**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ**

**УТВЕРЖДАЮ**
Заведующий кафедрой

_____

«___»_____20__ г.

# Методическая разработка и указания к лабораторной работе по дисциплине «Информационные технологии в управлении»

для студентов направления– 38.03.04 «Государственное и муниципальное управление»
(для всех профилей подготовки)

***Лабораторная работа №3***
***Процедура настройки Брандмауэра в Windows 7***

Рассмотрено УМК
«___» _____20__ г.
Протокол №____
Председатель УМК
_____

**Ставрополь, 2022 г.**

Рецензент:
доктор технических наук, профессор Федоренко В.В.

Одобрено учебно-методической комиссией экономического факультета Ставропольского государственного аграрного университета

Методические указания к лабораторной работе разработаны в соответствии с программой курса «Информационные технологии в управлении» и предназначены для студентов направления – 38.03.04 «Государственное и муниципальное управление» (для всех профилей подготовки)

Составитель:
Доцент, к.т.н. Рачков В.Е.

**СОДЕРЖАНИЕ:**

1. Меры безопасности при работе на компьютере…… 4
2. Введение…… 5
3. Процедура настройки брандмауэра PC с ОС Windows 7……. 6
4. Архивация данных и восстановление ОС Windows 7……..……. 22
5. Лабораторная работа №3 ……. 12
6. Приложение А……..……..13

## *1.* Меры безопасности при работе на компьютере

Конструкция компьютера обеспечивает электробезопасность для работающего на нем человека. Тем не менее, компьютер является электрическим устройством, работающим от сети переменного тока напряжением 220 В., а в мониторе напряжение, подаваемое на кинескоп, достигает нескольких десятков киловольт. Чтобы предотвратить возможность поражения электрическим током, возникновения пожара и выхода из строя самого компьютера при работе и техническом обслуживании компьютера необходимо соблюдать следующие меры предосторожности:

- сетевые розетки, от которых питается компьютер, должны соответствовать вилкам кабелей электропитания компьютера;
- запрещается использовать в качестве заземления водопроводные и газовые трубы, радиаторы и другие узлы парового отопления;
- запрещается во время работы компьютера отключать и подключать разъемы соединительных кабелей;
- запрещается снимать крышку системного блока и производить любые операции внутри корпуса до полного отключения системного блока от электропитания;
- запрещается разбирать монитор и пытаться самостоятельно устранять неисправности (опасные для жизни высокие напряжения на элементах схемы монитора сохраняются длительное время после отключения электропитания);
- запрещается закрывать вентиляционные отверстия на корпусе системного блока и монитора посторонними предметами во избежание перегрева элементов расположенных внутри этих устройств;
- повторное включение компьютера рекомендуется производить не ранее, чем через 20 секунд после выключения.

## *2.* Введение

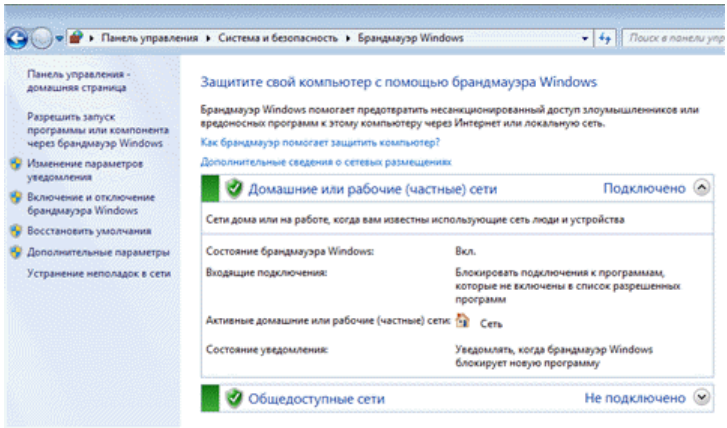
В лабораторную работу включены задания по тематике имеющей непосредственное отношение к вопросам защиты информации.

Лабораторная работа предполагает отработку двух ключевых вопросов:

1. Изучение процедур настройки брандмауэра PC с ОС Windows 7
2. Реализация процедур настройки брандмауэра PC с ОС Windows 7.

## *3.* Процедуры настройки брандмауэра PC с ОС Windows 7

Брандмауэр Windows 7 препятствует несанкционированному доступу вредоносных программ из Интернета и локальной сети. В частности, встроенный брандмауэр успешно защищал предыдущие ОС Windows от проникновения червей MSBlast и Sasser, известных своим эпидемическим распространением. Если вы используете сторонний фаервол – уровень защиты значительно выше. В противном случае, встроенный брандмауэр должен быть включен.




Запуск из командной строки или окна Выполнить (WIN+R): control.exe /name Microsoft.WindowsFirewall

***Изменения в брандмауэре Windows***

В брандмауэре Windows 7 произошел ряд изменений, в первую очередь функциональных.

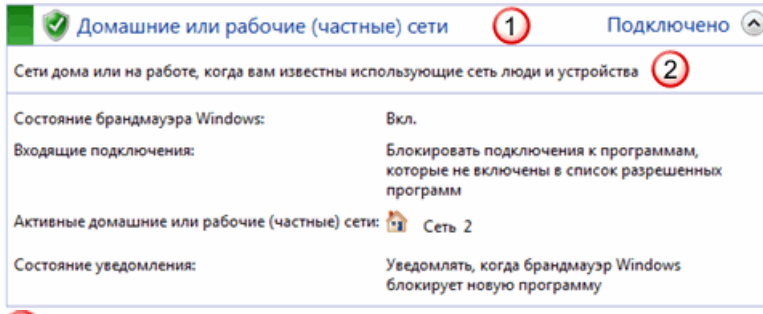
Основным нововведением брандмауэра Windows 7 является одновременная работа нескольких **сетевых профилей**.

- общий - публичные (общедоступные) сети, например, в кафе или аэропорту;
- частный - домашние или рабочие сети;
- доменный - доменная сеть в организации, определяемая автоматически.

В Windows Vista только один профиль мог быть активен в любой момент времени. Если было включено несколько профилей, наиболее безопасный из них становился активным. Например, при одновременном подключении к публичной и домашней сетям, активным становился общедоступный профиль, обеспечивающий более высокую безопасность. В Windows 7 все три профиля могут быть активны одновременно, обеспечивая соответствующий уровень безопасности для каждой сети.

***Изменения в пользовательском интерфейсе***

Пользовательский интерфейс брандмауэра в панели управления стал более информативным.




1 Четко обозначается профиль и его состояние

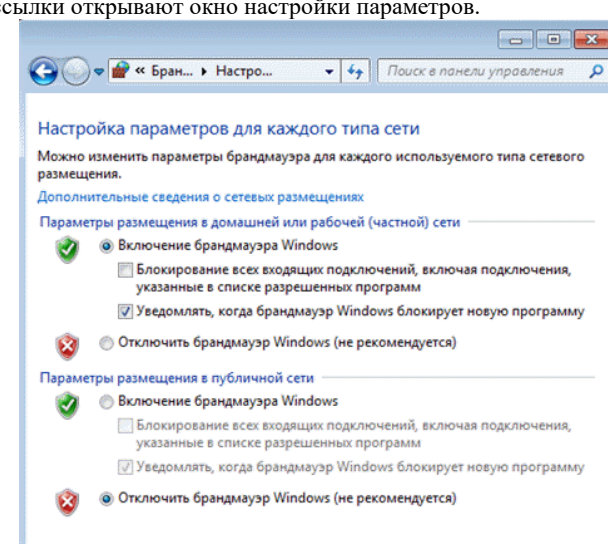
2 Приводится описание профиля

***Настройка параметров брандмауэра***

В левой панели присутствуют две ссылки:

- изменение параметров уведомления;
- включение и отключение брандмауэра Windows.

Обе ссылки открывают окно настройки параметров.




Для каждого профиля можно задать собственный набор параметров. Если брандмауэр включен, логично также включить уведомления о блокировке новой

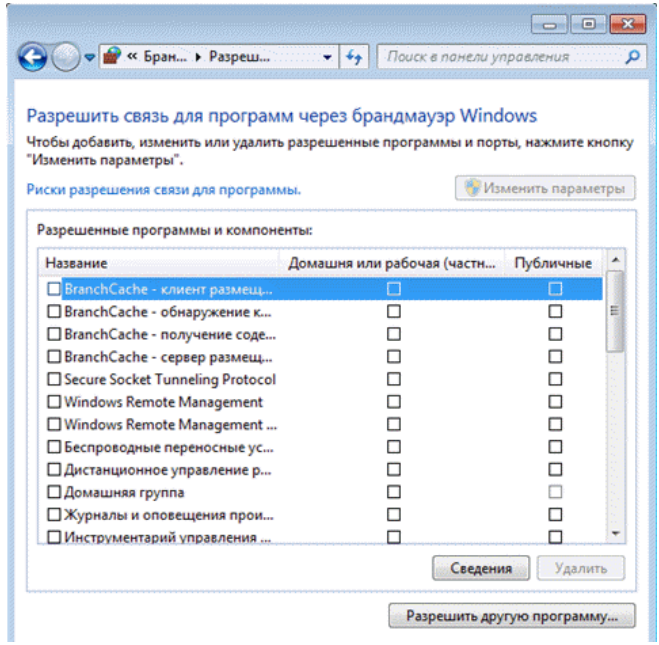
программы, чтобы ее поведение не вызывало у вас недоумения в случае блокировки. В диалоговом окне блокировки также имеется возможность разрешить или заблокировать программу для каждого профиля.

### *Сброс настроек брандмауэра*

Чтобы восстановить стандартные значения брандмауэра, щелкните ***Восстановить умолчания*** в левой панели. В открывшемся окне подтвердите свое желание вернуть все в исходное положение.

### *Разрешение запуска программ и компонентов*

Брандмауэр Windows 7, конечно, включен по умолчанию, а его стандартные настройки подойдут большинству пользователей. Если вам требуется настроить разрешения для конкретной программы или компонента ОС, щелкните ***Разрешить запуск программы или компонента через брандмауэр*** Windows в левой панели и в открывшемся окне нажмите кнопку ***Изменить***.



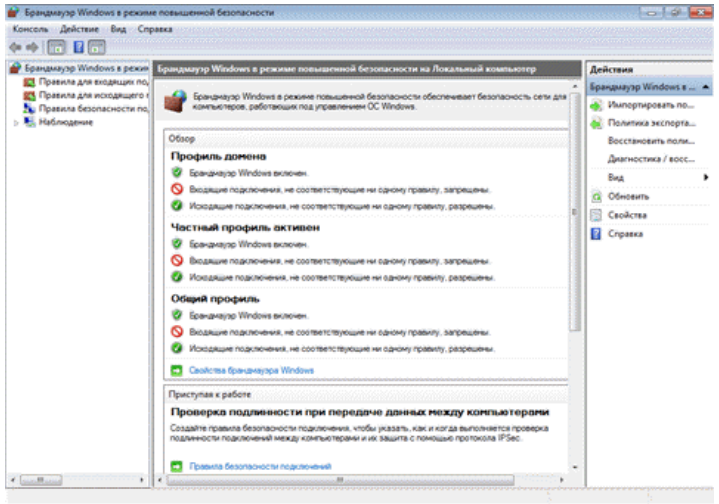

Щелкните необходимый компонент и установите разрешения для каждого профиля. Для добавления в список конкретной программы, нажмите кнопку ***Разрешить другую программу***.

### *Рекомендации по настройке*

Рекомендация по использованию брандмауэра Windows 7 очень проста - он должен быть включен всегда, если вы не используете сторонний фаервол. Тем самым вы обезопасите себя, например, от проникновения распространенных сетевых червей. В большинстве случаев домашним пользователям подойдут стандартные параметры брандмауэра. Если же вы используете сторонний фаервол, то при его установке встроенный брандмауэр, скорее всего, будет отключен, во избежание конфликтов между двумя программами, выполняющими одинаковую функцию.

### *Дополнительные параметры брандмауэра*

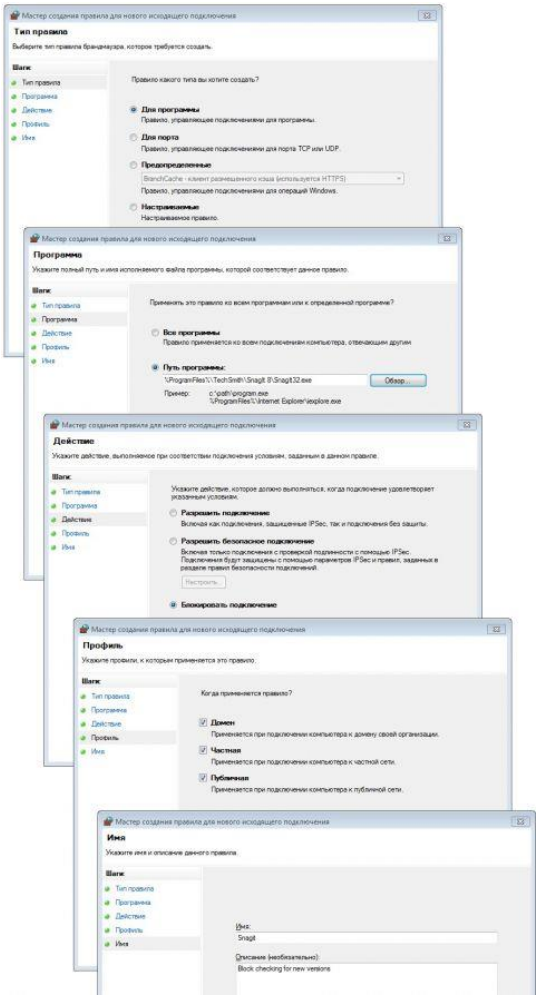
Если вас разочаровала скромность доступных настроек брандмауэра, не спешите огорчаться. У него есть расширенный режим, который реализован с помощью оснастки консоли управления Microsoft (MMC). В левой панели щелкните ***Дополнительные параметры*** и перед вами предстанетБрандмауэр Windows в режиме повышенной безопасности.




Запуск из командной строки или окна **Выполнить** (WIN+R): wf.msc

Элемент панели управления предназначен для домашних пользователей, а оснастка консоли MMC ориентирована на ИТ-специалистов. В режиме повышенной безопасности брандмауэр позволяет конфигурировать не только локальный компьютер, но и удаленные компьютеры и объекты групповой политики.

Для всех профилей уже существуют предустановленные наборы правил. Безусловно, вы можете изменить их или добавить собственные правила для входящих и исходящих подключений. Создание правил реализовано с помощью мастера. Например, чтобы заблокировать приложению доступ в Интернет, щелкните **Правила для исходящего подключения** в левой панели, а затем - Создать правило в правой панели. Мастер создания правил проведет вас через несколько этапов.

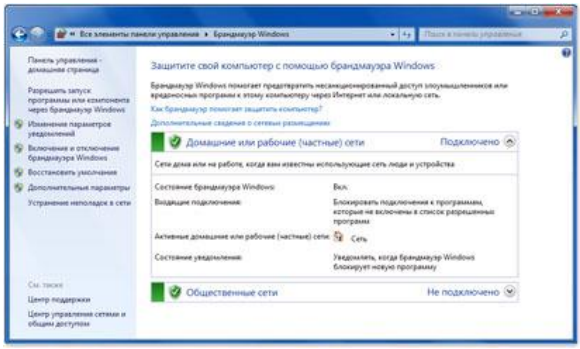


В брандмауэре Windows 7 произошло много изменений по сравнению с Windows Vista. Например, для каждого профиля фильтрация трафика возможна на основе:

- пользователей и групп службы каталогов Active Directory
- исходным и целевым IP-адресам
- IP-портам
- параметрам IPsec
- типам сетевых интерфейсов
- служб и т. д.

Работа брандмауэра подобна закрыванию на замок входной двери в доме: он защищает от проникновения внутрь непрошенных гостей (в нашем случае злоумышленников и вредоносных программ). БрандмауэрWindows в Windows 7 включен по умолчанию, поэтому его не требуется настраивать. Кроме того, он стал более гибким и удобным в использовании.

Теперь можно точно настроить требуемые параметры защиты и уведомлений для каждого профиля сети: домашней, рабочей и общедоступной. При подключении к общедоступной сети, например в библиотеке или кафе, можно блокировать все входящие подключения. При использовании дома или на рабочем месте данный параметр можно выключить. Профили можно легко переключать независимо от установленного для них уровня защиты.




Windows Брандмауэр можно настроить для обеспечения безопасности различных сетевых сред.

## *4. Лабораторная работа №3*
## *Процедуры настройки брандмауэра PC с ОС Windows 7*

**Цель работы:**

1. Изучить процедуры настройки брандмауэра PC с ОС Windows 7.
2. Привить навыки в настройке брандмауэра PC с ОС Windows 7 для различных профилей.

**Время:** 2 часа.

**Место проведения:** Компьютерный класс

**Методическое обеспечение работы:**

1. ПЭВМ с установленной операционной системой Windows 7.
2. Методические указания к выполнению лабораторной работы.

**Порядок проведения лабораторной работы**

***1. Изучить процедуры настройки брандмауэра PC с ОС Windows 7.***

Пользуясь сведениями, приведенными в параграфе 3 данной методической разработки, студенты, с использованием ПЭВМ, изучают процедуры настройки ***бр***андмауэра PC с ОС Windows 7.

***2. Получить навыки разработки алгоритма действий по настройки брандмауэра PC с ОС Windows 7 (45 минут).***

Пользуясь сведениями, приведенными в параграфе 3 данной методической разработки, студенты, с использованием ПЭВМ разрабатывают в приложении Microsoft PowerPoint алгоритм действий по настройке брандмауэра PC с ОС Windows 7 для различных профилей (в соответствии с вариантом).

3. Результаты работы оформляются в отчете к лабораторной работе и представляются преподавателю в ходе защиты (Приложение А).

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ**

# ОТЧЕТ

***о выполнении лабораторной работы***
***по дисциплине «Информационные технологии в управлении»***

**Тема лабораторного занятия:**

_____

_____

**Выполнил:**
_____
_____

**Дата выполнения:**
_____
_____

**Отметка о выполнении лабораторной работы:**
_____
_____

**Ставрополь, 2014**

## 1. Цель работы

## 2. Краткие теоретические сведения об объекте исследования

## 3. Результаты проделанной работы

(принципиальная схема, результаты измерений, графики, чертежи)

## 4. Выводы о проделанной работе

(Основные результаты, полученные в ходе исследований, соответствие их теории)