**Лабораторная работа №2**

**На тему: Настройка компьютера для безопасной работы с внешними носителями и в ИНТЕРНЕТ.**

**Студент:** Артюшов Андрей Геннадьевич

**Группа**: 3221

**Позиция в группе**: 1

# **Определение параметров компьютера**

Для определения наименования видеокарты, типа монитора, процессора, жестких дисков и других характеристик необходимо выбрать пункты в «Диспетчере устройств» (правой кнопкой меню «Пуск») (см. Рис. 1).

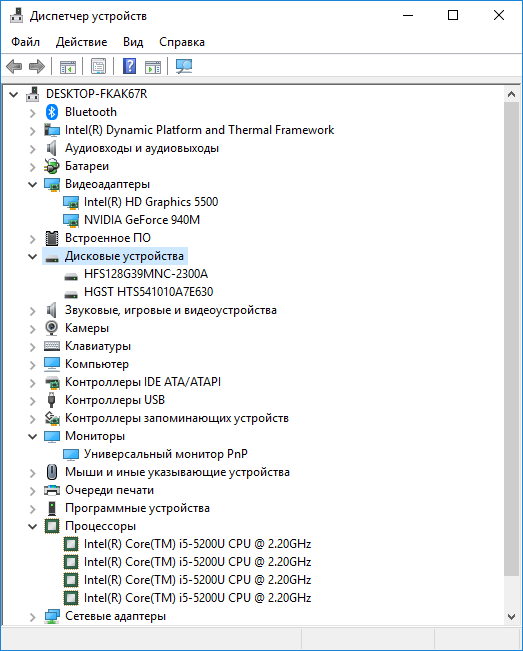


Рис. 1

Для того чтобы получить информацию о дисках, необходимо зайти в раздел “Управление дисками” (правой кнопкой меню «Пуск») (см. Рис. 2).

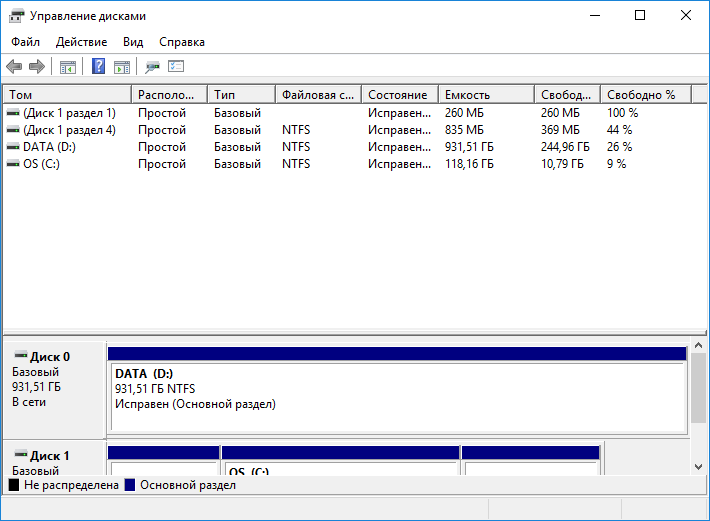


Рис. 2

Для того чтобы узнать тип системы необходимо зайти в раздел “Система” по нажатию правой кнопки мыши по “Пуск”, а дальше найти всю нужную информацию (см. Рис. 3)

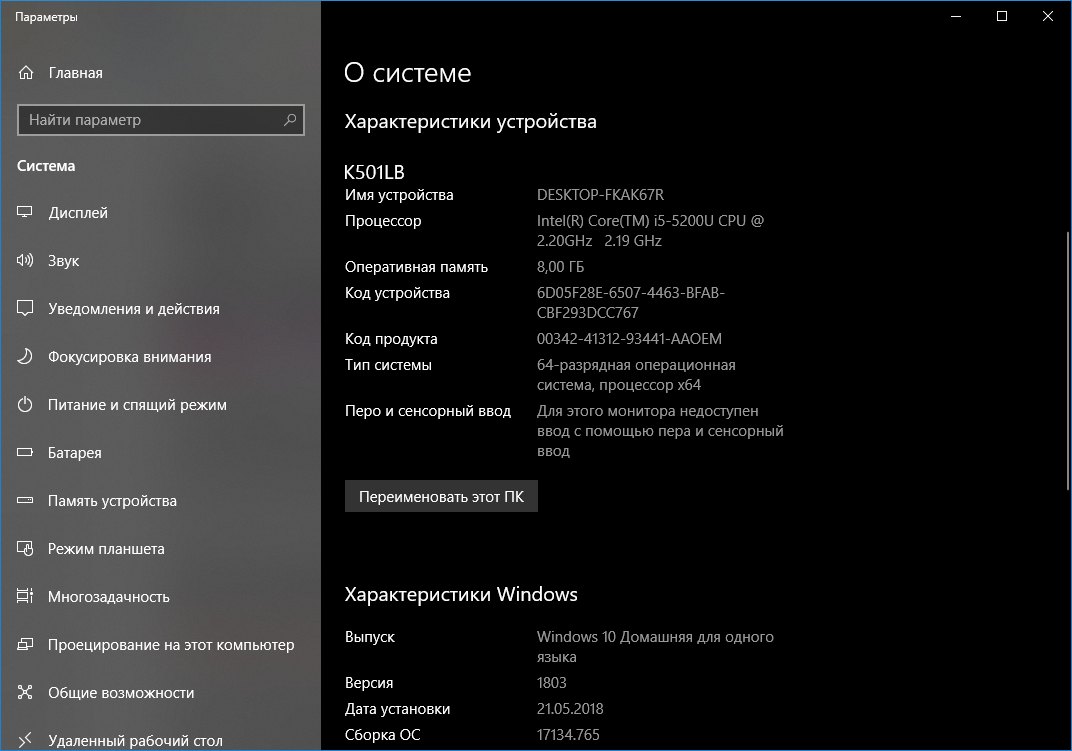


Рис. 3

Узнать количество ядер процессора можно в “Диспетчере задач”, для того чтобы вызвать это окно нужно воспользоваться комбинацией клавиш Ctrl+Shift+Esc; Далее зайти в раздел “Производительность”, и там будет нужная нам информация (см. Рис. 4).

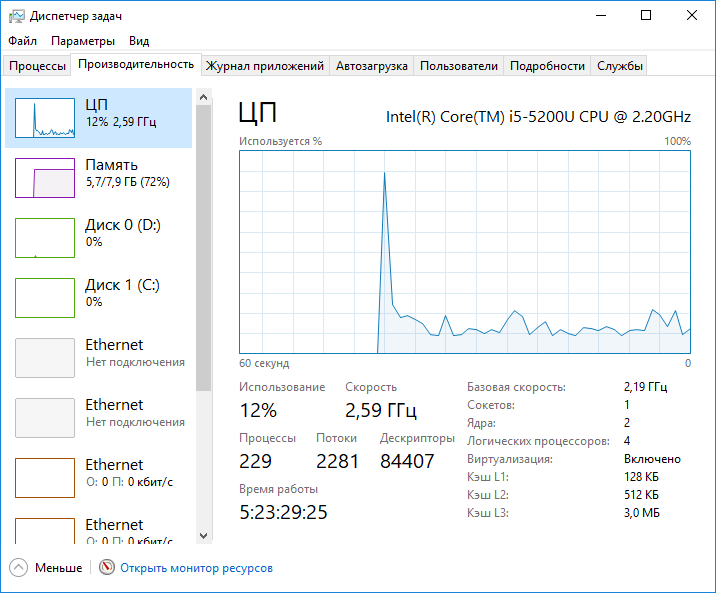


Рис. 4

# **Способы отключения автозапуска с любых носителей.**

## **Отключение программ в автозапуске**

Часто на компьютер попадают программы, установку которых мы порой даже не замечаем, а они в свою очередь добавляются в автозагрузку системы и нагружают ее, тем самым замедляя работу компьютера, это в лучшем случае. В плохом, эти программы могут представлять вредоносное ПО, которое может использовать ресурсы системы в чужих целях. Для того чтобы убрать или же добавить программу в автозапуск нам необходимо попасть в “диспетчер задач”, а далее в раздел “автозагрузки”. Далее можно увидеть перечень программ, которые запускаются вместе с запуском системы, чтобы отключить автозагрузку надо щёлкнуть по программе, затем нажать на кнопку “отключить” в нижней правой части диспетчера задач (см. Рис. 7).

При установке некоторых программ на компьютер, они автоматически добавляются в автозагрузку, чем сильно замедляют работу компьютера, при этом визуально они могут даже не отображаться, в том числе вредоносное ПО. Для отключения необходимо открыть «Диспетчер задач», а далее перейти в раздел автозагрузки. Там можно увидеть список программ, которые запускаются вместе с системой. Для того, чтобы отменить их автозагрузку, достаточно нажать на программу и выбрать «отключить» в нижней левой части панели (см. Рис 5).

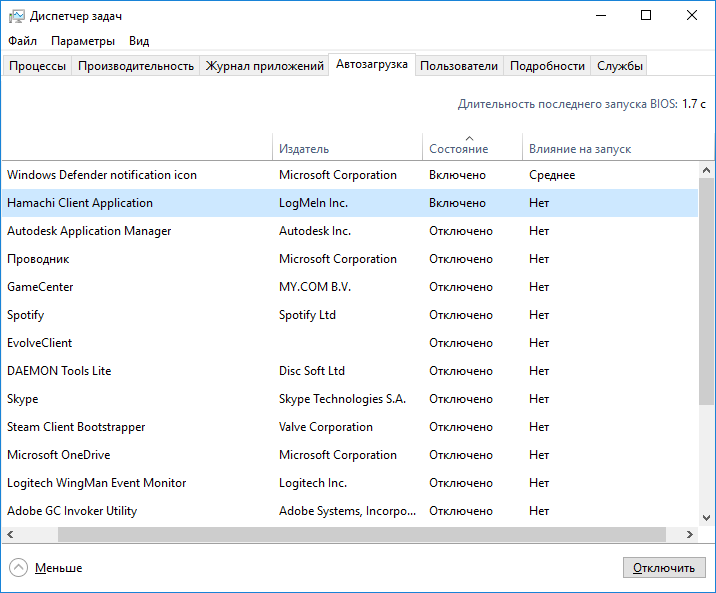


Рис. 5

## **Применение групповой политики gpedit.msc**

Перейдём в редактор локальной групповой политики. Для этого используем комбинацию клавиш Win+R и вводим gpedit.msc. Попав в окно, можно наблюдать огромное множество “действий”, которые выполняются системой (см. Рис. 6).

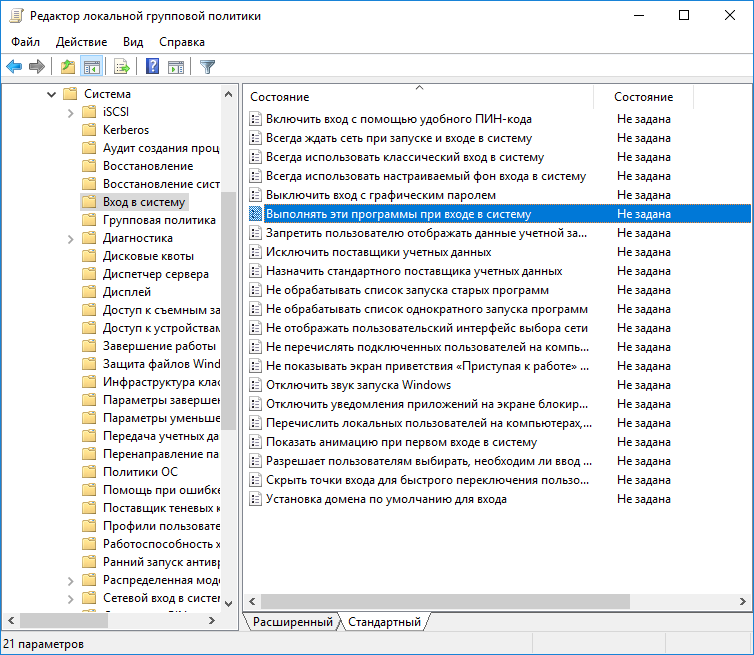


Рис. 6

Далее проведем анализ параметра “состояние” раздела “Выполнить эти программы при входе в систему”, по результатам которой оказалось, что в автозапуске отсутствуют программы за пускающиеся под управлением политик (см. Рис. 7).

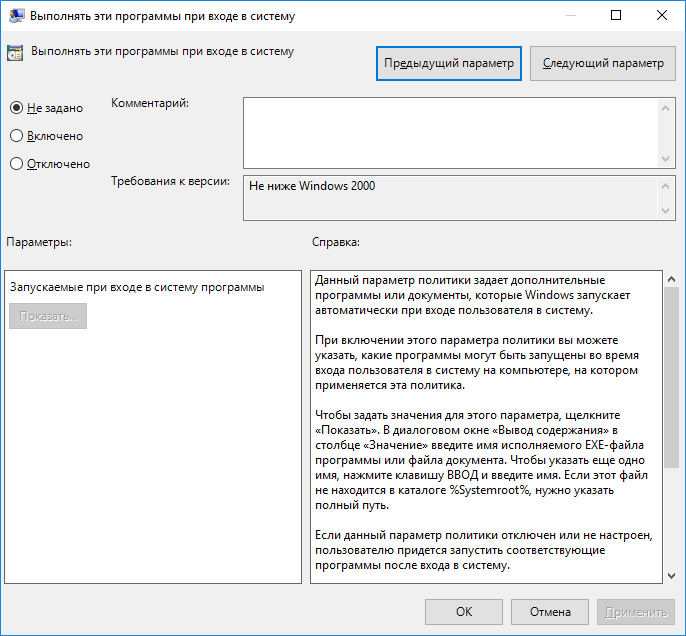


Рис. 7

## **Отключение автозапуска компакт-дисков, съемных дисков и флешек**

Отключение автозапуска подключаемых устройств крайне полезна в случае, если на носителе находится вредоносное ПО (см. Рис. 8).

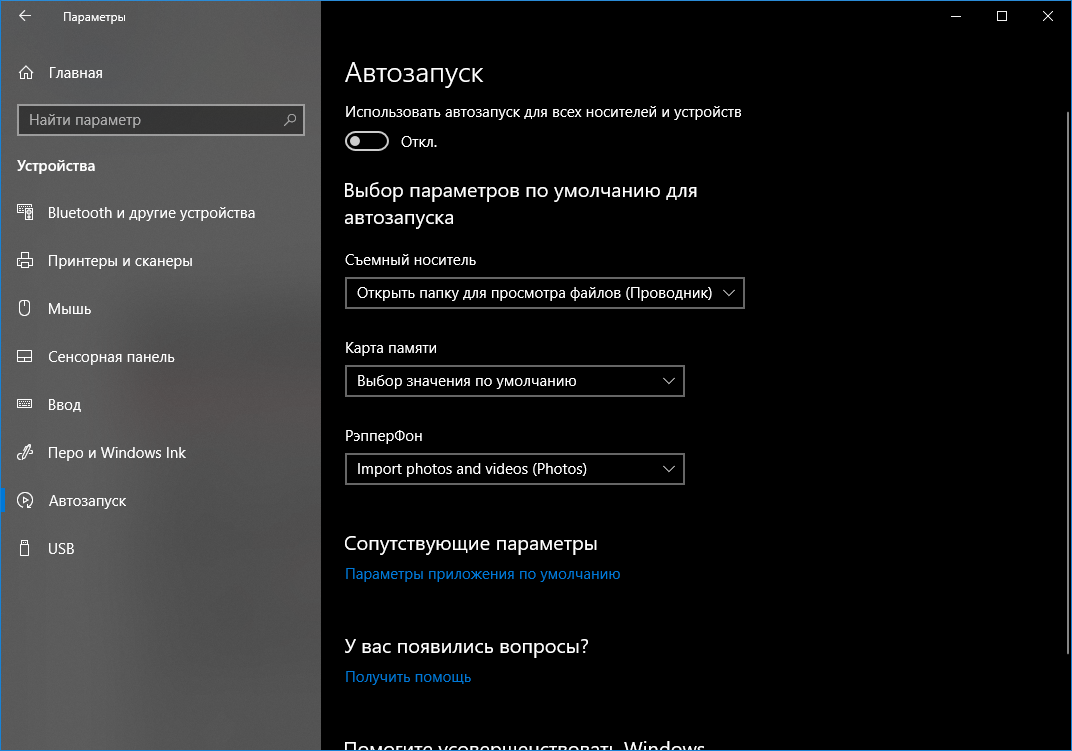


Рис.8

# **Способы блокирования файла Autorun.inf**

## **Создание неудаляющейся папки autorun.inf**

Для того чтобы вредоносное ПО не переходило на компьютер или, другими словами, не запускалось в автоматическом режиме, нужно создать неудаляющуюся папку autorun.inf на внешнем носителе. Чтобы создать такую папку, необходимо попасть в командную строку. Сделать это можно путем зажатия Shift и правого клика в проводнике, затем выбираем “Открыть окно команд” и в открывшейся командной строке написать “md autorun.inf\name..\” и нажать Enter (см. Рис. 9), после чего удалить такую папку без форматирования будет невозможно.

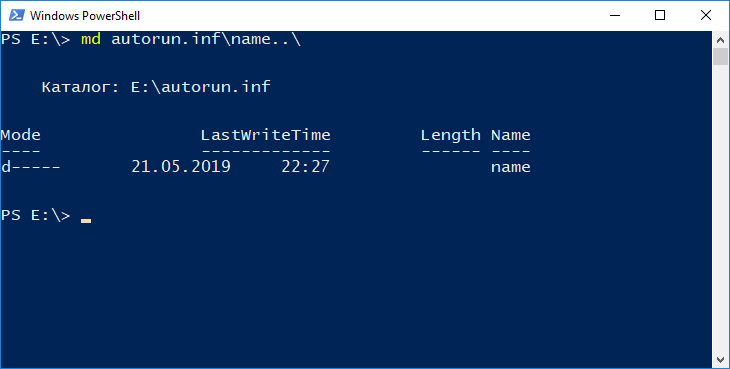


Рис. 9

Рис. 12

## **Блокирование с использованием Panda USB Vaccine**

Некоторые программы вредоносного характера работают путем изменения autorun.inf. Данная программа представляет из себя помощника по отключению автозапуска со всех внешних устройств (см. Рис. 10). На подключенном носителе создается файл, который не удаляется и не дает вирусной программе создать на носителе свой собственный файл запуска. Следует напомнить, что программа предоставляет защиту только от установки вредоносных-автозапускающихся программ, другой защиты она не предоставляет, но это не делает ее менее полезной.

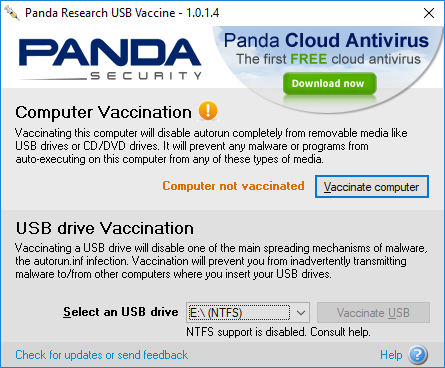


Рис. 10

# **Восстановление компьютера после блокирования вредоносными программами-вымогателями**

## **Создание диска восстановления**

Для создания диска восстановления нужно зайти в окно “Создание диска восстановления” для этого нажмите “Win+s” и введите “Создание диска восстановления”. Далее следуем указаниям (см. Рис. 11).

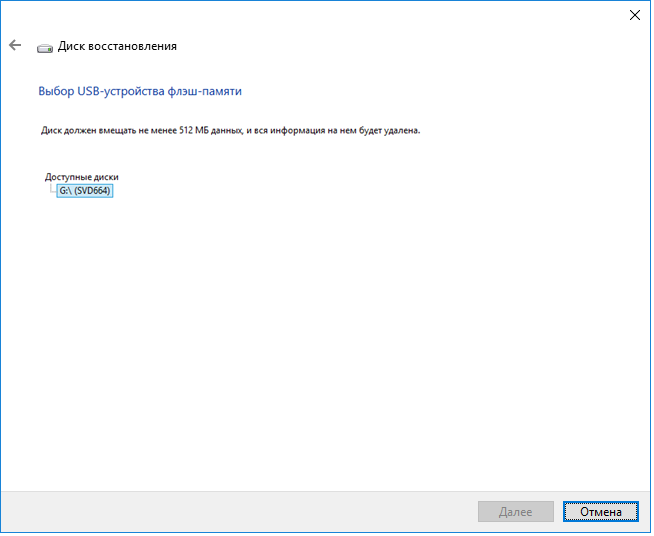


Рис. 11

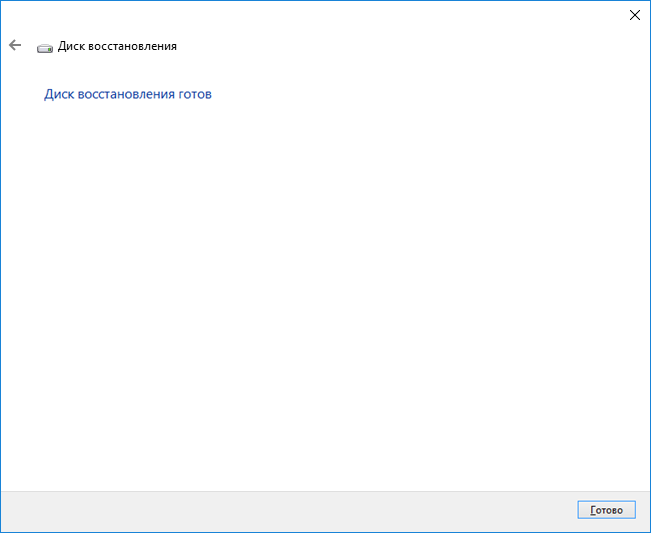


Рис. 12

## **Создание точки восстановления**

Точки восстановления Windows сохраняются системой на жестком диске компьютера. Под них выделяется определённая его часть, по мере заполнения диска более давние точки восстановления удаляются и на их место сохраняются новые. Создание точки восстановления дает возможность восстановить систему, путем отката изменений до места сохранения. Для создания точки восстановления необходимо нажать “Win+s” и ввести «Создание точки восстановления» (см. Рис. 13).

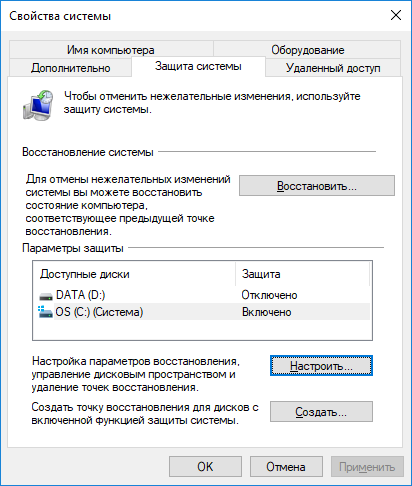


Рис. 13

## **Восстановление при помощи программы Kaspersky Rescue Disk**

Когда компьютер серьезно заражен вирусами, простая очистка при помощи антивирусного сканнера не всегда возможна. Иногда бывает, что система попросту не загружается, или тормозит настолько сильно, что проверка и удаление вирусов займет целую уйму времени. В таких ситуациях может помочь специальная антивирусная утилита – Kaspersky Rescue Disk. Данная программа представляет собой виртуальную оболочку, в которой вы сможете беспрепятственно запустить проверку компьютера на вирусы, а при необходимости также поработать со встроенным редактором реестра, файловым менеджером и веб-браузером.

Для начала нужно смонтировать USB загрузочный диск, для этого можно использовать программу Rufus (см. Рис. 14).

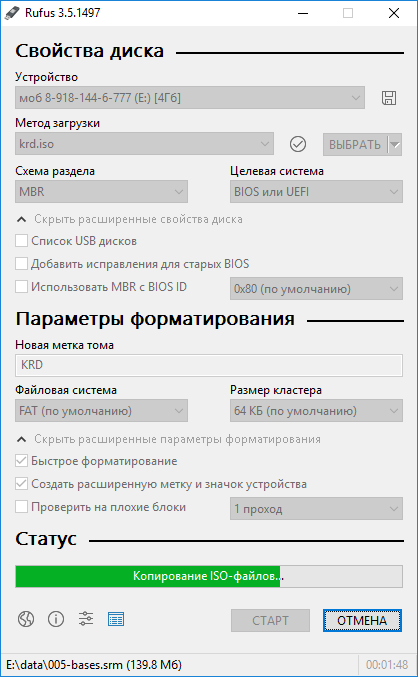


Рис. 14

Для запуска виртуальной оболочки первым делом нужно зайти в настройки BIOS на вашем компьютере и настроить загрузку с флешки. После этого запустится виртуальный рабочий стол Kaspersky Rescue Disk, с которого можно выполнить лечение компьютера от вирусов. Чтобы зайти в утилиту проверки на вирусы, щелкните по значку Kaspersky Rescue Disk. Также на рабочем столе имеются ярлык для входа в диспетчер файлов, ярлык запуска редактора реестра и веб-браузер. Для начала запуска лечащей утилиты щелкните на пункте выполнить проверку объектов (см. Рис. 19).

Рис. 19

После окончания восстановления системы перезагрузите компьютер и установите в BIOS загрузку с жесткого диска.