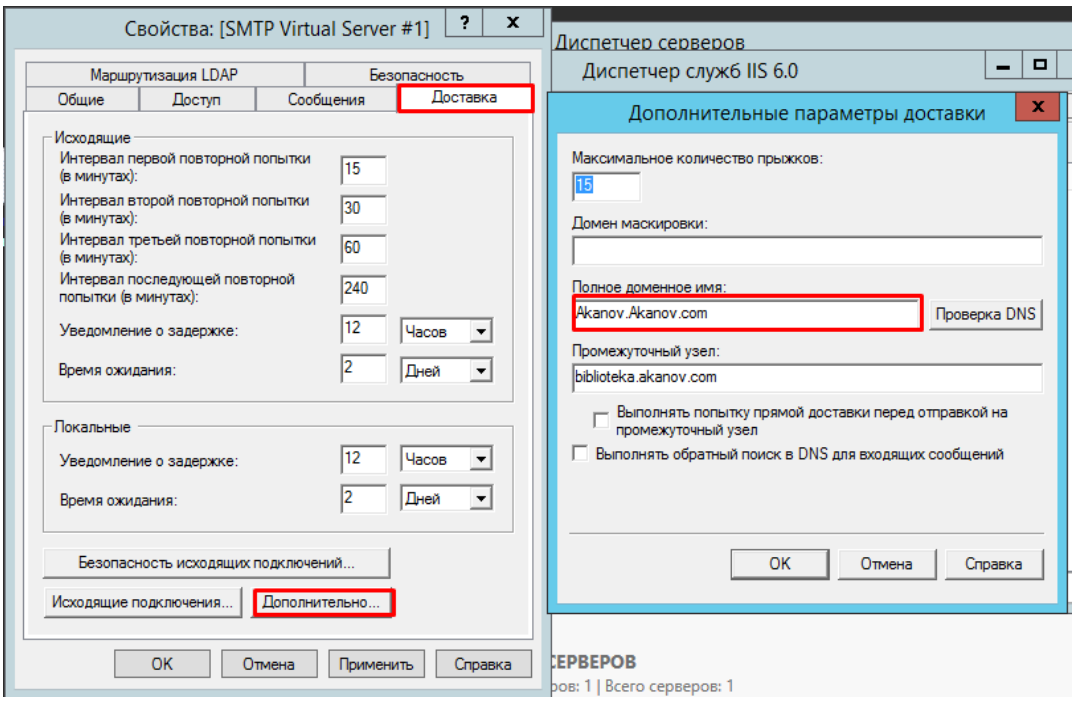



Рисунок 32 - Свойства SMTP Virtual server дополнительные параметры

При проверке DNS имя домена должно быть допустимым.

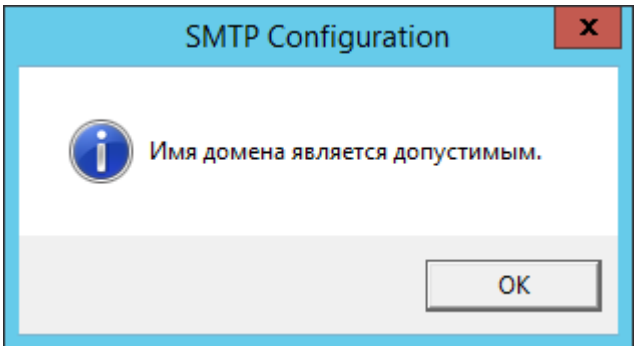



Рисунок 33 - Проверка DNS имени

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.

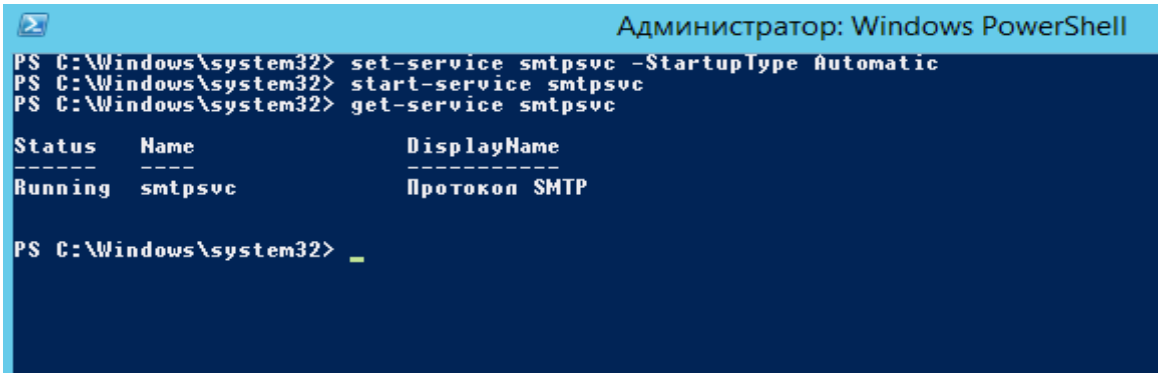



Рисунок 34 - Консоль PowerShell

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.

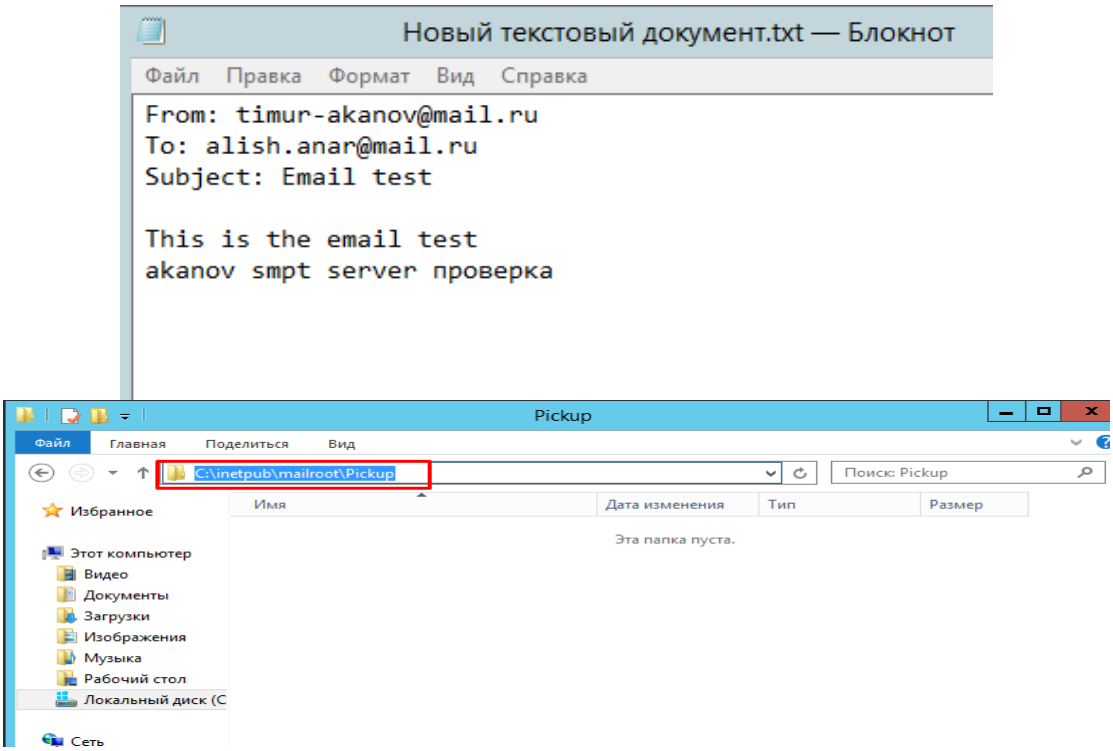



Рисунок 35 - Отправка почти через SMTP server

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

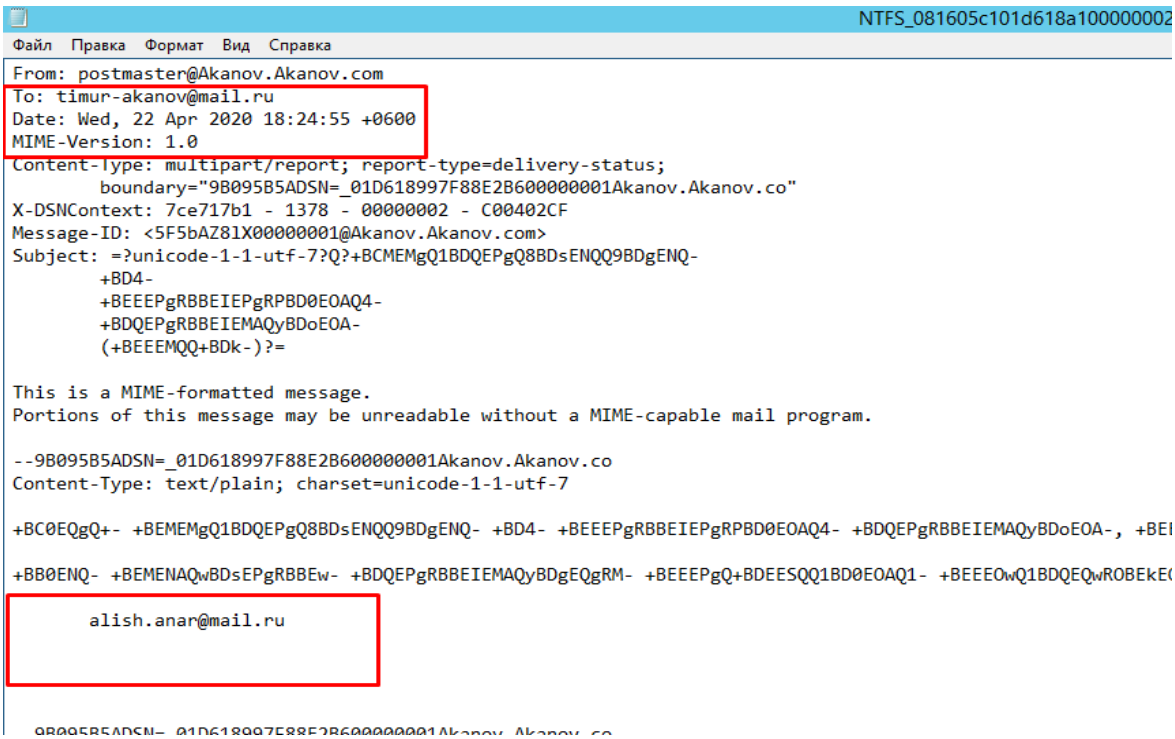



Рисунок 36 - Проверка подлинности отправки почты

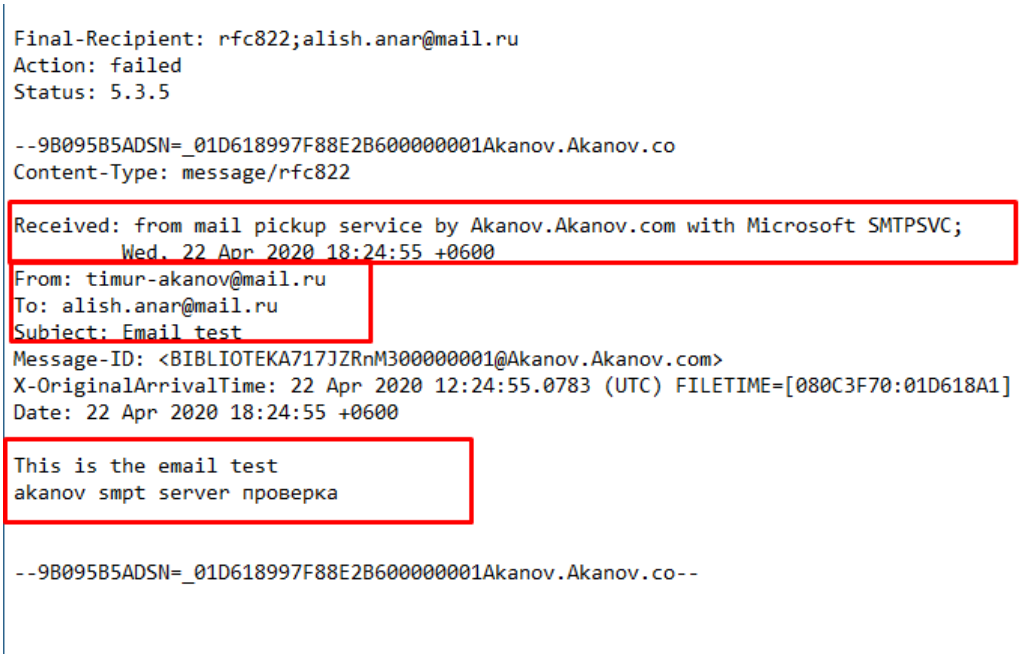



Рисунок 37 - Файл отправителя и получателя

### 3.2 Защита от DoS-атак при помощи маршрутизатора PFSENSE

Pfsense – это межсетевой экран для дистрибутива основанный на FreeBSD предназначен для пк . Настроить можно при помощью web-интерфейса, что позволяет облегчить пользование без глубоких знаний в сетевом оборудование. Pfsense используется как брандмауэр, маршрутизатор.

После установки и назначения на консоли появляется меню оболочки с рядом опций. Теперь pfSense готов к доступу через сеть, либо через интерфейс

LAN (если он назначен), либо через интерфейс WAN в одном развертывании интерфейса.

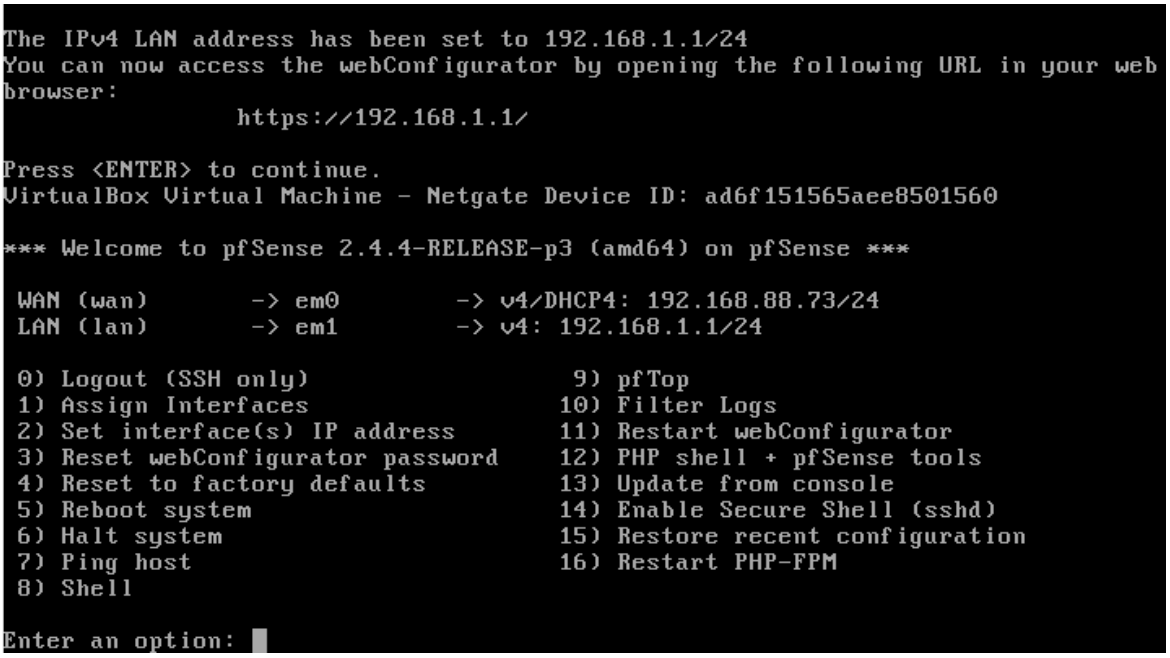



Рисунок 38 – Консоль pfsense

Далее переходим в web-интерфейс Pfsense и видим полный конфигурационный файл системы виртуальной машины.

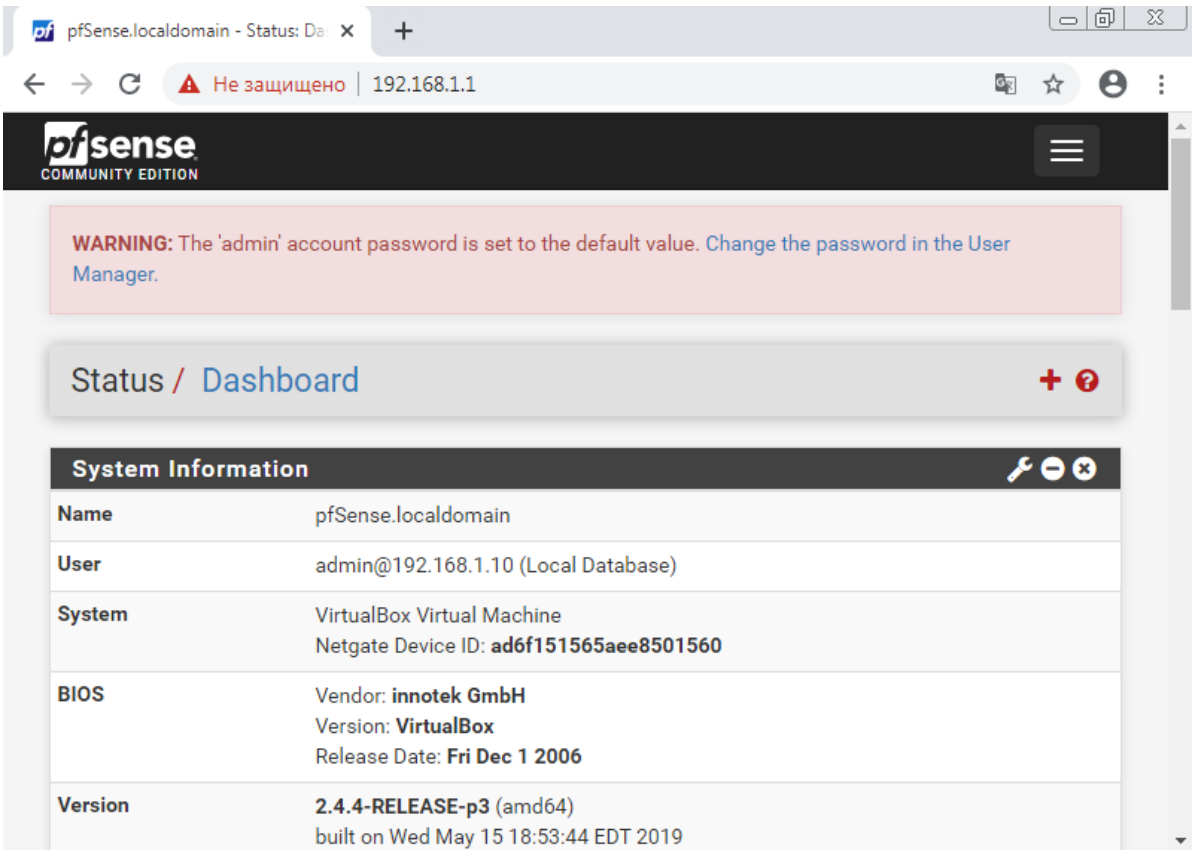



Рисунок 39 – web-интерфейс Pfsense

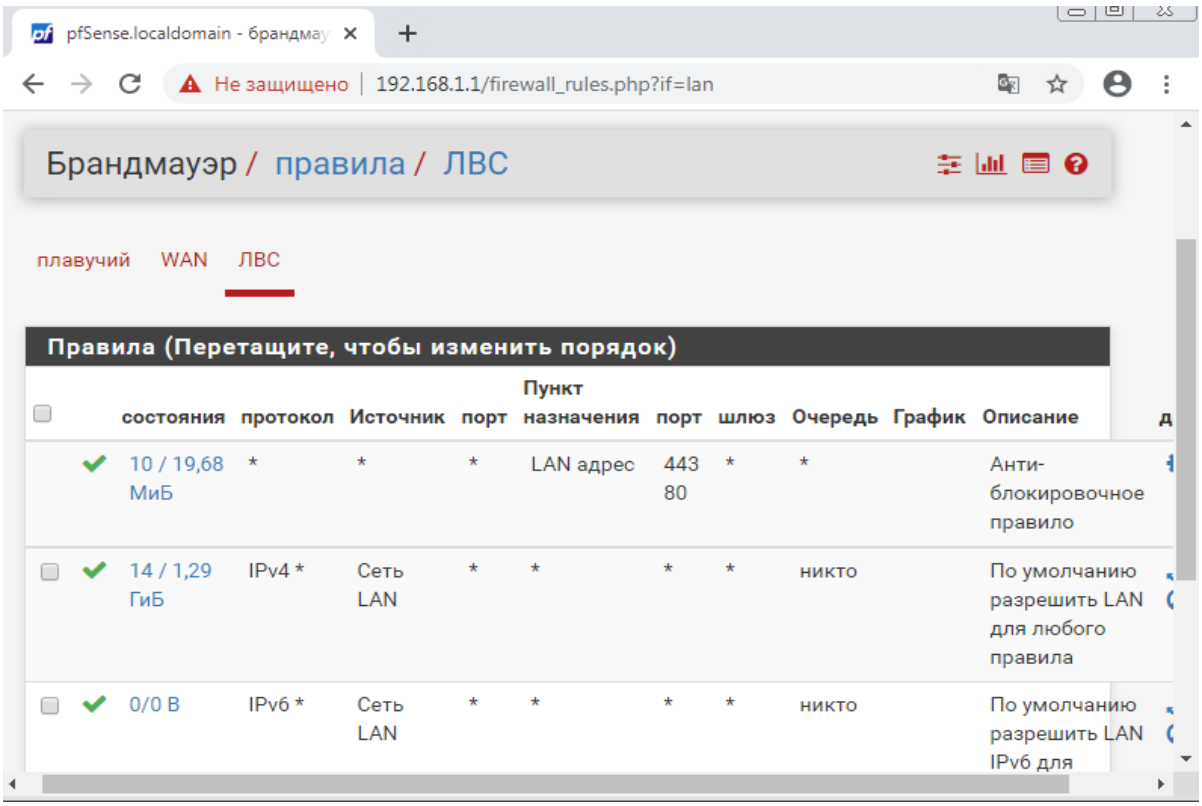



Рисунок 40 – Web-интерфейс firewall

После просмотра всех настроек, далее настраиваем block private networks and lookback addresses. Это настройка нужна для понимая сервера в каком диапазоне ip-address.

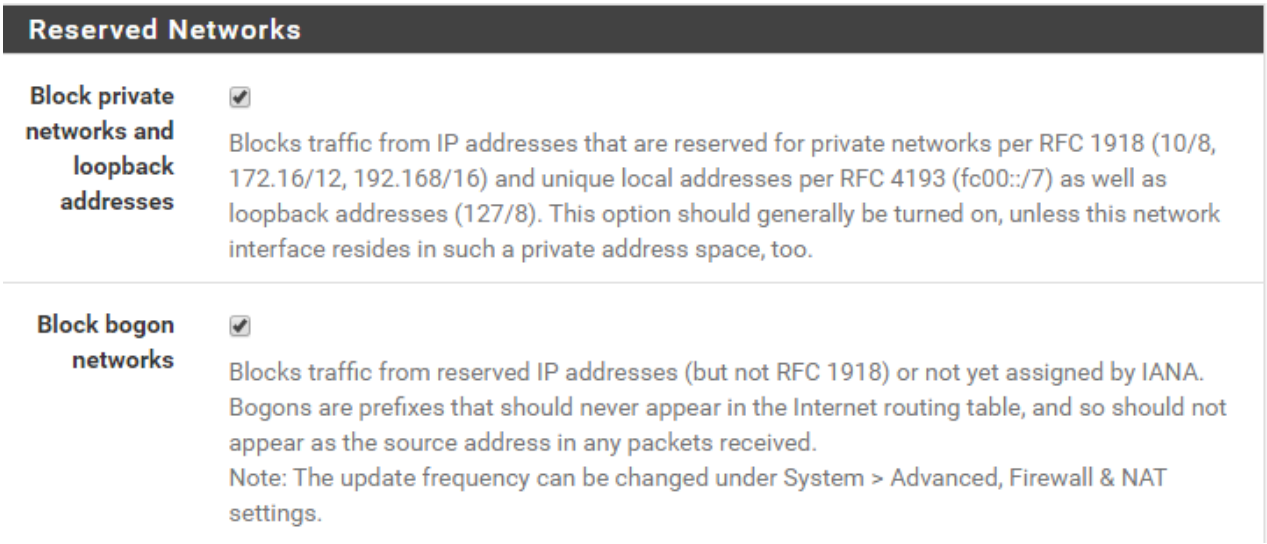



Рисунок 41 – Web-интерфейс block private networks list

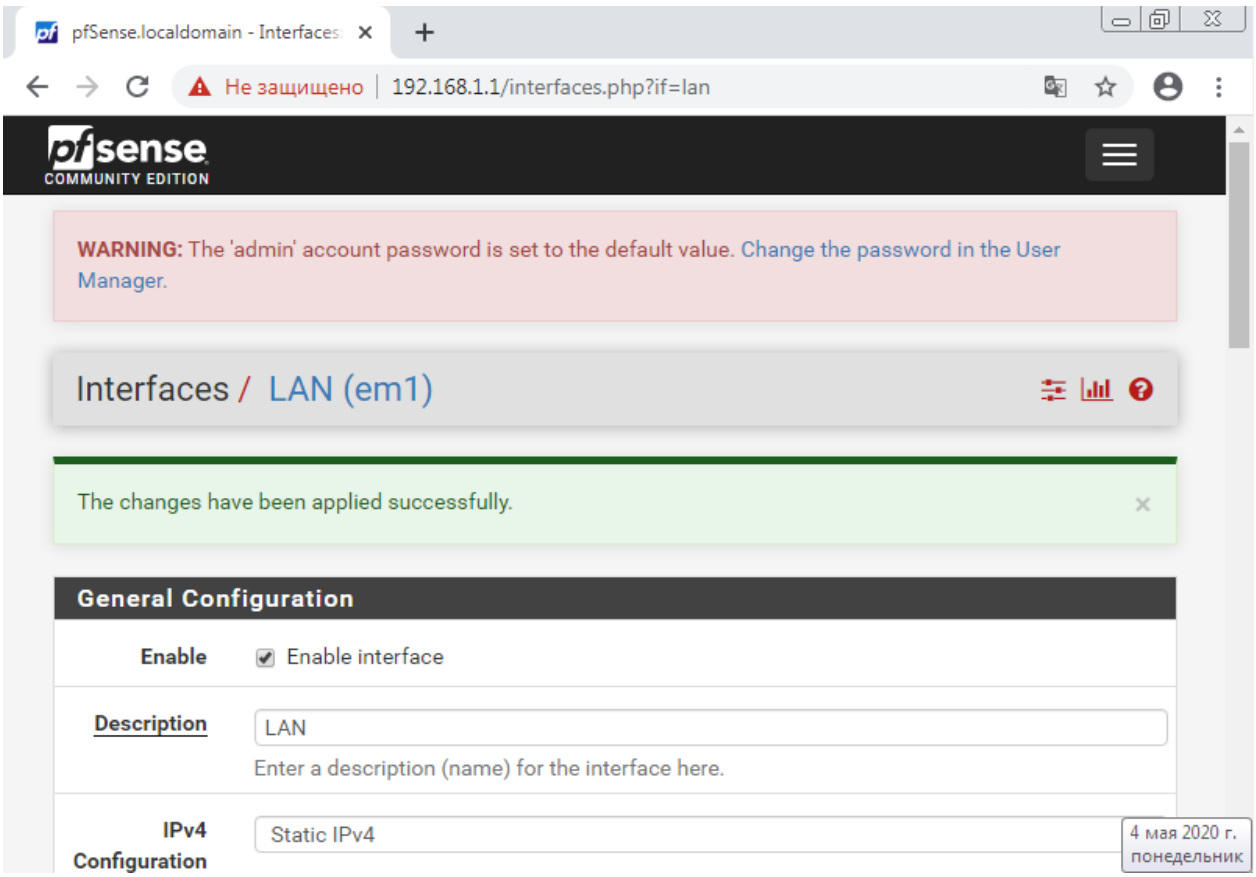



Рисунок 42 – Сохранение конфигураций web-интерфейс block private networks list

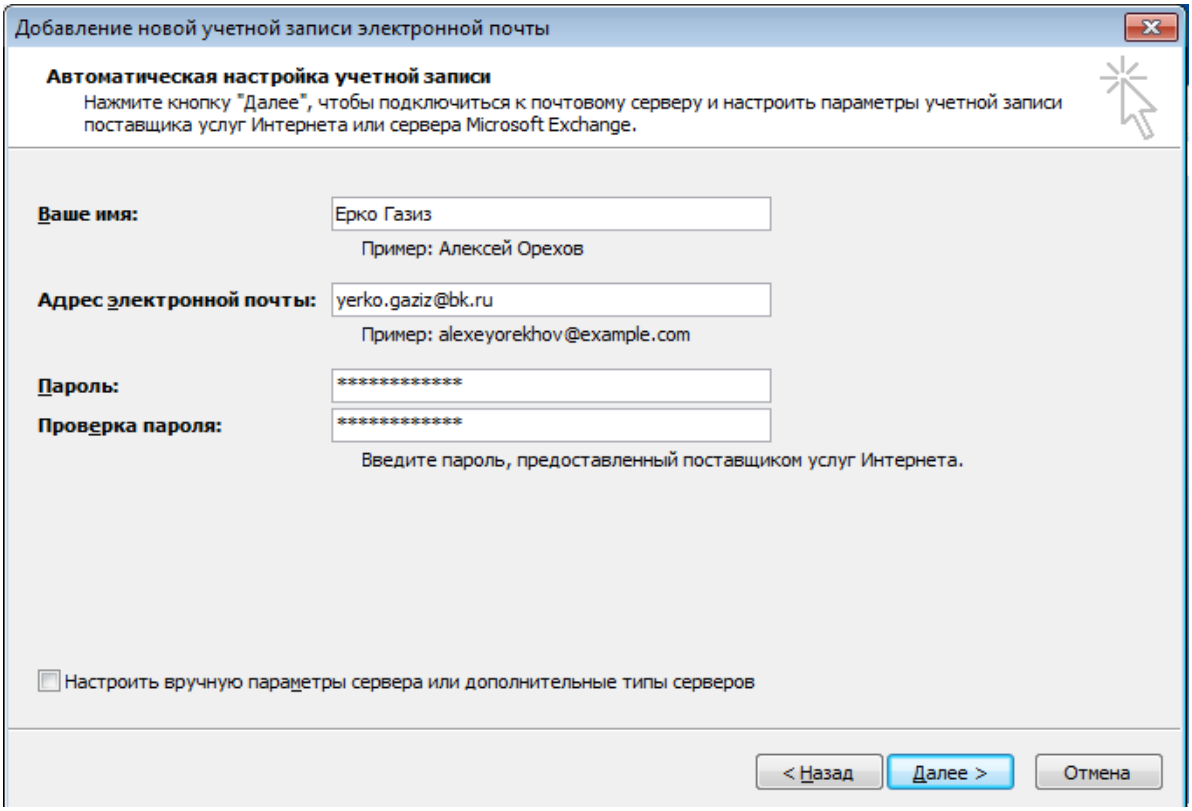



Рисунок 43 - Файл отправителя и получателя

### 3.3 Защита от спама и фильтрация. Репутационная фильтрация

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:

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

2. 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 44 - 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 1 - 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*, | |

*Продолжение таблицы 1*

| | |
|---|---|
| Введите следующие параметры: | |
| ***Sender/Recipient to Classify the email*** | Sender |
| ***Email*** | Blacklist |
| | baduser@*.ru |
| 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 |

*Продолжение таблицы 1*

| | |
|---|---|
| ***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 |
| 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 письма, часто называемые спамом, создают проблемы для пользователей и безопасности в Интернете. Большое количество нежелательных сообщений от группы людей, называемых «спамерами», может удалять ресурсы, содержать вредоносные программы и пытаться перенаправить пользователей на веб-страницы, использующие уязвимости браузера.

Неотъемлемой частью NetDefendOS SMTP ALG является спам-модуль, который обеспечивает фильтрацию спама. Это может значительно снизить нагрузку на почтовые ящики пользователей за брандмауэром. NetDefendOS предлагает два способа борьбы со спамом:

1. Удалить сообщения с высокой вероятностью спама. Разрешить низкий уровень спама.

2. Разрешить сообщения электронной почты с низкой вероятностью спама.

NetDefendOS использует фильтрацию спама для отправки сообщений с удаленного SMTP-сервера на локальный SMTP-сервер через брандмауэр, с которого локальные клиенты затем загружают электронную почту. Локально защищенный SMTP-сервер обычно устанавливается в зоне DMZ.

Ряд доверенных организаций поддерживают открытую базу данных IP-адресов SMTP-серверов, которые рассылают спам, который можно запрашивать через Интернет. Эти списки называются базой данных черного списка DNS (DNSBL), и эту информацию можно получить с помощью стандартизированного метода запроса, поддерживаемого NetDefendOS.

Ниже приведены все компоненты фильтрации спама, используемые DNSBL.


Рисунок 45 - Схема фильтрация спама

Фильтрация спама с использованием DNSBL.

При настройке функции фильтрации спама вы можете отправить IP-адрес сервера, который отправляет сообщение одному или нескольким серверам DNSBL для поиска IP-адресов в базе данных спама DNSBL.

Сервер отвечает, что IP-адрес отсутствует в списке или отсутствует в списке. В последнем случае, когда IP-адрес находится в списке, сервер DSNBL указывает, что электронная почта может быть спамом. Кроме того, он обычно может предоставлять информацию, называемую TXT-записью, которая является текстовой интерпретацией списка.

Администратор может настроить SMTP ALG для доступа к нескольким DNSBL-серверам, чтобы генерировать отзывы об исходном адресе электронной почты. Когда приходит новое сообщение, серверу предлагается определить, содержит ли сообщение спам, в зависимости от исходного адреса.

Администратор NetDefendOS назначает значение веса каждому настроенному серверу, чтобы можно было рассчитать взвешенную сумму на основе всех ответов.

На основании рассчитанной суммы администратор может настроить одно из следующих действий:

1. Капля Если сумма превышает или равна предварительно определенному порогу отсева, сообщение считается спамом и будет удалено или отправлено в специальный почтовый ящик. Если сообщение не получено, администратор отправляет сообщение об ошибке на отправляющий SMTP-сервер.

2. Помечено как Спам (Спам-ярлык). Если сумма больше или равна предопределенному порогу СПАМА, сообщение считается спамом и отправляется получателю вместе с сообщением и текстом.

Пример расчета порогового значения. Предположим, у вас есть три сервера с конфигурацией DNSBL: dnsbl1, dnsbl2 и dnsbl3. Им даны веса 3, 2 и 2 соответственно. Установленный лимит спама 5.

Если dnsbl1 и dnsbl2 считают сообщение спамом, а dnsbl3 - нет, то мы получаем сумму 3 + 2 + 0 = 5, потому что общая сумма 5 равна 5 (или больше). Пороговое значение считается почтовым спамом.

Если установленный порог отбрасывания равен 7, вы должны ответить на все DNSBL-серверы, чтобы удалить сообщение из рассчитанной суммы (3 + 2 + 2 = 7).

Если рассчитанная сумма больше или равна порогу удаления, сообщение не будет отправлено получателю. Вместо этого администратор может выбрать один из двух вариантов отклоненных сообщений:

Вы можете указать конкретный адрес электронной почты для всех удаленных сообщений. Если это сделано, NetDefendOS может добавить сообщения TXT, отправленные серверами DNSBL, которые идентифицируют сообщение как спам, к теме отправленного сообщения.

Если у получателя нет адреса для отклоненных сообщений, NetDefendOS удалит их. Администратор может указать, что сообщение об ошибке было отправлено на адрес отправителя, а также сообщения TXT с серверов DNSBL, которые определили сообщение как спам.

Чтобы настроить фильтр нежелательной почты с использованием DNSBL в SMTP ALG, выполните следующие действия.

Решите, какие DNSBL-серверы использовать. Сервер может быть один или несколько. Несколько серверов могут выступать в качестве резервной копии друг друга, а также для подтверждения статуса отправителя.

Определите значение веса для каждого сервера, которое определяет важность значения, когда вы решаете, что сообщение не является спамом при расчете измеренного количества.

Определите порог спама. Если измеренное количество больше или равно пороговому значению, сообщение считается спамом.

Два порога были определены:

- spam threshold - пороговое значение сообщений, помеченных как спам;
- drop limit - лимит удаления сообщений.

Пороговое значение спама должно быть меньше порогового значения сброса. Если пороговые значения одинаковы, используется только пороговое значение сброса.

Определите текстовую метку в качестве префикса в поле темы сообщения, которое считается спамом.

Также укажите адрес электронной почты, на который будут отправляться все удаленные сообщения.Задание: Необходимо проверить входящие потовые сообщений на спам.

Добавим новый SMTP ALG

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

Таблица 2 - 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 |

*Продолжение таблицы 2*

| | |
|---|---|
| ***bl.spamcop.netorg*** | Weight Value 1 |
| ***list.dsbl.org*** | Weight Value 1 |
| ***zen.spamhaus.org*** | Weight Value 1 |

Таблица 3 - 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 диссертации является разработка программно-технических средств для обеспечения безопасности объекта. Актуальность этой темы заключается в том, что в настоящее время информация является ценным ресурсом, и ее необходимо должным образом взаимодействовать, и если предположить вероятность потери данных, она оценивается как огромная материальная потеря.

Это исследование может быть использовано для реализации корпоративной сети почтового сервера. Благодаря этому исследованию безопасность внутреннего и внешнего пространства объекта, прилегающей территории, людей, материальной и интеллектуальной собственности обеспечивается, контролируется круглосуточно и контролируется в режиме реального времени анализом событий и данных.

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

Вопросы безопасной человеческой жизни должны решаться на всех этапах жизненного цикла, будь то разработка, эксперименты или методология, используемые на практике.

С точки зрения вредоносности считается безопасным работать с компьютерными технологиями (риск смерти составляет менее 0,0001 в год). Рабочая нагрузка компьютерного работника также минимальна, так как уровень умственного напряжения в этом виде деятельности включает потребление 2000 ... 2400 ккал энергии в день.

Однако при работе с компьютерными технологиями работник подвергается ряду неблагоприятных факторов, зависящих от характера производственного процесса, условий производства:

- повышение интенсивности работы и ее однообразия;

- характер зрительной работы;

- тепловыделение от оборудования;

- под воздействием шума;

- воздействия вредного, ионизирующего и неионизирующего излучения

- плохое освещение в комнате и освещение на рабочем месте.

Анализ мер и мер по защите от воздействия вредных производственных факторов.

Анализ условий труда.

При исследовании и установке программного обеспечения сотрудник должен работать с компьютерным оборудованием в течение длительного времени. Рабочая зона - это зона временного или постоянного проживания работника. Поскольку работник может сидеть долго, вам необходимо обеспечить максимальный комфорт, позволяющий работать комфортно и без вредных воздействий. Эти меры должны включать в себя: оптимальное размещение компьютерного оборудования и мебели, достаточное рабочее место, чтобы работник мог выполнять все необходимые действия и движения; работник должен получать необходимое количество света для снижения визуальной нагрузки. Существует несколько видов освещения, естественное и искусственное. [1]

Естественный свет - это дневной свет, который проходит через световые отверстия. Этот тип освещения варьируется в зависимости от окружающей среды, времени суток и времени года.

Искусственное освещение - это освещение естественным светом ночью и в местах, где не хватает естественного света.

Использование искусственного и естественного освещения также называется смешанным освещением.

Правильный выбор освещения и освещения в виде ламп и светильников, а также правильное размещение обеспечивает независимую величину отражения света 40 кд / м ^ 2 на рабочей станции и рабочей поверхности. Белые люминесцентные лампы следует использовать для искусственного ношения. Металлогалогенные лампы мощностью до 250 Вт могут использоваться в промышленных условиях и офисных зданиях.

### 4.1 Характеристики рабочего помещения.

Исследовательское здание рассчитано на три рабочих места. Расположен на первом этаже здания. Визуальная модель комнаты показана на рисунке 48.

Описание здание: длина L = 10 метров, ширина B = 5 метров, высота H = 3 метра. Помещение было построено и оборудовано в соответствии с санитарными требованиями от 02.12.2020, т.е. площадь одного рабочего места должна составлять 4,5 квадратных метра, а монитор должен находиться на расстоянии 60 см от источника. Рабочее пространство работника соответствует требованиям и составляет 50 м2.

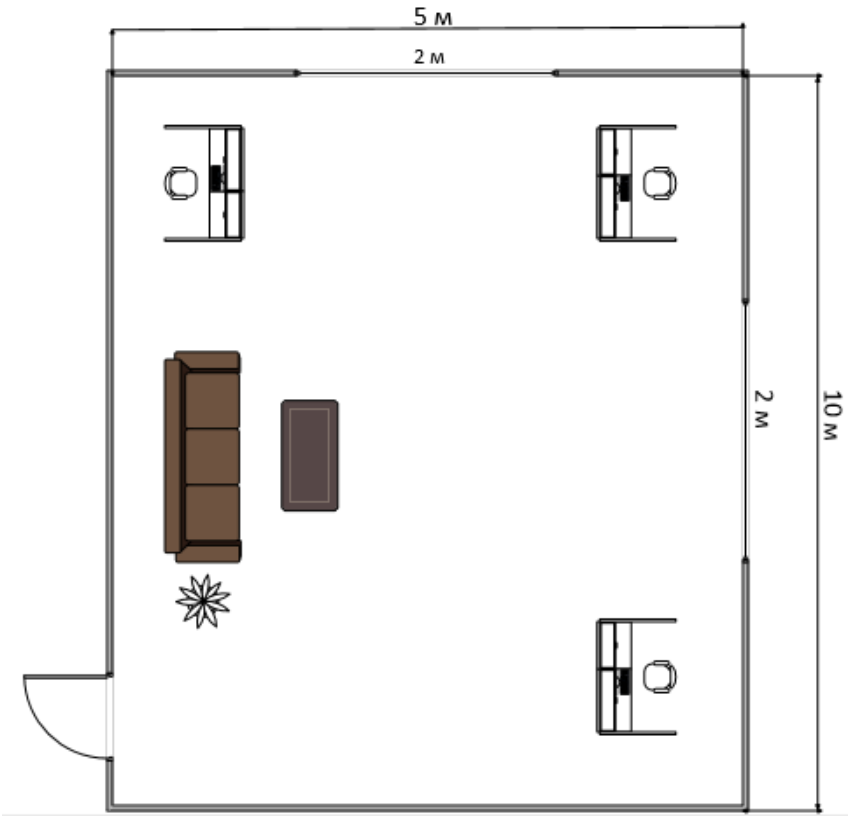



Рисунок 46 - Рабочее помещение

Используемое оборудование и его характеристики
Ноутбук Lenovo ideopad E5-575G. Технические характеристики:

- Intel(R) Core i7 5 поколения 6490DU (CPU 2.80 GHz);
- AMD Radeon graphics;
- ОЗУ 8 ГБ;

- HDD 1 ТБ;
- электропитание: 221-251В, 51Гц, 401 Вт;
- габариты(мм): 270 - 414 – 32,5.

Модем: 6-х портовый с коммутатором 10/1000 Мбит/с.
Стул: высота 0,7 м.
Стол: высота – 0,9 м, длина – 5 м, ширина – 2 м.

### 4.2 Расчет естественного освещения

Одним из основных показателей на определенном уровне является освещение. Качество освещения важно для создания комфортной рабочей обстановки. Хороший уровень света необходим для комфортной работы и также может привести к ухудшению здоровья и ухудшить качество работы. Согласно стандартам освещения (СНиП 11-4-79). Важно выполнить расчеты освещения, чтобы определить площадь естественных световых проемов и характеристики искусственного освещения. Формула для расчета площади легких отверстий при естественном освещении (1):

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

где $S_n$ – площадь помещения, м$^2$;
$e_n$ – нормированное значение КЕО, %;
$K_n$ – коэффициент запаса;
$h_0$ – световая характеристика окон (5,5 - 39);
$K_{зо}$ – коэффициент затемнения окон зданиями стоящими напротив (1,0-1,7);
$r_1$ – коэффициент повышение КЕО за счет отраженного света от поверхности помещения (1,07 - 1,8);
$t_0$ - общий коэффициент светопропускания равен от 0,2-0,9.

Данные характеристики, длина помещения равна 5 метров, а ширина равно 4 метра, найти площадь пола по формуле:

$$S_n = L \text{ x } B, \quad (4.2)$$

Площадь световых проемов естественного бокового освещения определяется формулой (1), необходимы следующие значения:

где $e_n = 1{,}5$ %;
$K_n = 2$;
$h_0 = 21$;
$K_{зо} = 1{,}2$;
$r_1 = 1{,}5$;
$t_0 = 0{,}8$.

Надо подставить значение данных в формулу (4.1) и вычислить площадь световых проемов:

$$S = \frac{50x1,5x2x21x1,2}{100x0,8x1,5} = 32,5 \text{ м}^2 , \quad (4.1)$$

Рассчитав площадь оконного пространства, значение вышло 32.5 $м^2$, из чего следует вывод что освещение площадью 3 $м^2$ достаточно для создания комфортных условий освещения.

### 4.3 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]:

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

где, N или n — кратность (раз в час);

Q - нужное количество свежего воздуха в час, $м^3/ч$;

V - объем помещения, $м^3$; 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]

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

где, V у. в. — объем удаляемого воздуха, $м^3/ч$;

V пом — объем помещения, $м^3$.

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]:

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

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 этом разделе моей дипломной работе я рассмотрел и рассчитал световые показатели для условий труда. Эти показатели являются одними из важнейших в организации труда, они всегда должны соответствовать стандартам и нормам, так как они помогают создать комфортные условия для работника и не мешают его работе. Исходя из расчетов, могу сказать, что нет естественного света от окна длиной 3 метра и шириной 2, чтобы осветить помещение площадью 50 м2. Комбинированное освещение, которое включает в себя естественное и искусственное освещение, требуется для комфортной работы. Исходя из расчетов, полученных при выполнении этого раздела, в моем случае мне нужно использовать 2 лампы DRL-80 3800 лк. Если необходимые условия соблюдены, работник может выполнять всю необходимую работу и исследования 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 Анали рисков информационной безопасности

Риск информационной безопасности - это вероятность раскрытия или потери в результате информационных атак или утечки данных в организации.

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.

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

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.

Редактировать сжатые / архивные файлы. 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 перегрузке сети, поэтому мониторинг соблюдения ограничений на количество вложений, указанных 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 («административные», «человеческие ресурсы», «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, можно провести дополнительный анализ почтового потока компании, исправить систему, проанализировать случаи, связанные со злоупотреблением почтовыми услугами компании и т. Д.

На картинке. 50 - таблица 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).

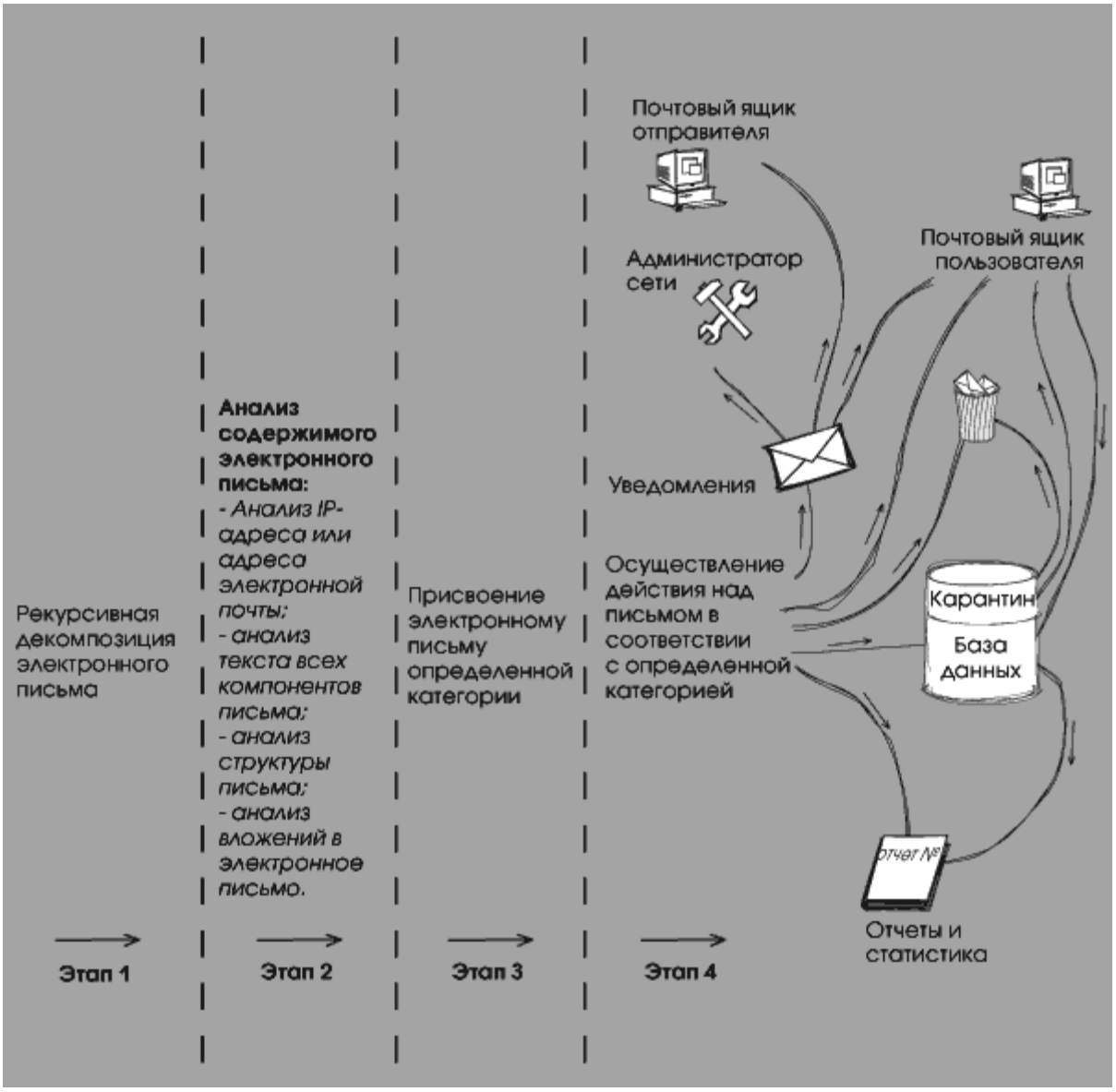



Рисунок 47 - Схема обработки сообщения системой контроля содержимого электронной почты

### 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:

$$R = V * U, \quad (5.1)$$

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 5 - 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 6, где описано значение ущерба для расчета .

Таблица 6 - 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

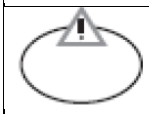
В данной работе применяется такой метод оценивания рисков как Coras.

В данной методологии информационные системы представлены как сложный комплекс с учётом человеческого фактора, а не только на основе используемых технологий.

Программное обеспечение использует UML графический описательный язык для моделирования объектов в области разработки программного обеспечения.

UML - широко используемый язык; это открытый стандарт, который использует графические обозначения для создания абстрактной модели системы, называемой моделью UML. UML в основном используется для идентификации, визуализации, проектирования и документирования программных систем.

Таблица 7 - 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 48 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.

Рисунке 49, 50 - 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 51 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 52 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 53 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 на рисунке 48

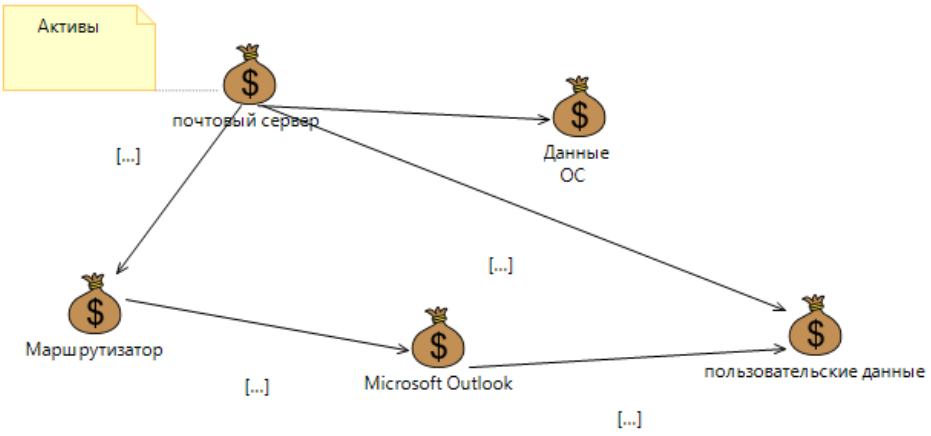



Рисунок 48 – Активы на которые влияют уязвимости

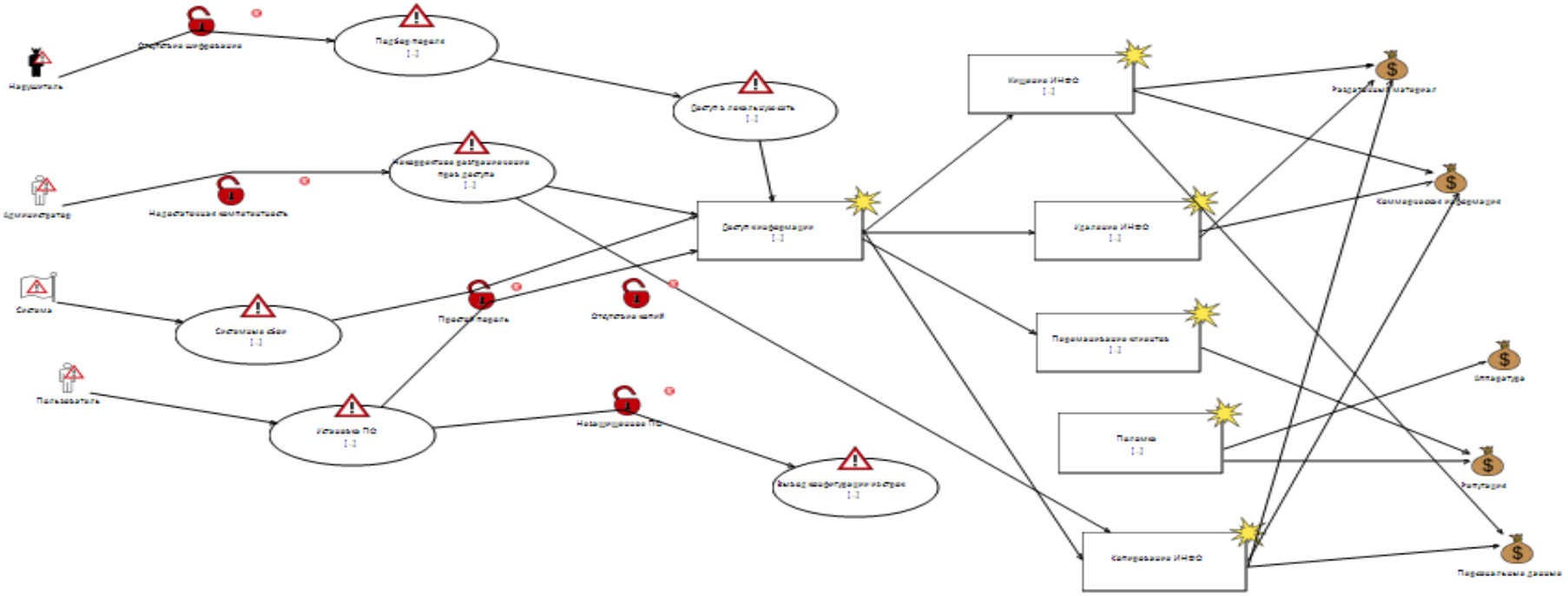


Рисунок 49 - Модель угроз информационной безопастности

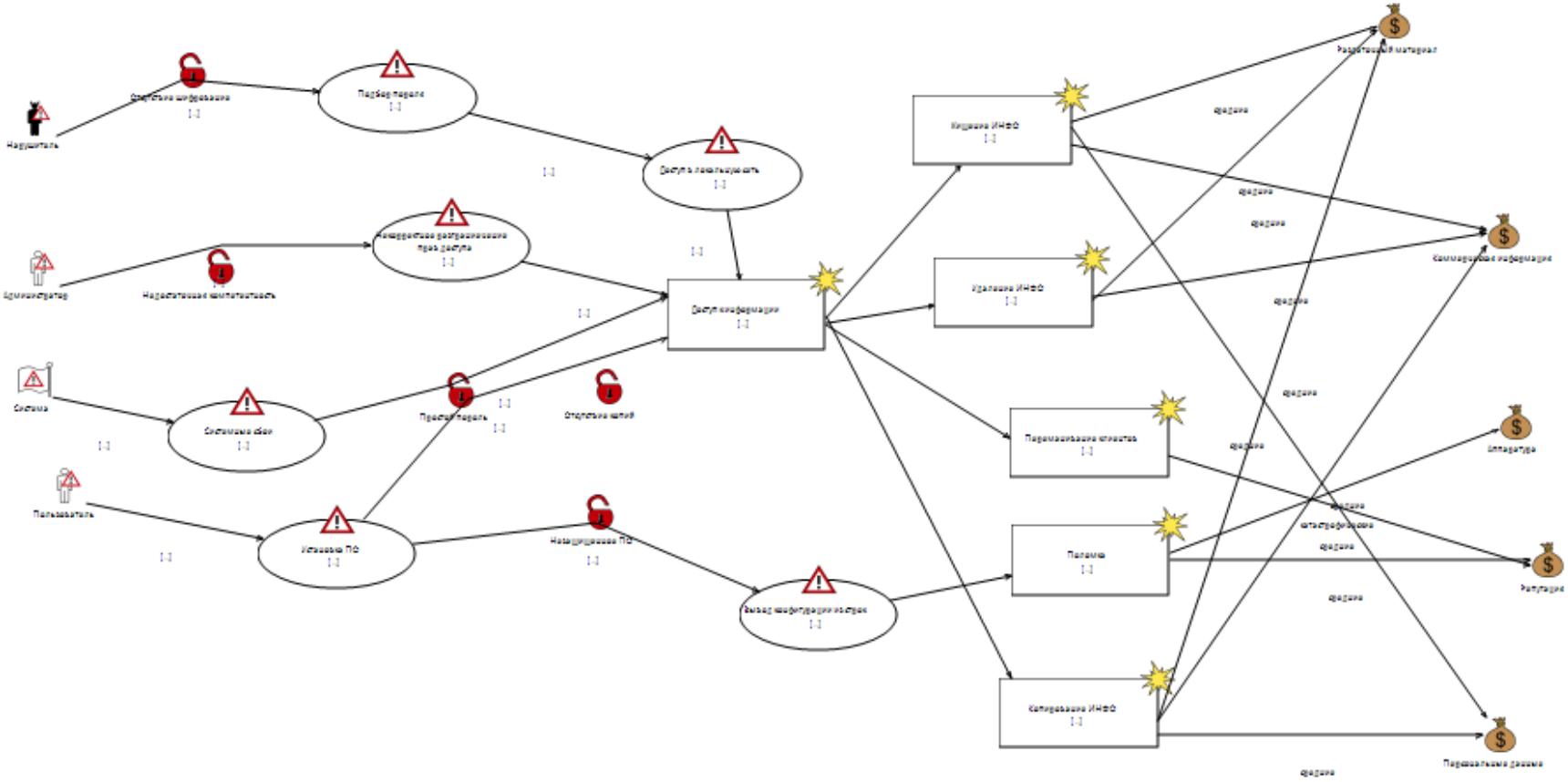


Рисунок 50 - Модель вероятностными риска

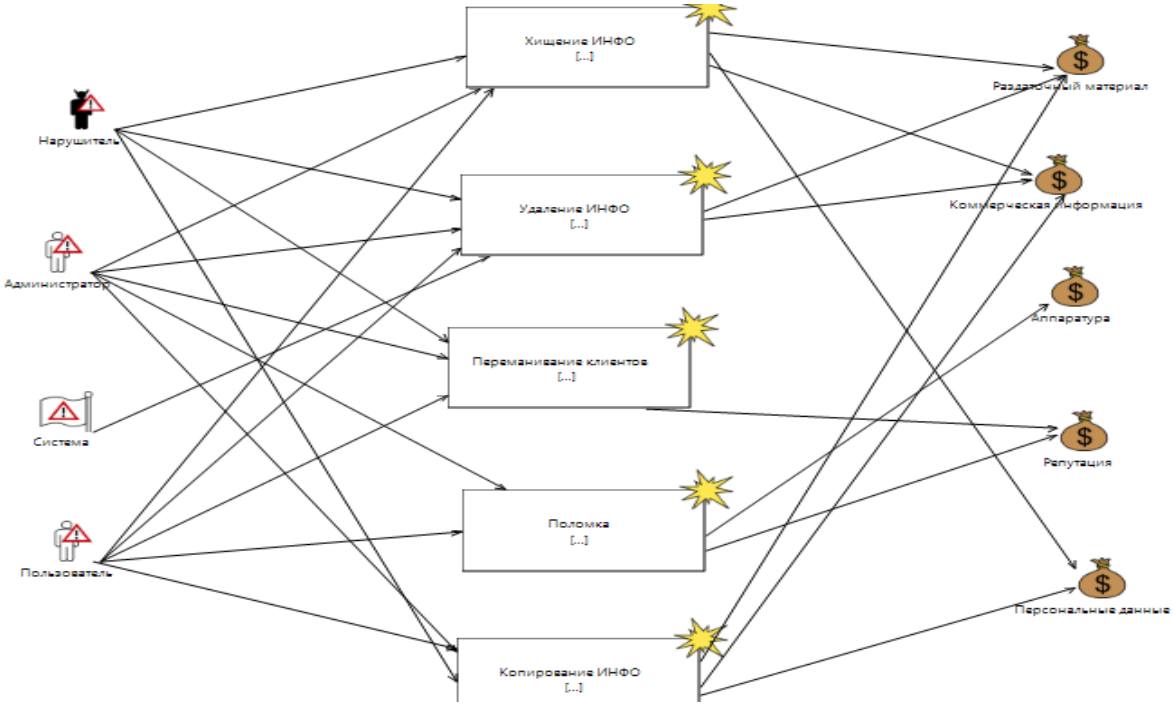



Рисунок 51 – Диаграмма риска информационной безопасности

Теперь мы определим последствия для каждого актива для каждого риска, если таковые имеются (Рисунок 52).

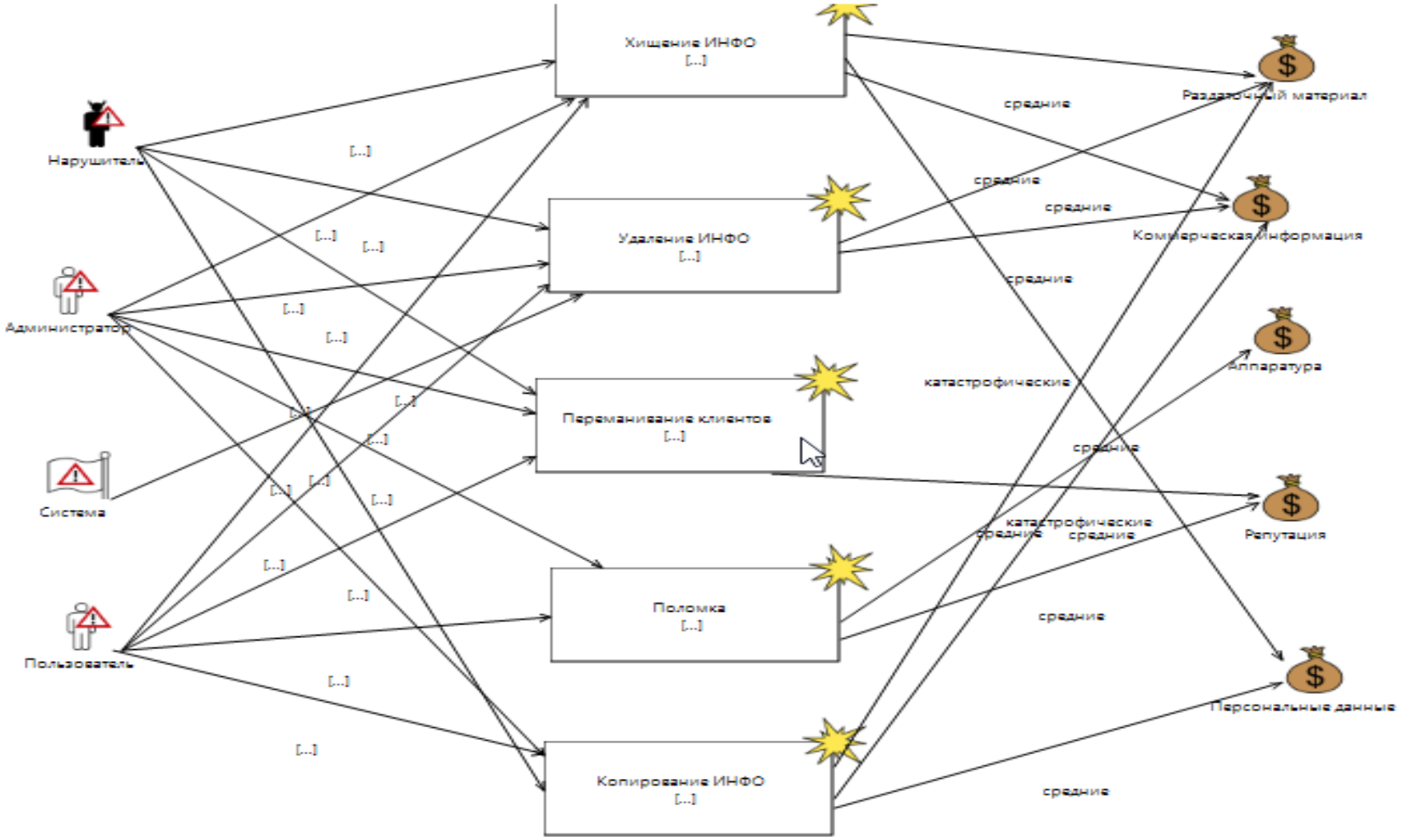



Рисунок 52 – Диаграмма рисков с описанием последствий осуществления угрозы

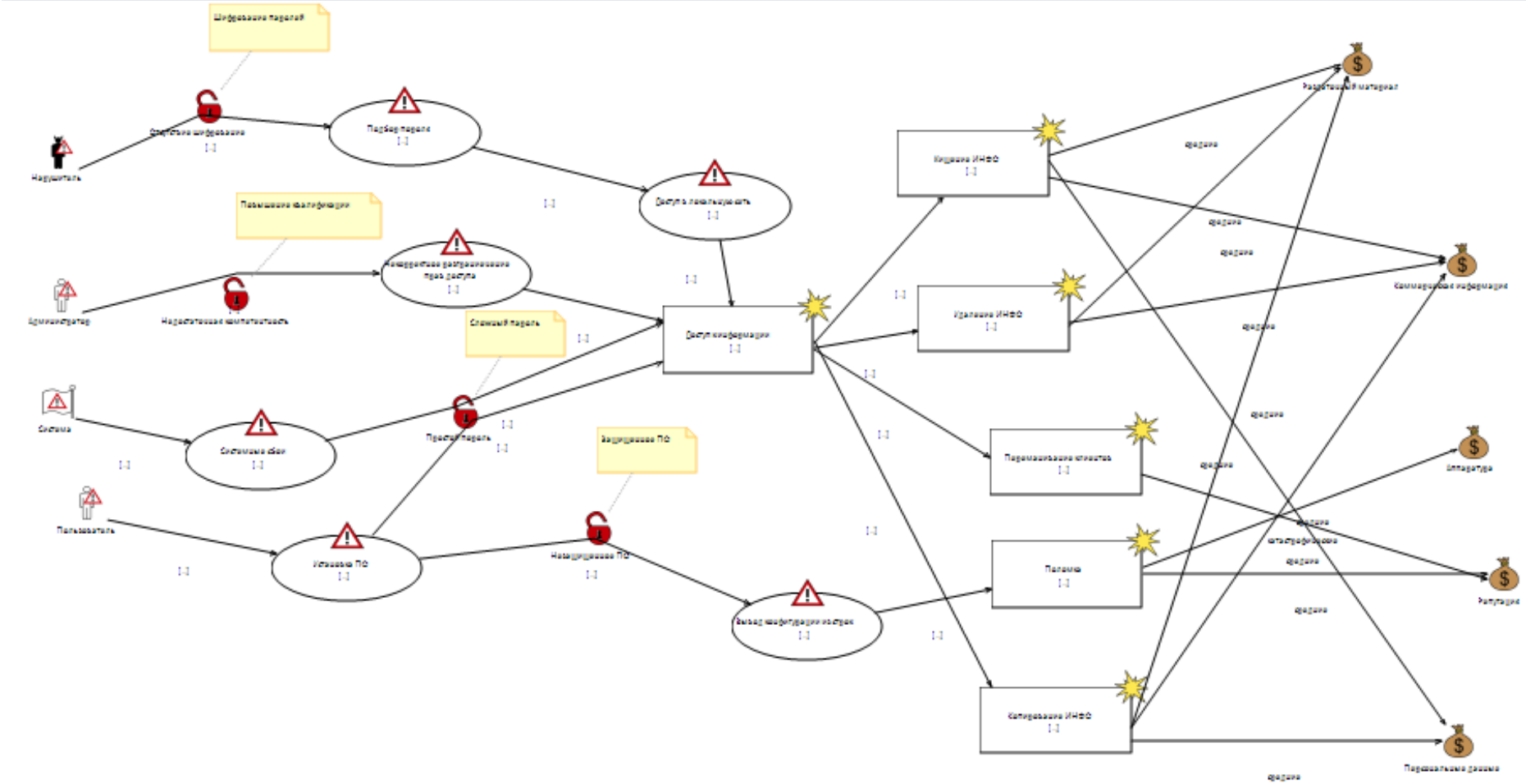


Рисунок 53 – Диаграмма угроз после добавления противодействий

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

По итогам данной дипломной работы была создана виртуальная корпоративная сеть с использованием Windows server 2012, Windows 7, Outlook 2012 , защитная меры были произведены при помощью виртуального маршрутизатора PFSENSE. Был настроен black, white листы в web-интерфейсе PFSENSE. Вопросы обеспечения защиты электронной почты, в данной дипломной работе, способствуют базовой (фундаментальной) теоретической и практической подготовки в области систем информационной безопасности

Выполнение этих задач развивает, обрабатывать, анализировать и систематизировать научно-техническую информацию, выбирать перспективные методы решения профессиональных задач на основе современного оборудование электронной почты.

Коллективное решение задач проектирования систем безопасности предполагает активное приобретение навыков правильной формулировки основных требований к параметрам элементов систем безопасности, их сборки, контроля безопасности. Система в целом, основанная на анализе требований клиентов и обследовании объектов.

## Список литературы

1 В. Олифер, Н. Олифер "Компьютерные сети. Принципы, технологии, протоколы, 2016. - 176 с.

2 Уильям Станек "Microsoft Windows Server 2012. Справочник администратора, 2017. - 196 с.

3 Крейг Хант, "TCP/IP — Сетевое администрирование, 2019. - 162 с.

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 Настройка pfSense в качестве корпоративного Прокси Сервера. URL: http://fadmin.ru/article/nastroyka-pfsense-v-kachestve-korporativnogo-proksi-servera (дата обращения: 10.03.2020).

14 Рекомендации по безопасности FreeBSD. URL: https://docs.netgate.com/pfsense/en/latest/releases/2-0-2-new-features-and-changes.html#freebsd-security-advisories (дата обращения: 20.03.2020).