МИНОБРНАУКИ РОССИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**“ТВЕРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ”**

**(ФГБОУ ВО «ТГУ»)**

Математический факультет

Кафедра Компьютерной безопасности и

математических методов управления

**ОТЧЕТ**

по производственнойпрактике

студентки 4 курса М-45 группы

Беловой Юлии Германовной

Специальность 10.05.01 Компьютерная безопасность

Специализация «Математические методы защиты информации»

Зав. кафедрой \_\_\_\_\_\_\_Андреева Елена Аркадьевна\_\_\_\_\_\_\_\_\_\_\_ 09.06.2017

*Подпись, расшифровка, ученая степень, звание*

Обучающийся \_\_\_\_\_\_\_\_\_Белова Юлия Германовна\_\_\_\_\_\_\_\_\_\_ 09.06.2017

*Подпись, расшифровка подписи*

Руководитель ООП\_\_\_Семыкина Наталья Александровна\_\_\_\_\_\_\_09.06.2017

*Подпись, расшифровка подписи, ученая степень, звание*

Руководитель практики от предприятия

\_\_\_Прохорцев Игорь Алексеевич\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 09.06.2017

*Подпись, расшифровка подписи, ученая степень, звание*

Тверь 2017

**Оглавление**

[Введение 3](#_Toc487708539)

[Описание теоретических и практических аспектов выполненной работы 4](#_Toc487708540)

[1. Терминология 4](#_Toc487708541)

[2. Практическая часть 10](#_Toc487708542)

[Заключение 19](#_Toc487708543)

[Список использованных источников 20](#_Toc487708544)

# **Введение**

Корпорация ИМС имеет широкую сеть региональных филиалов и сервисных центров на территории России и стран СНГ. Один из филиалов находится у нас в Твери. Они оказывают сервисные услуги по обслуживанию измерительных систем и технологического оборудования, которые позволяют заказчикам непрерывно получать достоверные результаты измерений и существенно сократить эксплуатационные затраты, практически исключить операционные риски.

ИМС реализует полный цикл услуг:

* Проведение метрологического и технического аудита;
* Проектные и проектно-конструкторские работы;
* Комплектацию проектов и поставку приборов, систем;
* Производство и поставка технологического оборудования и систем;
* Метрологическое оснащение;
* Строительство промышленных объектов;
* Монтаж и шефмонтаж оборудования;
* Пусконаладочные работы и ввод в эксплуатацию;
* Гарантийное, постгарантийное и техническое обслуживание.

На время прохождения практики, с 12 июня по 9 июля, нашей группе практикантов поставили задачу по установке, изучению и применению межсетевых экранов для защиты офисных сетей.

# **Описание теоретических и практических аспектов выполненной работы**

1. ***Терминология***

**Межсетевой экран** — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик.[1]

Основной задачей межсетевого экрана является предотвращение нежелательного доступа в локальную сеть. Примером нежелательного доступа является нарушитель, который пытается осуществить незаконное проникновение в системы, доступные по сети. Он может просто получать удовольствие от взлома, а может стараться повредить информационную систему или внедрить в нее что-нибудь для своих целей. Например, целью хакера может быть получение номеров кредитных карточек, хранящихся в системе. Другим примером нежелательного доступа является размещение в вычислительной системе чего-либо, что воздействует на прикладные программы и сервисы, которые вычислительная система предоставляет своим пользователям.

Для работы с межсетевым экраном мы пользовались следующими формулировками:

**DHCP** (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. [2]

**DNS** (англ. Domain Name System — система доменных имен) — компьютерная распределенная система для получения информации о   
доменах. [3]

**TCP** (Transmission Control Protocol, протокол управления передачей) **—** один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных. Сети и подсети, в которых совместно используются протоколы TCP и IP называются сетями TCP/IP. В стеке протоколов IP TCP выполняет функции протокола транспортного уровня модели OSI.

Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи. Реализации TCP обычно встроены в ядра ОС. Существуют реализации TCP, работающие в пространстве пользователя. [4]

**IP-адрес** - это двоичное 32-разрядное число, которое идентифицирует, в какой из подсетей постоянно находится компьютер, а также уникальный номер компьютера в той подсети. Для лучшего восприятия это число преобразуется в четыре десятичных числа со значениями в пределах от 0 до 255.

**Маска подсети** определяет, какая часть IP-адреса является сетевым адресом, а какая часть является адресом хоста. Маска делает это "маскируя", т.е. "закрывая" с помощью двоичного числа ту часть сетевого IP-адреса, которая отведена для нумерации подсетей. [5]

**Сетевой шлюз** (англ. gateway) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной). [6]

Межсетевые экраны чаще всего используются при подключении сети к интернету, но они могут применяться и для разграничения трафика внутри одной организации. Например, можно установить межсетевой экран, чтобы ограничить соединения с внутренней подсетью, в которой обрабатываются конфиденциальные данные.

Классической моделью, описывающей принципы сетевого взаимодействия, является модель **OSI** (Open Systems Interconnection). Данная модель описывает сетевое взаимодействие как набор вложенных друг в друга уровней. Данные протоколов более высокого уровня расположены в теле протоколов более низкого уровня. Каждый уровень выполняет определенные функции, для которых разработаны специальные протоколы. В модели OSI определено семь уровней (табл. 1). [7]

|  |  |  |
| --- | --- | --- |
| Уровень 7 | Прикладной уровень | Этот уровень отвечает за взаимодействие приложений по сети, т.е. на этом уровне общаются приложения. |
| Уровень 6 | Представительский уровень | Этот уровень отвечает за кодирование данных, для того чтобы их потом можно было передать по сети и соответственно преобразует их обратно, для того чтобы приложение понимало эти данные. |
| Уровень 5 | Сеансовый уровень | Отвечает за поддержание сеанса между передачей данных. |
| Уровень 4 | Транспортный уровень | Отвечает за надежность передачи данных. |
| Уровень 3 | Сетевой уровень | Предназначен для определения пути,  по которому должны пройти данные. |
| Уровень 2 | Канальный уровень | Обеспечивает взаимодействие на физическом уровне. |
| Уровень 1 | Физический уровень | Физическая передача данных. |

Таблица 1

**NAT** (Network Address Translator)— это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Преобразование адреса методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма которого состоит в замене адреса источника (англ. source) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. destination) в ответном пакете. [8]

Принимая пакет от локального компьютера, роутер смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому роутер «на лету» транслирует (подменяет) обратный IP-адрес пакета на свой внешний (видимый из интернета) IP-адрес и меняет номер порта (чтобы различать ответные пакеты, адресованные разным локальным компьютерам). Комбинацию, нужную для обратной подстановки, роутер сохраняет у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер сотрет у себя в таблице запись о n-ом порте за сроком давности.

Пример осуществления публикации локальных ресурсов во внешней IP-сети:

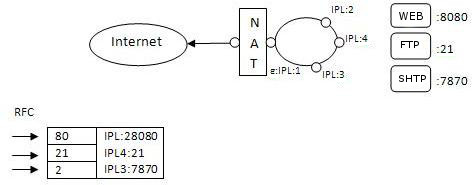


Рисунок 1

**DMZ** (демилитаризованная зона, ДМЗ) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного может выступать, например, веб-сервис: обеспечивающий его сервер, который физически размещён в локальной сети, должен отвечать на любые запросы из внешней сети, при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа. [9]

Цель ДМЗ — добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.

**Оснастка.** Встроенная консоль управления MMC предоставляет обширные возможности для управления компьютером. Microsoft и многие сторонние разработчики приложений используют эту платформу для создания своих консолей управления. [10]

Для управления системой и приложениями в консоли MMC используются *оснастки* — небольшие программы, позволяющие настроить разные аспекты операционной системы. ОС Windows поставляются с большим количеством встроенных оснасток, которые можно использовать для управления системой. Их можно использовать для управления параметрами пользователей, приложениями Windows, безопасностью и многими другими жизненно важными компонентами системы.

Например, в Windows 7 есть следующие встроенные оснастки MMC:

* Сертификаты (Certificates) позволяет настроить доступные в системе хранилища сертификатов. Сертификаты помогают обеспечить безопасную среду работы.
* Управление компьютером (Computer Management) фактически представляет собой набор оснасток, используемых для планирования задач, управления дисковым устройством, мониторинга производительности и для многих других задач по настройке и управлению.
* Диспетчер устройств (Device Manager) предназначен для просмотра и настройки установленного в системе оборудования. Позволяет отключать устройства, обновлять драйверы и устранять возможные неполадки.
* Управление дисками (Disk Management) служит для управления дисками и томами, позволяя создавать тома, форматировать диски и включать функции отказоустойчивости.
* Просмотр событий (Event Viewer) позволяет просматривать журналы системных событий, что помогает своевременно выявлять неполадки системы или приложений. Кроме того, журнал Безопасность (Security) позволяет обнаруживать попытки несанкционированного доступа.

1. ***Практическая часть***

Во время выполнения нашей задачи, мы работали с третьим уровнем модели OSI, так как мы занимались настройкой оборудования для работы. Реализация межсетевого экрана производилась на маршрутизаторе Cisco ASA 5505:



Рисунок 2

Для работы с маршрутизатором, необходимо было восстановить заводские настройки оборудования, установить пароль. Это было выполнено в консольном режиме, при помощи программы PuTTY.

**PuTTY** — свободно распространяемый клиент для различных протоколов удалённого доступа, включая SSH, Telnet, rlogin. Также имеется возможность работы через последовательный порт. PuTTY позволяет подключиться и управлять удаленным узлом (например, сервером). В PuTTY реализована только клиентская сторона соединения — сторона отображения, в то время как сама работа выполняется на стороне сервера. [11]

Области применения программы PuTTY:

* удаленное администрирование Linux.
* подключение к виртуальным серверам по протоколу SSH.
* настройка сетевых маршрутизаторов через последовательный порт.
* соединение с удаленными Telnet-терминалами и пр.

При запуске программы PuTTY для работы с маршрутизатором были заданы следующие настройки, показанные на рисунке 3:

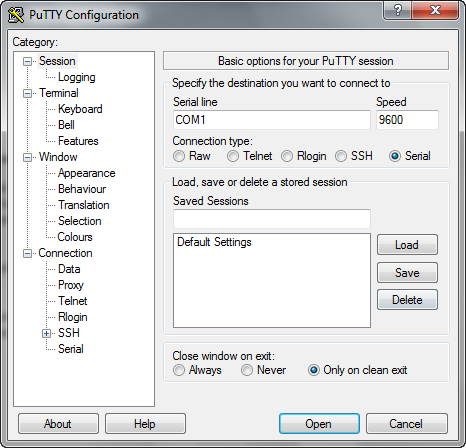


Рисунок 3

Для работы с маршрутизатором, необходимо было подключить его при помощи COМ-порта:



Рисунок 4

Подключение осуществлялось по следующей схеме:

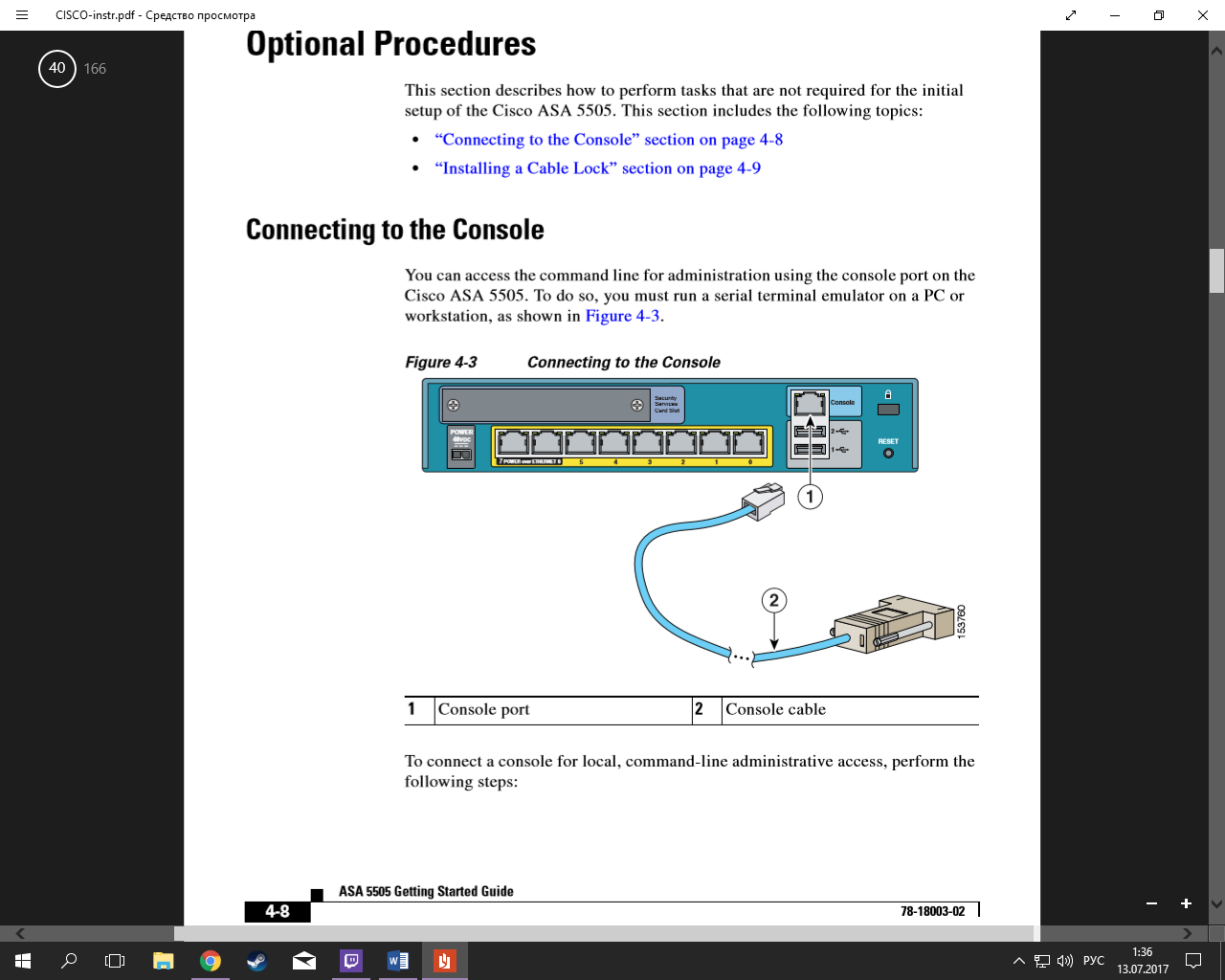


Рисунок 5

После подключения и запуска программы были выполнены следующие команды:

|  |  |
| --- | --- |
|  | rommon #1> confreg |
|  | rommon #1> boot |
|  | rommon #1> enable   |  | | --- | | hostname# copy startup-config running-config | | hostname# configure terminal | |

Далее мы создали пароль для работы с маршрутизатором и задали его, закончили настройку:

|  |  |
| --- | --- |
|  | hostname(config)# enable password (пароль) |
|  | hostname(config)# config-register 0x10011 |
|  | hostname(config)# exit |
| hostname(config)# copy running-config startup-config | |

 И для корректной работы с маршрутизатором мы перезагрузили его:

|  |
| --- |
| hostname(config)# reload |

После этих действий мы решили настроить демилитаризованную зону и создать веб-сервер.

Так как наша производственная практика проходила на некрупном предприятии, то в локальной сети офиса ip-адреса имели вид «192.168. . », как это обычно принято в небольших офисах. Эта информация потребовалась нам для дальнейшей работы с маршрутизатором.

Мы осуществили подключение к сети Интернет на ноутбуке, выделенном нам для работы. Требовалось задать статический ip-адрес для машины. Был выбран ip-адрес 192.168.22.1, маска подсети – стандартная, 255.255.255.0:

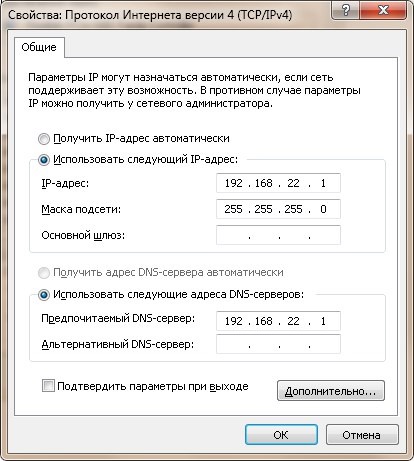


Рисунок 6

Созданная нами локальная сеть функционирует в пределах нашего предприятия, мы же хотим, чтобы у нас была возможность обращаться к этому серверу для удаленной работы по сети Интернет. Для этого требуется настроить переадресацию (NAT), чтобы при обращении к нашему маршрутизатору, обеспечивающему выход в Интернет, запросы посылались на веб-сервер, расположенный в зоне DMZ.

Для этого мы зашли в настройки роутера (рисунок 7), задали параметры для нашего общедоступного веб-сервера и запустили его:

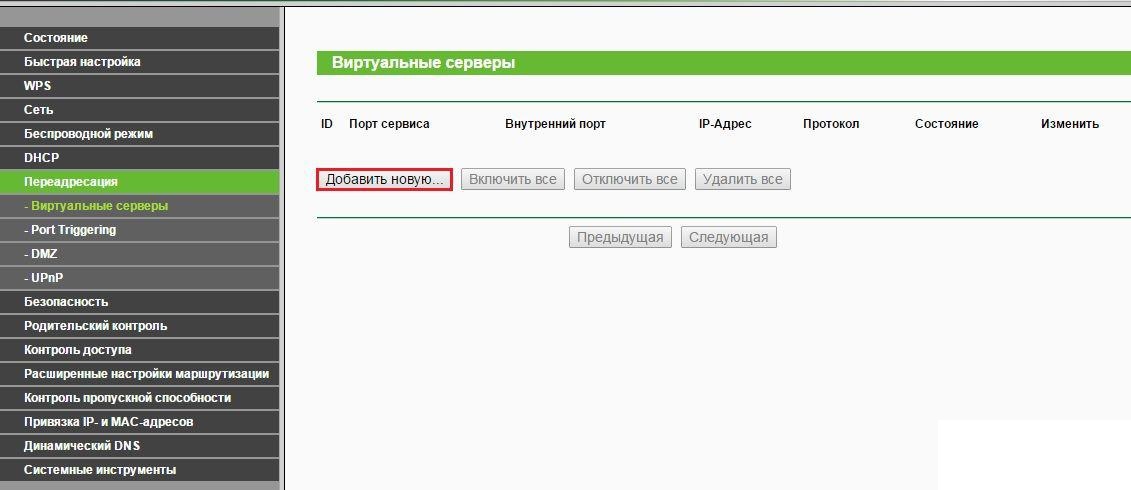


Рисунок 7

Для получения доступа из внешней сети к созданному нами веб-серверу, обращаться к серверу придется через другой ip-адрес, так как упомянутый выше ip-адрес 192.168.22.1 используется только в локальной сети, мы не можем его использовать вне этой сети. Ip-адрес для обращения к нашему серверу имеет следующий вид: 176.120.179.255. Как мы можем видеть на рисунке 7, веб-сервер успешно функционирует:

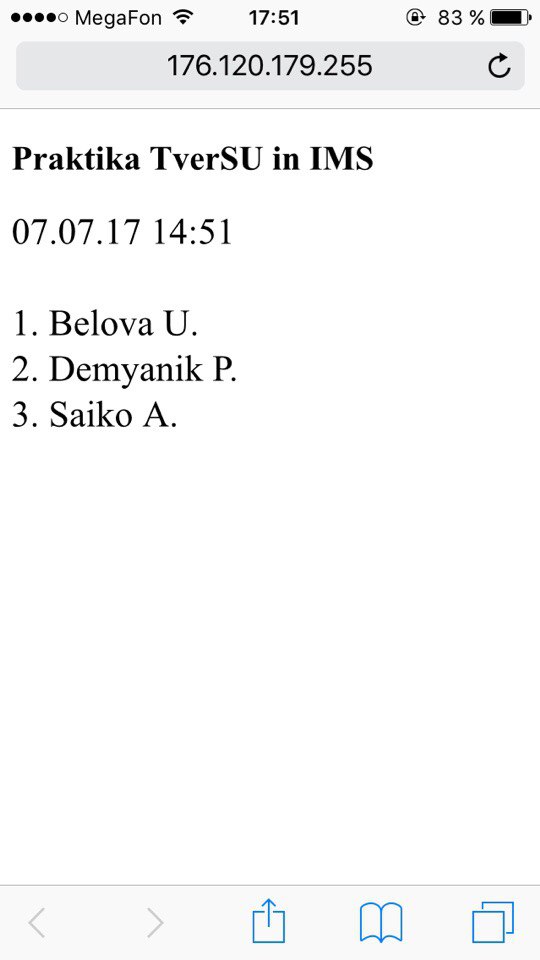


Рисунок 8

Таким образом, мы успешно справились с поставленной перед нами задачей – изучили создание межсетевых экранов, опробовали его на практике.

Теперь поговорим о DMZ и зачем нам это потребовалось.

Когда все узлы корпоративной сети содержатся в одной, общей для всех сети («Внутренняя сеть»), в рамках которой коммуникации между ними не ограничиваются, есть один недостаток: в случае взлома, при котором нарушитель получит контроль над одним из опубликованных в интернете серверов, ему для дальнейшей атаки становятся доступны все остальные узлы и каналы связи корпоративной сети.

Для устранения указанного этого недостатка узлы сети, доступные из интернета, помещают в специально выделенный сегмент – демилитаризованную зону (DMZ). DMZ организуется с помощью межсетевых экранов, отделяющих ее от Интернета и от внутренней сети (рисунок 9)

Изображение выглядит как текст

Описание создано с высокой степенью достоверности

Рисунок 9

К плюсам можно отнести:

* Повышенная защищённость сети от взломов отдельных сервисов. Даже если один из серверов будет взломан, нарушитель не сможет получить доступ к ресурсам, находящимся во внутренней сети (например, сетевым принтерам, системам видеонаблюдения и т.д.).

А к минусам:

* Сам по себе вынос серверов в DMZ не повышает их защищенность.

Помимо этого, во время прохождения производственной практики, мы ознакомились с основами администрирования учетный записей посредством Microsoft Management Console. Используя консоль управления (рисунок 10), мы научились пользоваться стандартными оснастками для разграничения доступа к определенным частям операционной системы в учетных записях.

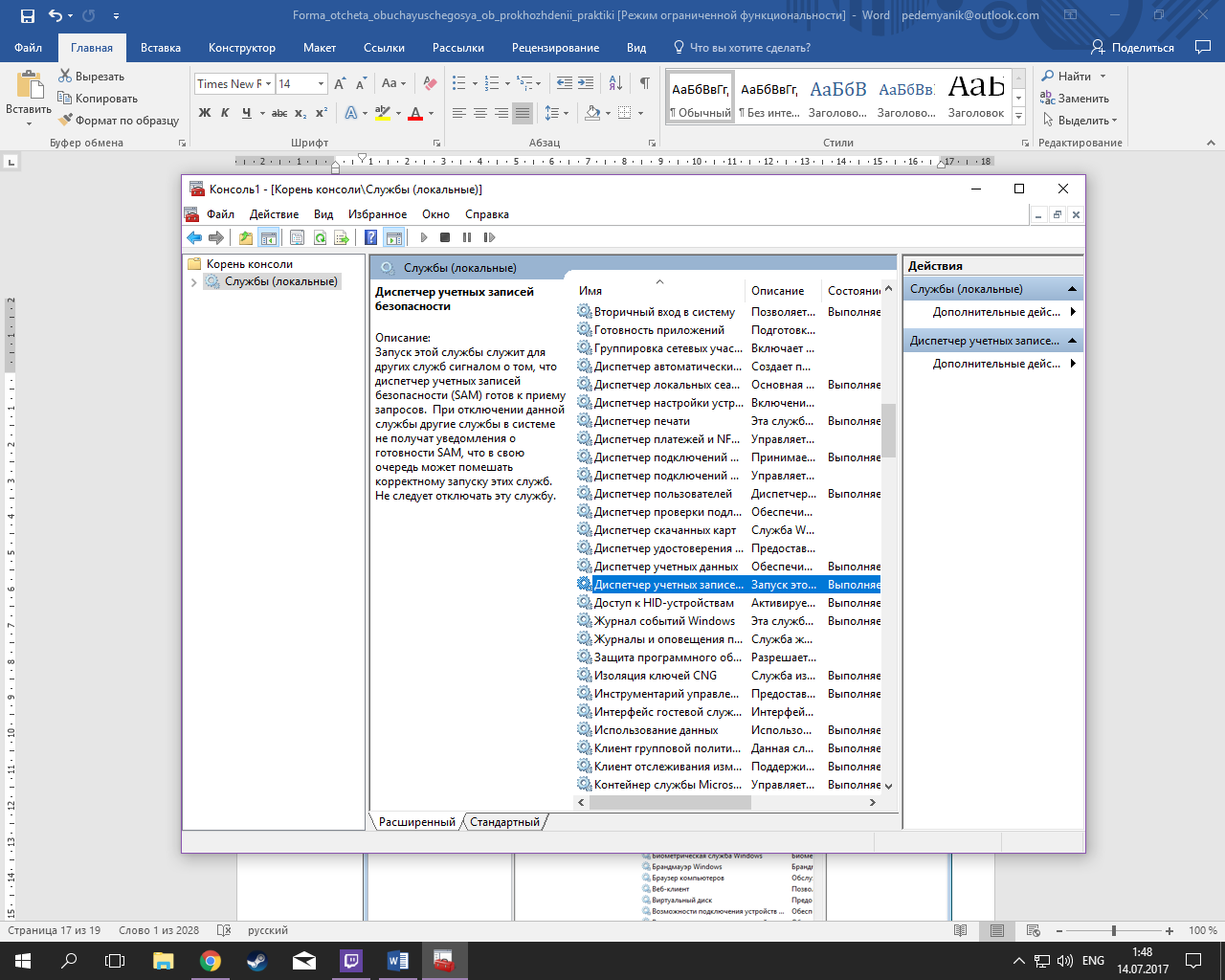


Рисунок 10

Для работы с консолью управления, на ноутбуке была создана дополнительная учетная запись со стандартными правами пользователя. Предполагалось, что это учетная запись одного из сотрудников, работающего на данном компьютере. Во избежание злокачественных действий со стороны пользователя, требовалось лишить его доступа к панели управления. Данная задача выполнялась при помощи стандартной оснастки:

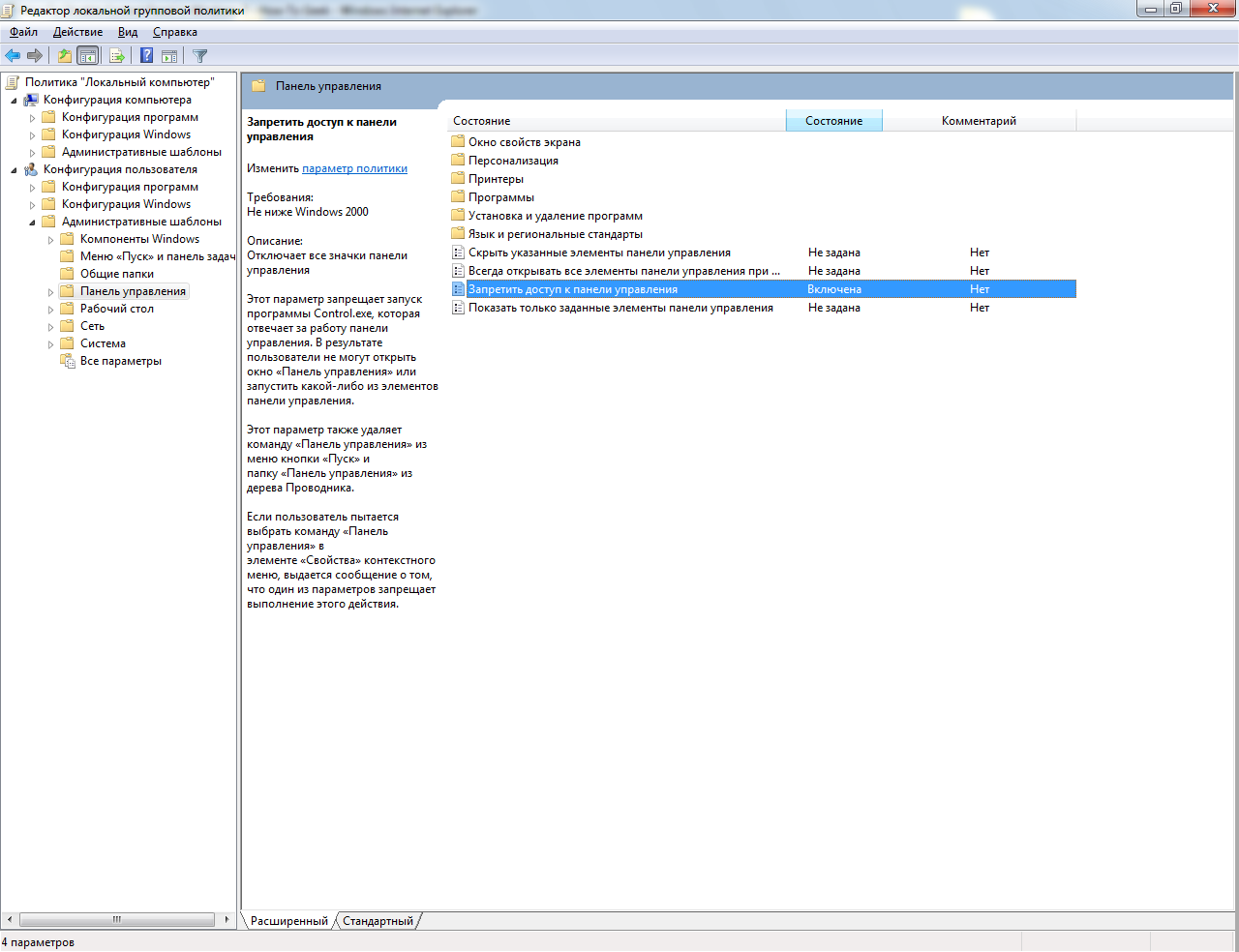


Рисунок 11

Помимо этого, аналогичным образом был запрещен доступ пользователя к диспетчеру задач, языковой панели и к некоторым потенциально уязвимым приложениям.

# **Заключение**

Ни одна фирма не может обойтись без собственной корпоративной сети в офисах, поэтому одним из базовых навыков специалиста по компьютерной безопасности должен быть навык работы с сетями, их создание, организация, настройка, защита. Именно этому навыку нас обучали на предприятии «ИМС-Тверь».

Во время прохождения практики мы успешно настроили маршрутизатор Cisco ASA 5505, узнали новые понятия, вспомнили и закрепили уже пройденный нами материал, ознакомились с тем, как осуществляется защита сетей на предприятиях, в офисах и попробовали сами её обеспечить. Мы создали веб-сервер, настроили его и получили доступ к нему из внешней сети, так как он был создан в ДМЗ. Помимо этого, мы воспользовались консолью управления Microsoft Management Console для получения опыта администрирования учетных записей при помощи оснасток.

# **Список использованных источников**

1. <http://www.cisco.com/c/ru_ru/products/security/firewalls/what-is-a-firewall.html>
2. <https://otvet.mail.ru/question/68018178>
3. <https://ru.wikipedia.org/wiki/DNS>
4. <https://ru.wikipedia.org/wiki/Transmission_Control_Protocol>
5. <https://refdb.ru/look/1470087.html>
6. <https://ru.wikipedia.org/wiki/Сокет_(программный_интерфейс)>
7. <https://ru.wikipedia.org/wiki/Сетевая_модель_OSI>
8. <https://ru.wikipedia.org/wiki/NAT>
9. <https://ru.wikipedia.org/wiki/DMZ_(компьютерные_сети)>
10. <https://technet.microsoft.com/ru-ru/library/hh505659.aspx>
11. <https://ru.wikipedia.org/wiki/PuTTY>
12. <http://rootadmin.org.ua/?p=210>