### Лабораторная №12,13

**Тема:** политика безопасности. Блокировка сайтов, настройка и установка плагинов. **Цель:** ознакомится с firewall (брандмауэр), научится настраивать под свои нужды и устанавливать блокировку сайтов функциями встроенного firewall «Брандмауэр Windows», а так же блокировать сайты инструментами Goole и Yandex.

Тип занятия: закрепление материала.

Оборудование: ПК, методические указания.



ЧПройдите в папку C:\Windows\System32\drivers\etc, поставьте отображение всех файлов в блокноте и откройте файл hosts (тот, который без расширения). Открывать с помощью блокнота!!!

1.сделайте ,чтобы vk.com был заблокирован

**2. сделайте редирект(перенаправление) 4pda.ru на сайт Яндекс-музыки**(или любое другое перенаправление сайтов)

Для того, чтобы узнать IP сайта

- 1. Откройте командную строку (В меню Пуск cmd)
- 2. Введите команду ping адрес\_сайта после чего нажмите Enter

адрес\_сайта смотреть в поисковой строке



#### Информация по команде PING

#### Команда PING - отправить эхо-запрос по протоколу ICMP на имя или IP-адрес целевого узла

Команда **PING** это, пожалуй, самая используемая сетевая утилита командной строки. **PING** присутствует во всех версиях всех операционных систем с поддержкой сети и является простым и удобным средством опроса узла по имени или его IP-адресу.

Для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений **ICMP**(Internet Control Message Protocol). Команда **ping** позволяет выполнить отправку управляющего сообщения типа **Echo Request** (тип равен 8 и указывается в заголовке ICMP-сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого icmp-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел дожжен отправить icmp-пакет с теми же данными, которые были приняты, и типом сообщения **Echo Reply** (код типа в ICMP-заголовке равен 0). Если при обмене icmp-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики.

Формат командной строки:

#### ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]] [-w таймаут] конечноеИмя

Параметры:

-t - Непрерывная отправка пакетов. Для завершения и вывода статистики используются комбинации клавиш Ctrl + Break (вывод статистики и продолжение), и Ctrl + C (вывод статистики и завершение).

-а - Определение адресов по именам узлов.

-п число - Число отправляемых эхо-запросов.

- І размер - Размер поля данных в байтах отправляемого запроса.

-f - Установка флага, запрещающего фрагментацию пакета.

-i TTL - Задание срока жизни пакета (поле "Time To Live").

-v TOS - Задание типа службы (поле "Type Of Service").

-г число - Запись маршрута для указанного числа переходов.

-з число - Штамп времени для указанного числа переходов.

-ј списокУзлов - Свободный выбор маршрута по списку узлов.

-к списокУзлов - Жесткий выбор маршрута по списку узлов.

-w таймаут - Максимальное время ожидания каждого ответа в миллисекундах.

Примеры использования:

ping google.com - эхо-запрос к узлу с именем google.com с параметрами по умолчанию количество пакетов равно 4, длина массива данных = 32 байта.

ping -6 ya.ru - пинг узла ya.ru с использованием протокола Ipv6

ping -a 192.168.1.50 - выполнить пинг с определением имени конесного узла по его адресу.

ping -s 192.168.0.1 computer - пинг узла computer от источника 192.168.0.1. Используется когда на компьютере имеется несколько сетевых интерфейсов.

ping w 5000 ya.ru - пинг с таймаутом ожидания равным 5 секунд ( по умолчанию — 4 сек). ping -n 5000 -l 1000 ab57.ru - опрос узла ab57.ru 5000 раз, пакетами с данными длиной в 1000байт. Допустимая максимальная длина данных — 65500.

ping -n 1 -l 3000 -f ya.ru - пинг с запретом фрагментации пакета.

ping -n 1-r 3 ya.ru - отправить 1 эхо-запрос на узел ya.ru с отображением первых 3-х переходов по маршруту.

ping -i 5 ya.ru - пинг с указанием времени жизни TTL=5. Если для достижения конечного узла потребуется большее количество переходов по маршруту, то маршрутизатор, прервавший доставку ответит сообщением "Превышен срок жизни (TTL) при передаче пакета."

<u>http://ab57.ru/cmdlist/ping.html</u> можно почитать подробней)

#### 3. Открываем файл хоста и вписываем замену

На первое место ставиться IP того, что откроется в место сайта <mark>4pda.ru</mark>, т.е. IP сайта яндекс музыки(213.180.204.186), далее через пробел или Tab пишем IP домена или название с которого, будет перенаправляться(<mark>4pda.ru</mark>).

hosts — Блокнот		3
<u>Ф</u> айл Правка Фор <u>м</u> а	т Вид Справка	
<pre># Copyright (c) #</pre>	1993-2009 Microsoft Corp.	
# This is a samp	ole HOSTS file used by Microsoft TCP/IP for Windows.	
<pre># This file cont # entry should b # be placed in t # The IP address # space. #</pre>	ains the mappings of IP addresses to host names. Each be kept on an individual line. The IP address should the first column followed by the corresponding host name. and the host name should be separated by at least one	
# Additionally, # lines or follo	comments (such as these) may be inserted on individual wing the machine name denoted by a '#' symbol.	
# # For example:		
# 102.54.94 # 38.25.63	1.97 rhino.acme.com # source server 3.10 x.acme.com # x client host	
# localhost name # 127.0.0. # ::1 127.0.0.1	e resolution is handled within DNS itself. 1 localhost localhost localhost	
#127.0.0.1 213.180.204.186 213.180.204.186	4pda.ru 4pda.ru www.4pda.ru	
#127.0.0.1 #127.0.0.1	vk.com velgame.ru	
127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1	www.nbproject.planyear.ru www.nbproject.yiibubl1.ru www.nbproject.yiibubl.ru www.framework.yiites.ru www.nbproject.yiites.ru www.subdomain.localhost www.nbproject.card1.ru www.subdomain.test1.ru	
<	4	

<u>Очень важный момент: большинство сайтов имеют как бы 2 адреса – с www и без www перед</u> именем домена, поэтому для полного перенаправления на другой сайт необходимо делать в файле hosts две записи – собственно, с www и без www. Выглядит это примерно так:

<u>77.88.21.11 vk.com</u> <u>77.88.21.11 www.vk.com</u>

# Блокировка сайт в брандмауэре(firewall) Windows

Встроенный фаервол «Брандмауэр Windows» в Windows 10, 8 и Windows 7 также позволяет заблокировать отдельные сайты, правда делает это по IP-адресу (который может меняться для сайта со временем).

Процесс блокировки будет выглядеть следующим образом:

**1.** Откройте командную строку и введите *ping адрес\_сайта* после чего нажмите Enter. Запишите IP-адрес, с которым ведется обмен пакетами.

2. Запустите брандмауэр Windows в режиме повышенной безопасности (можно использовать поиск Windows 10 и 8 для запуска, а

<mark>в 7-ке</mark> — <u>Панель управления — Система Безопасности — Брандмауэр Windows —</u> включение отключение брандмауэра <u>— Дополнительные параметры).</u>

1. Система Безопасности



#### **2.** Брэндмауэр Windows



3. Включите, если не включен у вас firewall



4. Вернитесь в предыдущее меню и выберете Разрешенные программы. Выберете те программы, которые вы хотите, чтобы запускались через firewall.



### 5. Вернитесь в предыдущее меню и выберете Дополнительные параметры

				1
🤆 🌖 👻 🖬 🕨 Панель управлени	я 🕨 Система и безопасность 🕨 Брандмауэр Windo	WS	<ul> <li>4) Поиск в панели упра \$</li> </ul>	,
Панель управления - домашняя страница	Защитите свой компьютер с помоц	цью брандмауэра Windows		
Разрешить запуск программы или компонента через	Брандмауэр Windows помогает предотвратить н вредоносных программ к этому компьютеру чер	несанкционированный доступ злоумышленников или рез Интернет или локальную сеть.		
брандмауэр Windows	Как брандмауэр помогает защитить компьютер	12		
Изменение параметров уведомлений	Дополнительные сведения о сетевых размещен	иях		
Включение и отключение брандмауэра Windows	Домашние или рабочие (ча ————————————————————————————————————	астные) сети Не подключено 🛞		
🥹 Восстановить умолчания	🛛 🔮 <u>О</u> бщественные сети	Подключено 🍙		
Дополнительные параметры	Сети в общественных местах, например, в аэр	опортах или кафе		
Устранение неполадок в сети	Company for a second second	Prove		
	Состояние орандмауэра windows:			
	входящие подключения.	включены в список разрешенных программ		
	Активные общественные сети:	<b>Г</b> еть 8		
		Неопознанная сеть		
	Состояние уведомления:	Уведомлять, когда брандмауэр Windows блокирует новую программу		
7				
Си. также				
Центр поддержки				
Центр управления сетями и общим доступом				

6. В открывшемся окне и происходит настройка дополнительных параметров, таких, как правила подключения (можно создать свое) и профиль домена.

😥 Брандмауэр Windows в режиме г	повышенной безопасности	
<u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка		
🔐 Брандмауэр Windows в реж	Брандмауэр Windows в режиме повышенной безопасности (Локальный компью	Действия
<ul> <li>Правила для входящих под</li> <li>Правила для исходящего по</li> <li>Правила безопасности подк</li> <li>Наблюдение</li> </ul>	Брандмауэр Windows в режиме повышенной безопасности обеспечивает безопасн компьютеров, работающих под управлением OC Windows.	Брандмауэр Windows в режиме повышенной безопас Импортировать политику Политика экспорта
	Обзор	Восстановить политику по умолчанию
	Профиль домена	Диагностика / восстановление
	🧭 Брандмауэр Windows включен.	Вид
	Входящие подключения, не соответствующие ни одному правилу, запрещены.	О Обновить
	Исходящие подключения, не соответствующие ни одному правилу, разрешены.	 []] Свойства
	Частный профиль           Врандмаузр Windows включен.           Входящие подключения, не соответствующие ни одному правилу, запрещены.           Исходящие подключения, не соответствующие ни одному правилу, разрешены.	👔 Справка
	Общий профиль активен Брандмауэр Windows включен. Входящие подключения, не соответствующие ни одному правилу, запрещены. Исходящие подключения, не соответствующие ни одному правилу, разрешены. Свойства брандмауэра Windows	
	Приступая к работе Проверка подлинности при передаче данных между компью Создайте правила безопасности подключения, чтобы указать, как и когда выполняет подличности подключений между компьютерами и их защита с помощью протокола IP	
< )	Правила безопасности подключений Просмотр и создание правил брандмауэра Создайте правила брандмауэра, чтобы разрешить или запретить подключения к опре, или портан. Также ножно разрешить подключение, только если оно прошло проверку источникои является авторизованный пользователь, группа или компьютер. По умолч подключения блокируются, если они не соответствуют правилу, которое их блокируе •	
		1

# 7. Выбираем Правило входящих подключений и в окне Действия выбираем Создать правило



8. В Тип правила выбираем НАСТРАИВАЕМЫЕ, нажимаем далее

выоерите тип правила оранди	ауэра, которое треоуется создать.
<ul> <li>Тип правила</li> <li>Программа</li> <li>Протокол и порты</li> <li>Область</li> <li>Действие</li> <li>Профиль</li> <li>Имя</li> </ul>	Правило какого типа вы хотите создать?
	Подробнее о типах правил < Назад Далее > Отмен

Программа	
Укажите полный путь и имя исп	олняемого файла программы, которой соответствует данное правило.
Шаги:	
🕘 Тип правила	Применять это правило ко всем программам или к определенной программе?
Программа	Все программы
<ul> <li>Протокол и порты</li> <li>Область</li> </ul>	Правило применяется ко всем подключениям компьютера, отвечающим другим свойствам правила.
Действие	Путь программы:
Профиль	О <u>б</u> зор
● Имя	Пример: c:\path\program.exe %ProgramFiles%\prowser.exe
	Службы Настрои <u>т</u> ь Укажите службы, к которым применяется правило.
	Подробнее об указании программ < Назад Далее > Отмена

10.На вкладке Протокол и Порты, выбираем тип протокола Любой, нажимаем далее

🔗 Мастер создания правила	для нового входящего под	ключения	x
Протокол и порты			
Укажите протоколы и порты, к	которым применяется данное	е правило.	
Шаги:			
Тип правила	Укажите порты и прот	околы, к которым применяется это правило.	
🕘 Программа			
Протокол и порты	Тип протокола:	Любой 💌	
🛎 Область	Номер протокола:		
Действие			
🕘 Профиль	Локальный порт:	Все порты	
🕘 Имя			
		Пример: 80, 443, 5000-5010	
	удаленный порт.		
		Пример: 80, 443, 5000-5010	
	Параметры протокола	ICMP: Hactpouth	
		Haciporita	
	Дополнительные свед	ения о протоколах и портах	
		< Н <u>а</u> зад Дал <u>е</u> е > Отмена	

11.На вкладке <u>Область,</u> «<u>Укажите удаленные IP-адреса</u>, к которым применяется правило» отметьте пункт «<u>Указанные IP адреса</u>», затем нажмите «<u>Добавить» и добавьте IP-адрес сайта, который нужно заблокировать</u>., нажимаем далее

В нашем случае мы выбираем удаленный IP-адрес, нажимаем Добавить, в сплывающем окне указываем наш IP 4pda.ru (**104.20.42.23**), нажимаем окей

оандмауэр Windows в режиме повышенной без Правила для входящих подключений Правила для исходящего подключения	вила для входящих подключений Действия Правила для входя	ащих подключений
<ul> <li>Правила для исходящего подключения</li> <li>Правила безопасности подключения</li> <li>Наблюдение</li> <li>Мастер создания п</li> <li>Область</li> <li>Укажите локальный и у</li> <li>Шаги:         <ul> <li>Тип правила</li> <li>Протокол и порты</li> <li>Область</li> <li>Действие</li> <li>Профиль</li> <li>Имя</li> </ul> </li> </ul>	руппа провила для создать правиле правила для ПР-адрес укажите IP-адреса для соответствия: () IP-адрес или подсеть: 104.20.42.23 Примеры: 192.168.0.12 192.168.1.0/24 2002:9d3b:1a31:4:208:74ff:fe39:6c43 2002:9d3b:1a31:4:208:74ff:fe39:0/112 Диапазон IP-адресов: с: по: 3аранее заданный набор компьютеров: Основной шлюз Дополнительные сведения об указании IP-адресов ОК Отмена () Указанные IP-адреса:	Аданное правило. Добавить Изменить Удалить Аанное правило. Аобавить Изменить Удалить Аданное правило.

# 12.На вкладке <u>Действие</u>, выбираем <u>Блокировать подключение</u>

	Мастер создания правила для нового входящего подключения				
Д	ействие				
Ук	ажите действие, выполняем	ое при соответствии подключения условиям, заданным в данном правиле.			
W	аги:				
۲	Тип правила	Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.			
۲	Программа				
۲	Протокол и порты	Включая как подключения, защищенные IPSec, так и подключения без защиты.			
۲	Область	Разрешить безопасное подключение			
۲	Действие	Включая только подключения с проверкой подлинности с помощью IPSec.			
۲	Профиль	Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.			
۲	Имя	Настроить			
		Блокировать подключение			
		Подробнее о действиях			
		< Н <u>а</u> зад Дал <u>е</u> е > Отмена			

## 13.На вкладке <u>Профиль</u>, оставляем все без изменений, нажимаем Далее

Мастер создания правила для нового входящего подключения				
Профиль Укажите профили, к которым применяется это правило.				
	• · · · · · · · · · · · • • • · · · · ·			
Шаги:				
🧶 Тип правила	Для каких профилей применяется правило?			
Программа				
Протокол и порты	✓ Доменный			
🕘 Область	Применяется при подключении компьютера к домену своеи организации.			
Действие	✓ Частный			
🕘 Профиль				
● Имя	Публичный Применается при подключении компьютера к общественной сети.			
	приненяется при подключении контвютера к общественной сети.			
	Подробнее о профилях			
	< <u>На</u> зад <u>Далее</u> > Отмена			

## 14. На вкладке <u>Имя</u>, задаем <u>название и краткую инфу, нажимаем готово.</u>

💣 Мастер создания правила	для нового входящего подключения	×			
Имя					
Укажите имя и описание данного правила.					
Шаги:					
🕘 Тип правила					
Программа					
Протокол и порты	14				
Область	4pda				
Действие					
Профиль	Описание (необязательно): информационный сайт				
🧶 Имя					
	< Н <u>а</u> зад <u>Г</u> отово Отм	ена			
1					

## <mark>B windows 10</mark>

1. В поиск вводим «брандмауэр» и выбираем в Режиме повышенной безопасности



2. Выберите пункт «Правила для исходящего подключения» и нажмите «Создать правило».

🔗 Брандмауэр Windows в режиме повышенн	- 🗆 ×	
<u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка		
🗢 🌩 🖄 📰 🗟 🖬		
<ul> <li>Брандмауэр Windows в режиме повышенно</li> <li>Правила для входящих подключений</li> <li>Правила для исходящего подключения</li> <li>Правила безопасности подключения</li> <li>Наблюдение</li> </ul>	Правила для исход Имя © @{Microsoft.Bin © @{Microsoft.Bin © @{Microsoft.Bin © @{Microsoft.Cor © @{Microsoft.Cor © @{Microsoft.Cor © @{Microsoft.Cor © @{Microsoft.Cor	Действия         Правила для исходящего подключен         Создать правило         Фильтровать по профилю         Фильтровать по состоянию         Фильтровать по состоянию         Фильтровать по группе         Вид         Обновить         Экспортировать список
< >	< @{Microsoft.Win v	Справка

### 3. Укажите «Настраиваемые»

_	••••••		
1	Мастер создания правила для нового исходящего подключения		
T	ип правила		
B	ыберите тип правила брандма	вузра, которое требуется создать.	
ш	аги:		
۲	Тип правила	Правило какого типа вы хотите создать?	
۲	Программа	O <b>R</b>	
•	Протокол и порты		
۲	Область	правило, управляющее подключениями для программы.	
۲	Действие	○ Для порта	
۲	Профиль	Правило, управляющее подключениями для порта TCP или UDP.	
۲	Имя	○ Предопределенные	
		BranchCache - клиент размещенного кэша (используется HTTPS) 💛	
		Правило, управляющее подключениями для операций Windows.	
		• Настраиваемые	
		Настраиваемое правило.	
			_
		< Н <u>а</u> зад Дал <u>е</u> е > Отмена	

# 4. В следующем окне выберите «Все программы».

4	💡 Мастер создания прави	а для нового исходящего п	одключения	×				
П	Ірограмма							
Уı	кажите полный путь и имя и	юлняемого файла программы	ы, которой соответствует данное правило.					
Ш	апи:							
۲	Тип правила Применять это правило ко всем программам или к определенной программе?							
٠	Программа							
۲	Протокол и порты	<u>В</u> се программы						
۲	Область Правило применяется ко всем подключениям компьютера, отвечающим другим свойствам правила.							
۲	Действие		<b>`</b>					
۲	Профиль			Ofison				
•	Имя	Пример: с:\¢ %Рг	Пример: c:\path\program.exe %ProgramFiles%\browser\browser.exe					
		Службы	Службы Настроить					
	У	Укажите службы, к ко	оторым применяется правило. < Н <u>а</u> зад Да	л <u>е</u> е > Отмена				

5. В окне «Протокол и порты не изменяйте настроек.

6. В окне «Область» в разделе «Укажите удаленные IP-адреса, к которым применяется правило» отметьте пункт «Указанные IP адреса», затем нажмите «Добавить» и добавьте IP-адрес сайта, который нужно заблокировать(104.20.42.23).

Нажмите ОК, там же можно задавать сразу несколько IP-сайтов для блокировки, просто перечислить списком нужно.

🔗 Мастер создания правила для нового исходящего подкл			и IP-адрес			×
Область			Укажите IP-адреса для соответствия:			
Укажите локальный и удаленный IP-адреса, к которым применяе			۲	IP-адрес или подсеть:		
ш	аги:					
۲	Тип правила			Примеры: 192.168.0.12 192.168.1.0/24		
۲	Программа	Укажите локальные IP-		2002:9d3b:1a31:4:208:74ff.fe39:6c43 2002:9d3b:1a31:4:208:74ff.fe39:0/112		
۲	Протокол и порты	Элюбой IP-адрес				
۲	Область	Указанные IP-адреса:	0	Диапазон IP-адресов:		
۲	Действие			c:		
۲	Профиль			по:		
۲	Имя		0	Sanauge sanauuulik uafan kompuntenas		
				Основной шлюз		
		Настройка типов интерфей				
		правило: Укажите удаленные IP-				
		О Любой IP-адрес		OIN OINICIA		
				Побавить		
				Изменить		
				Удалить		
						_
				< Назад Далее > Отм	ена	

#### 7. В окне «Действие» укажите «Блокировать подключение».

💣 Мастер создания прав	ила для нового исходящего подключения	×			
Действие					
Укажите действие, выполня	емое при соответствии подключения условиям, заданным в данном правиле.				
Шаги:					
<ul><li>Тип правила</li><li>Программа</li></ul>	Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.				
<ul><li>Протокол и порты</li><li>Область</li></ul>	О <u>парешить подключения</u> , защищенные IPSec, так и подключения без защиты.				
Действие	Разрешить безопасное подключение				
<ul> <li>Профиль</li> <li>Имя</li> </ul>	Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений. <u>Настроить</u> <b>Блокировать подключение</b>				
	< Н <u>а</u> зад Дал <u>е</u> е > Отмен	13			

- 8. В окне «Профиль» оставьте отмеченными все пункты.
- 9. В окне «Имя» назовите свое правило (название на ваше усмотрение), описание не обязательно и нажмите ГОТОВО.

На этом все: сохраните правило и теперь брандмауэр Windows будет блокировать сайт по IP-адресу, при попытке открыть его.

# В браузерах

В Chrome нельзя заблокировать ресурсы штатными средствами. Для этого необходима установка дополнительных расширений. Поэтому этот способ подойдет для интернет-обозревателей, поддерживающих установку дополнений.

# <u>Дополнительное задание</u>

# Блокировка сайта в Google Chrome

Здесь рассмотрим, как заблокировать сайт в Google Chrome, хотя этот способ подойдет и для других браузеров с поддержкой расширений. В магазине Chrome для этой цели есть специальное расширение Block Site.

Для этого:

#### 1. Открываете Google Chrome нажимаете <u>Сервисы</u>

Новая вкладка	×							🤔 Виталий	_ 0 <mark>_</mark> ×
$\leftarrow \rightarrow \mathbf{G} \ \overline{\mathbf{O}} \ \mathbf{O}$								©্র	z 🚭 🗉
🔢 Сервисы 🝐 Google Диси	🙀 анекдотов.net - анекд 🕎 vk.com 🥀 Фильмы rutracker 201	🧉 Музыка Yandex 🕨 Адаптиров	анные книг						Другие закладк
Позаять сервной			Goo	oale		Почта	Картинки		0 8
		Введите поисковый :	запрос или URL	<ul> <li>Украина</li> <li>LadyBug Admin   Lo</li> </ul>	Читать книги онла				
				•	A constraint of the second sec				
		Secure12 Slack	YouTube	<ul> <li>Яндекс. Музыка</li> <li>Видекс музыка</li> </ul>	phpMyAdmin phpMyAdmin magnetic ma				
📵 🚞 🚾	🍋 💽 🖻 🍇 🛷						en 🕐 🍷	- 10 🌬	<b>♦</b> 16:58

#### 2.В интернет-магазине в Google Chrome вводите block site

Скачайте один из сервисов(расширений для хрома) и заблокируйте доступ к любому из сайтов и предоставите скрин заблокированного сайта!!!!



После установки расширения, вы можете получить доступ к его настройкам через правый клик в любом месте открытой страницы в Google Chrome, или же в правом углу меню настроек goole Chrome .

После установки расширения выполните следующие действия:

- 1. Заблокируйте доступ по времени и дням недели.
- 2. Установите пароль на изменение параметров блокировки (в разделе «убрать защиту»).
- **3.** заблокируйте сайта по адресу, если такое предусмотрено в расширении (и перенаправление на любой другой сайт при попытке входа на указанный.
- 4. заблокируйте слов (если слово встречается в адресе сайта, он будет заблокирован).

# Блокировка рекламы в Google Chrome

- 1. Открываете Google Chrome нажимаете Сервисы
- 2. В интернет-магазине в Google Chrome вводите adblock, устанавливаете расширения для Goole и реклама у вас на всех сайтах будет заблокирована.

- 1. В каких случаях может не пройти перенаправление(редирект) сайта через файл hosts?
- 2. Для чего нужен firewall?
- 3. Как определить IP адрес сайта?
- 4. В каких случаях используют правила исходящих подключений, а в каких исходящих подключений?
- 5. Как добавить новое правило и заблокировать определенный IP адрес?
- 6. Сколько IP адресов можно блокировать одновременно?
- 7. Можно ли блокировать IP адреса в определённом диапазон? Если да, то как?
- 8. Что делает команда ping?
- 9. Как установить расширение для блокировки страниц в goole Chrome? 10.

### Список использованных источников:

- 1. <u>http://studydoc.ru/doc/178007/laboratornaya-rabota.-sistemnyj-reestr-windows</u>
- 2. http://ab57.ru/reestr.html
- 3. <u>http://remontka.pro/block-website/</u>
- 4. <u>https://windows-9.net/kak-nastroit-brandmauer-windows-7.html</u>

### Содержание отчета:

- 1. Тема, цель лабораторной работы
- 2. Поэтапное описание выполнения лабораторной работы
- 3. Скриншоты выполнения и результирующий скриншот экрана
- 4. Краткие ответы на контрольные вопросы
- 5. Выводы