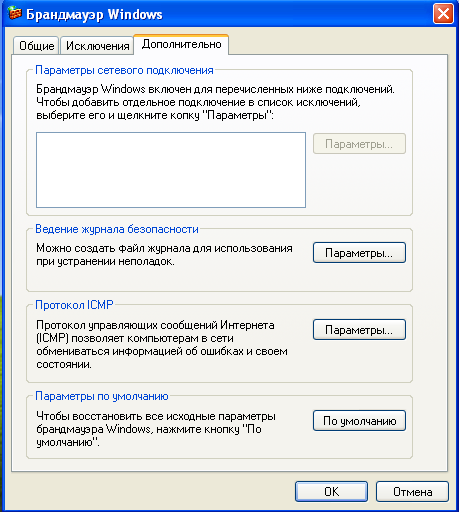
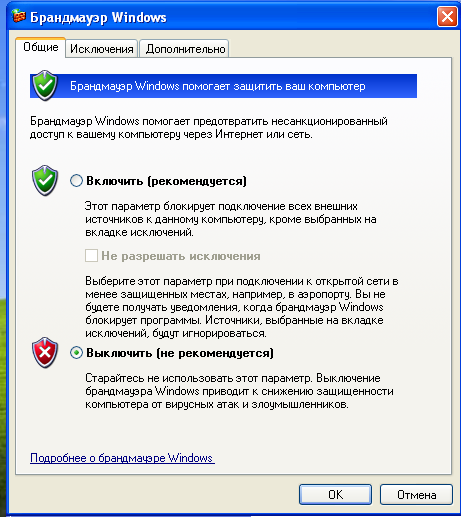
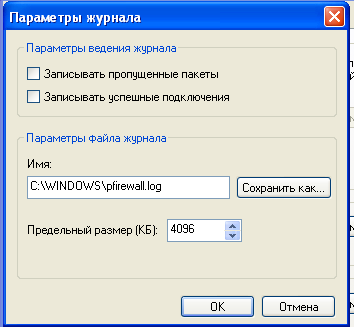
***Лабораторная работа №6. Защита от несанкционированного доступа и сетевых хакерских атак***

Задание №1. Брандмауэр Windows.

Включить брандмауэр Windows. Заходим в «‎Пуск», далее «‎Панель управления» и в ней выбираем «‎Брандмауэр Windows».

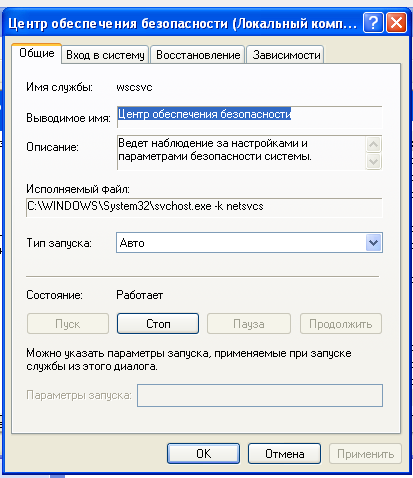


Включаем на вкладке «‎Общие». Добавляем исключения на вкладке «‎Исключения» и на вкладке «‎Дополнительно» можем изменять «‎Параметры сетевого подключения». Графа «‎Ведение журнала безопасности» необходима для того, чтобы выяснить, когда произошла неполадка и при каких обстоятельствах. Настроим его в соответствии с нашими запросами.

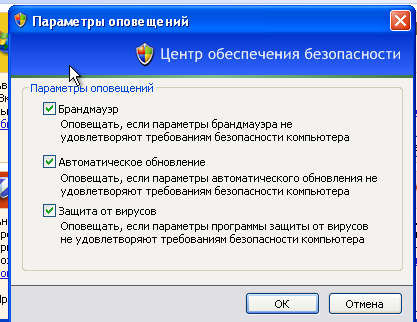
‎

Задание №2. Центр Обеспечения безопасности Windows.

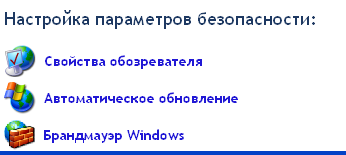
Заходим в «‎Пуск», далее «‎Панель управления» и в ней выбираем «‎Администрирование», «‎Службы». Находим «‎Центр обеспечения безопасности», дважды нажимаем и изменяем тип запуска на «‎Авто». Состояние должно быть «‎Работает». Нажимаем «‎Ок».



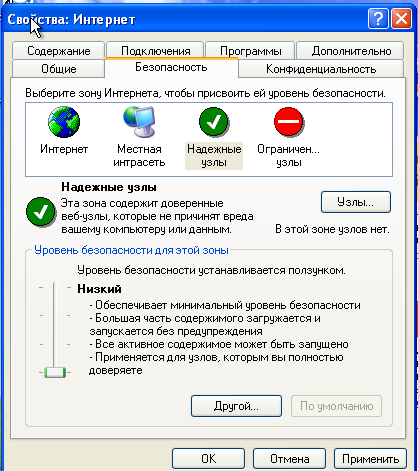
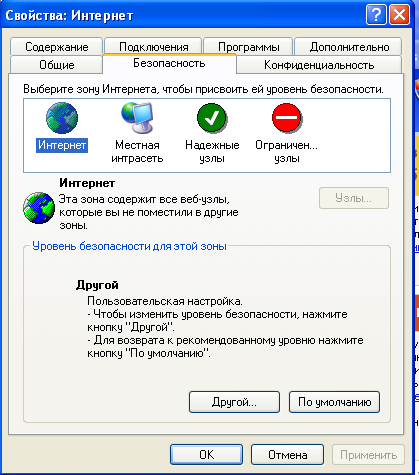
Заходим в «‎Пуск», далее «‎Панель управления» и в ней выбираем «‎Центр обеспечения безопасности». Для настройки оповещений слева необходимо нажать на «‎Изменить способ оповещения Центром обеспечения безопасности» и выбрать нужные параметры.



Разберемся со «‎Свойствами обозревателя» в нижней части окна «‎Центр обеспечения безопасности».



Здесь можно задавать безопасные узлы, менять уровень безопасности для каждой зоны.



Если в предыдущем меню выбрать «‎Автоматическое обновление», то откроется окно с редактированием автоматического обновления (логично).

