Цель работы:

Изучить и научиться настраивать изолированную программную среду (ИПС) на автономном автоматизированном рабочем месте (АРМ) пользователя средствами операционной системой Windows 7 для защиты информации от несанкционированного доступа (НСД).

Основные сведения:

Windows обладает достаточно обширным набором функций и утилит для изменения конфигурации и подключения новых устройств и ресурсов. С одной стороны, эти функции облегчают работу квалифицированному пользователю, но с другой - могут служить источником несанкционированного доступа (НСД). Защита информации от несанкционированного доступа НСД на каждом АРМ осуществляется индивидуально с учетом решаемых на нем задач и включает, в том числе, настройку изолированной (замкнутой) программной среды (ИПС) средствами ОС Windows.

Изолированная программная среда ИПС АРМ предназначена для ограничения возможностей пользователя по запуску программ, доступу к файлам, изменению параметров операционной системы (ОС). Настройка замкнутой программной среды обеспечивает возможность запуска только заданного набора программ и/или процессов для пользователя, т.е. исключает возможность запускать ему собственные, не разрешенные явно администратором, задачи.

Организация ИПС средствами ОС Windows осуществляется сокрытием от пользователя части элементов интерфейса путём присвоения параметрам реестра ОС определенных значений. При этом параметры реестра различных версий ОС Windows могут значительно различаться.

Редактор реестра содержит список его главных разделов (root keys, корневых ключей). Внутри них содержатся все значения реестра. Ниже приведен список с наиболее распространенными разделами и их содержимым (значениями).

- HKEY_CLASSES_ROOT (HKCR) – раздел, содержащий типы файлов, их расширения и OLE информацию.
- HKEY_CURRENT_USER (HKCU) – раздел, содержащий настройки текущего пользователя, вошедшего в Windows. Именно с ним осуществляться работа по настройке ППС.
- HKEY_LOCAL_MACHINE (HKLM) – раздел, содержащий конкретную информацию об установленном оборудовании, настройках программного обеспечения и другую информацию. Эти настройки используются для всех пользователей компьютера.

- HKEY_USERS (HKU) – раздел, содержащий информация обо всех пользователях компьютера (профилях).
- HKEY_CURRENT_CONFIG (HKCC) – раздел, содержащий подробности о текущей конфигурации аппаратных средств компьютера.

Структура реестра Windows строго иерархична и имеет четкое построение. Основная его составная часть – это ключи (или параметры), в которых и хранится вся информация (в нашем примере это ключ с названием «link»). Каждый параметр реестра Windows отвечает за определенное свойство системы. Ключи с данными о смежных настройках компьютера объединены в разделы, которые, в свою очередь, являются подразделами более крупных разделов и т.д.

Изменения в реестр вносятся путем создания определенных ключей и задания им нужных параметров, чтобы в результате была установлена ИПС.

Всего реестр позволяет выбирать из пяти типов параметров:

- REG_BINARY — тип двоичных параметров (Binary Value), которые представляют собой набор двоичных данных, доступных для редактирования только в шестнадцатеричном формате.
- REG_DWORD — тип параметра, имеющий числовое значение (DWORD Value), которое может задаваться либо в десятичном, либо в шестнадцатеричном формате.
- REG_SZ — тип параметра, значение которого задается в виде текстовой строки (String Value) фиксированной длины. Как правило, данный тип параметра содержит текст, который можно прочитать.
- REG_EXPAND_SZ — тип параметра, значение которого задается в виде строки данных переменной длины (Expandable String Value). Этот тип данных включает имена специальных переменных, обрабатываемых при использовании данных программой или службой. Когда программа или служба читает такую строку из реестра, то операционная система автоматически подставляет вместо имени специальной переменной ее текущее значение.
- REG_MULTI_SZ — тип параметра, значение которого задается в виде многострочного текста (Multi-String Value). К такому типу, как правило, относятся списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами.

Для применения параметра необходимо изменить установленное по умолчанию значение параметра «0» на «1».

Все политики безопасности настраиваются в соответствии с требованиями варианта № 8 (3Б).

Класс защищенности 3Б предназначен для АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Требования к классу защищенности 3Б:

Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Выполнение работы:

Для начала работы с реестром нужно зайти в редактор реестра. Для этого с помощью комбинации клавиш «Win + R» вызовем утилиту «Выполнить» и введём команду «regedit» (рис. 1).

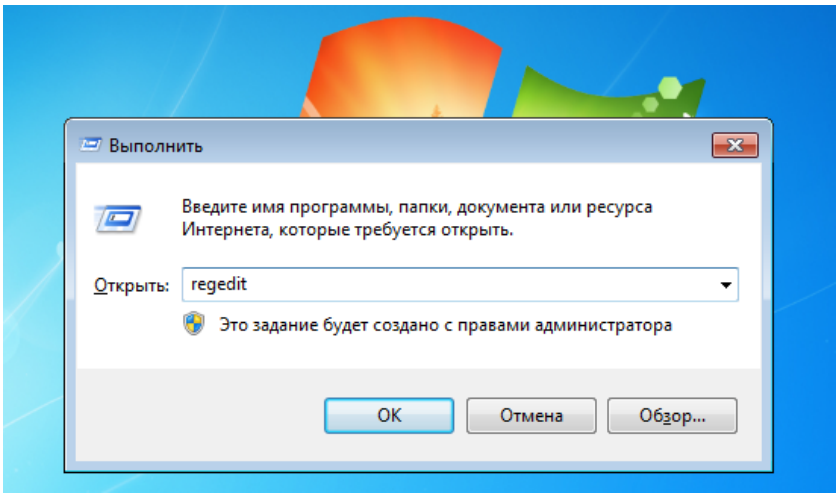

Рис.1 – вызов редактора реестра

Для работы нужно перейти в раздел *HKEY_CURRENT_USER* → *SOFTWARE* → *Microsoft* → *Windows* → *CurrentVersion* → *Policies.* После этого требуется создать раздел Explorer, но в данной версии Windows 7 такая папка имеется, поэтому пропускаем шаг с созданием и переходим к дальнейшему выполнению редактирования реестра.

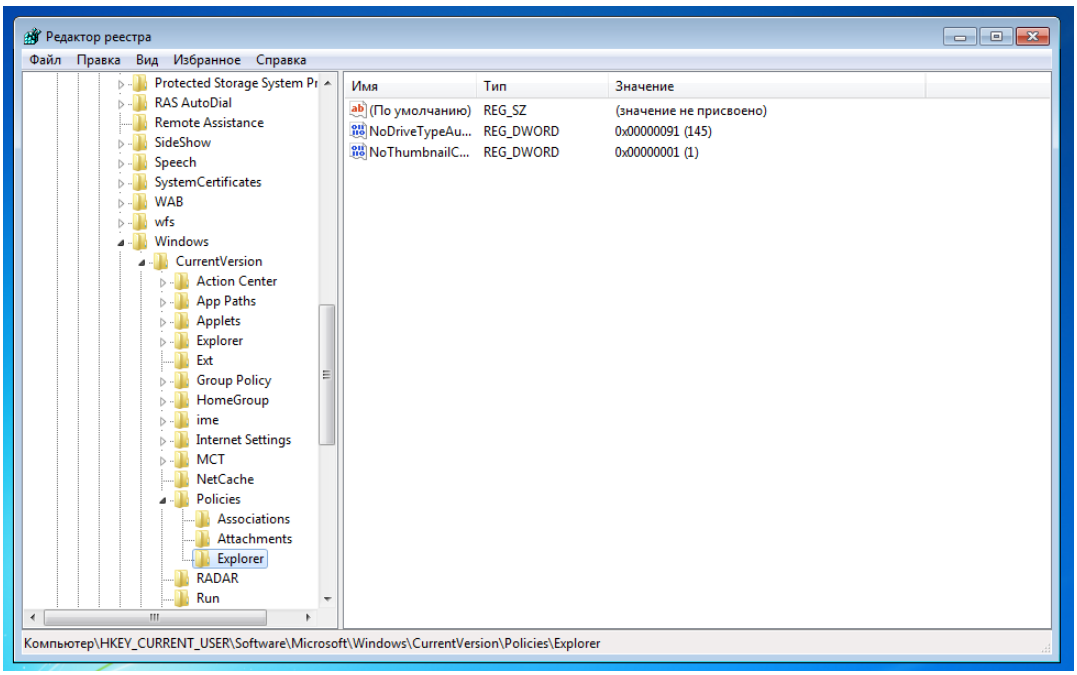

Рис.2 – папка Explorer

Как видно из рис. 2, в папке Explorer уже есть несколько параметров. Оставим их без изменения и начнем создавать свои параметры: *выделить раздел реестра Explorer → ПКМ → Создать → Параметр DWORD (32 бита)* (рис. 3).

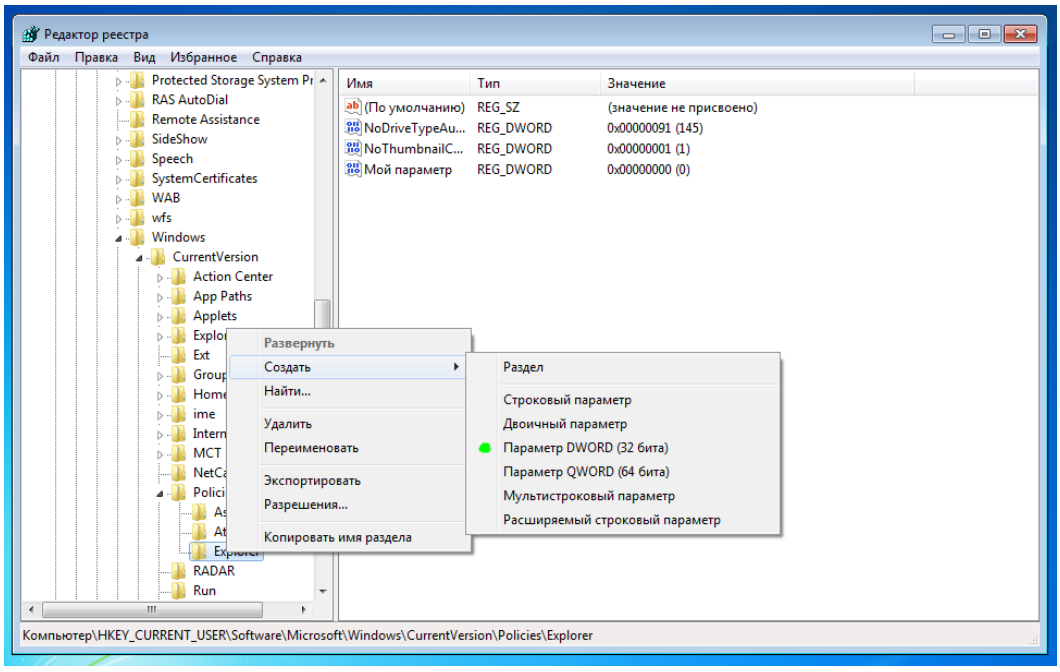

Рис.3 – создание собственного параметра

В результате будет создан новый параметр с заданным именем, с выбранным типом и со значением «0», поскольку параметр при создании инициализируется именно им. Изменим значение параметра на «1» (рис. 4).

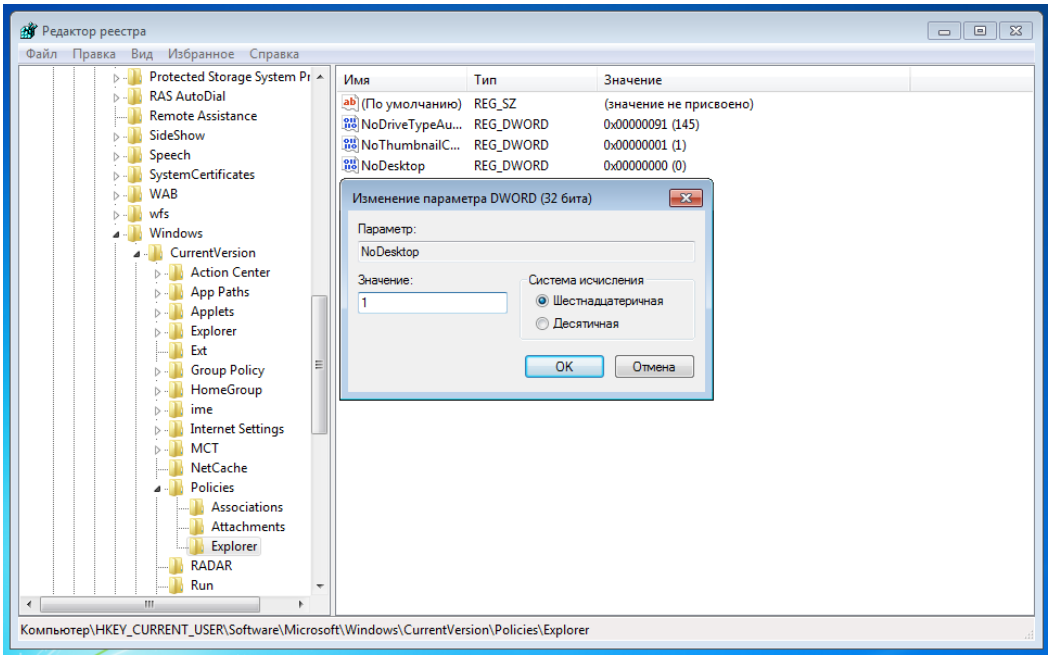

Рис.4 – изменение параметра

Параметр «NoDesktop» позволяет скрыть все элементы («ярлыки») на рабочем столе. Данная мера ограничивает действия пользователя в установке лишних ярлыков на рабочем столе. После перезагрузки с рабочего стола исчезли все ярлыки (рис. 5).

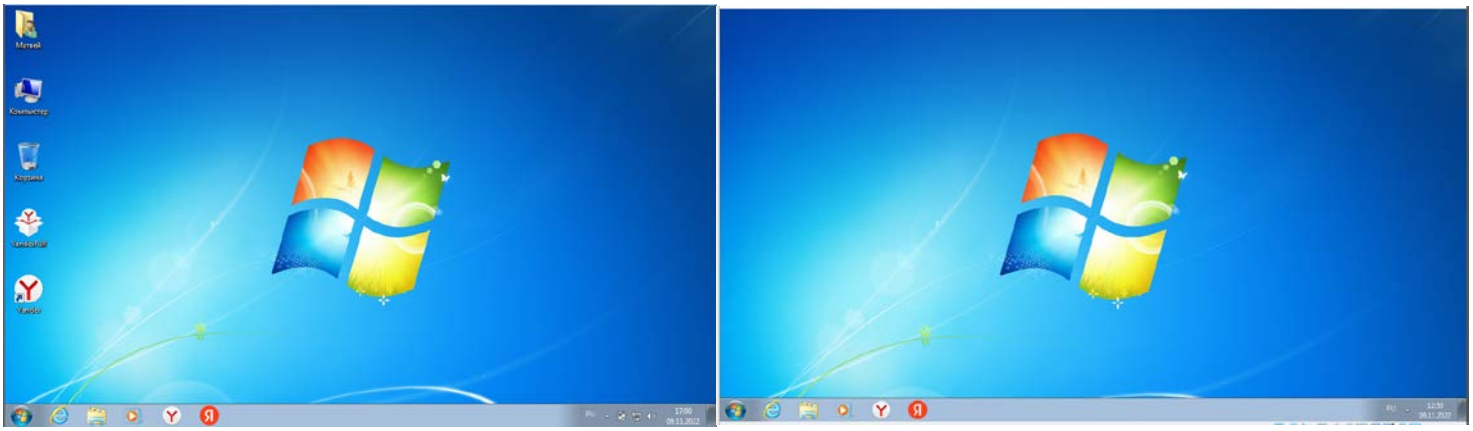

Рис.5 – рабочий стол до и после изменения реестра

С рабочего стола исчезли все ярлыки, а также на рабочем столе не работает контекстное меню (нажатие ПКМ не получают отклика). Однако, посмотреть содержимое все еще возможно через функционал Проводник (рис. 6).

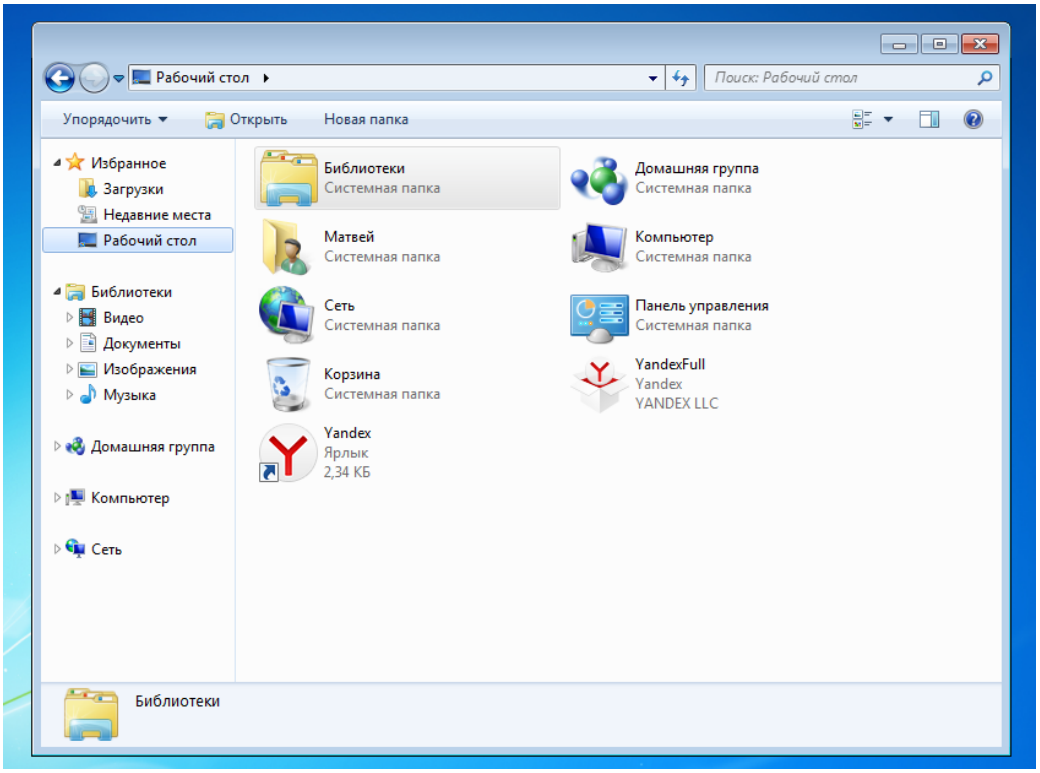

Рис.6 – содержимое рабочего стола

Внесем в реестр остальные нужные параметры:

- NoRun - Скрыть пункт меню «Выполнить» кнопки Пуск
- NoFind – Скрыть пункт меню «Найти» кнопки Пуск
- NoRecentDocsMenu - Скрыть пункт меню «Документы» кнопки Пуск
- NoFavoritesMenu - Скрыть пункт меню «Избранное» кнопки Пуск
- NoSetFolders - Скрытие пунктов меню «Принтеры» и «Панель управления» из меню «Настройка» кнопки Пуск
- NoWindowsUpdate - Скрытие пункта «WindowsUpdate» из меню Настройки кнопки Пуск
- NoSetTaskbar - Скрытие «Панели задач» и меню Пуск из меню «Настройка» кнопки Пуск
- NoSetActiveDesktop - Скрытие пункта «Рабочий стол ActiveDesktop» из меню Настройка кнопки Пуск
- NoChangeStartMenu - Запрет контекстного меню кнопки Пуск
- NoRecentDocsHistory - Очистка недавно открытых документов
- ClearRecentDocsOnExit - Очистка списка недавно открытых документов при выходе
- NoTrayContextMenu - Запрет контекстного меню для Панели задач

- NoFolderOptions - Запрет пункта «Свойства папок» из Меню настройка кнопки Пуск
- NoViewContextMenu - Запрет контекстного меню по правой клавише мыши на Рабочем столе
- NoCustomizeWebView - Запрет настройки вида конкретных папок

После создания новых параметров, папка Explorer выглядит так (рис. 7).

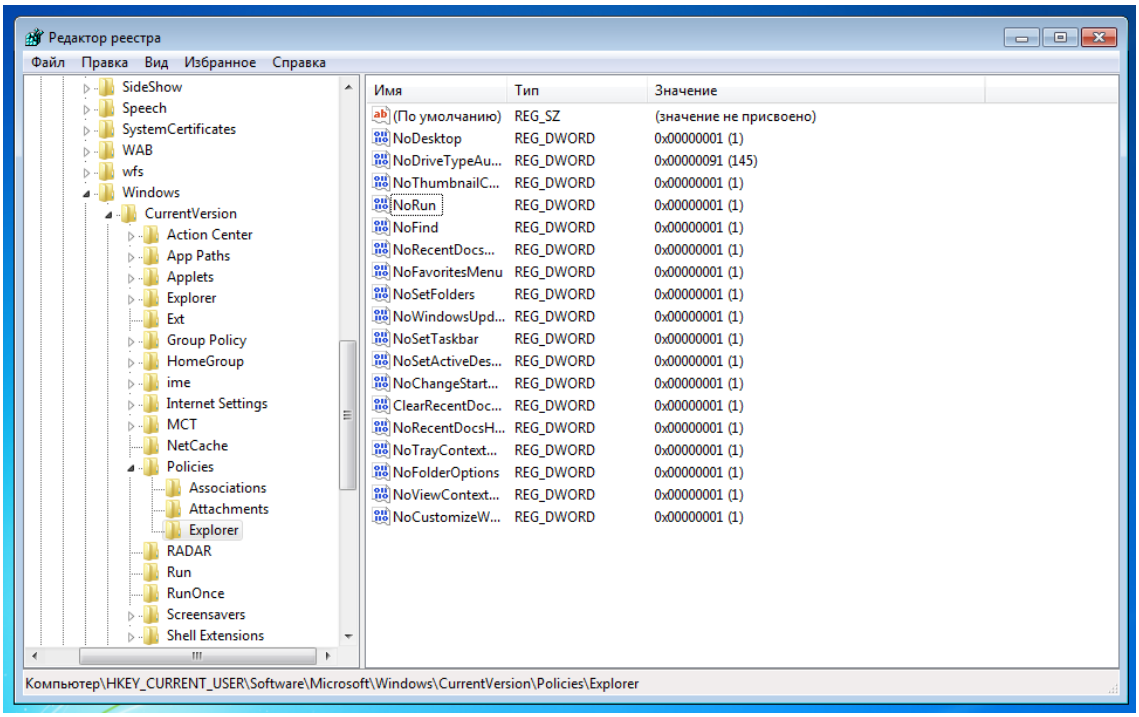

Рис.7 – содержимое папки Explorer

После того как настроены все выбранные параметры реестра, важно сохранить полученные значения в файл, т.к. резервная копия параметров реестра позволит не только вернуться к настроенным параметрам в случае необходимости, но и ускорит процесс настройки других АРМ. Экспорт всей директории Explorer в отдельный файл позволит не только получить короткий доступ к реестру, но и удобно работать с реестром через редактирование отдельного файла.

Для этого в редакторе реестра необходимо: *выделить раздел реестра Explorer → в строке меню выбрать Файл → Экспорт → место сохранения* (рис. 8).

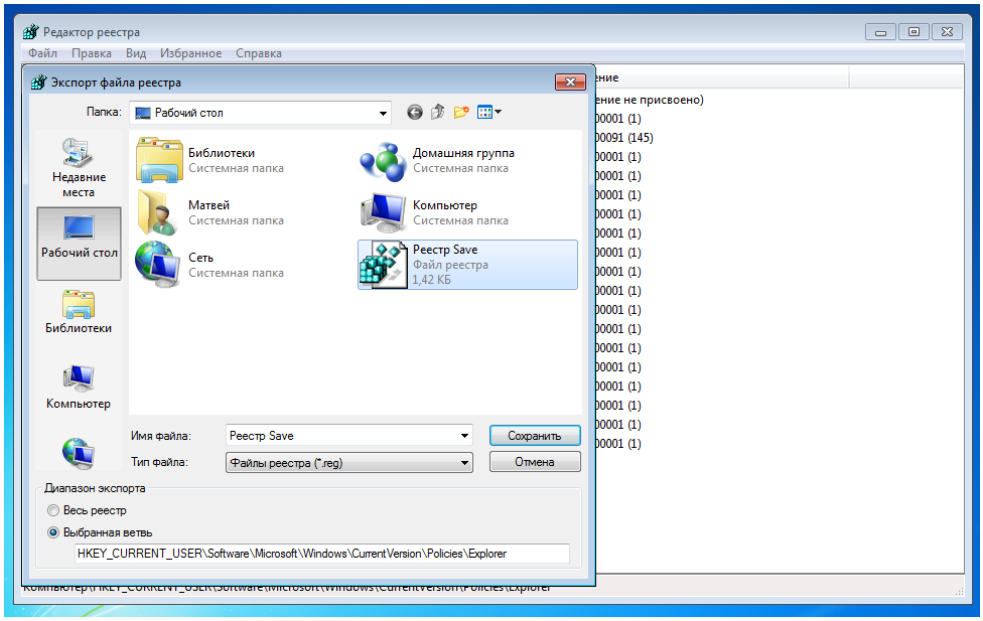

Рис.8 – сохранение файла реестра

После экспортирования раздела реестра с REG-файлами, которые он содержит, можно работать, как с обычным текстовым файлом, используя для этого стандартные текстовые редакторы (рис. 9).

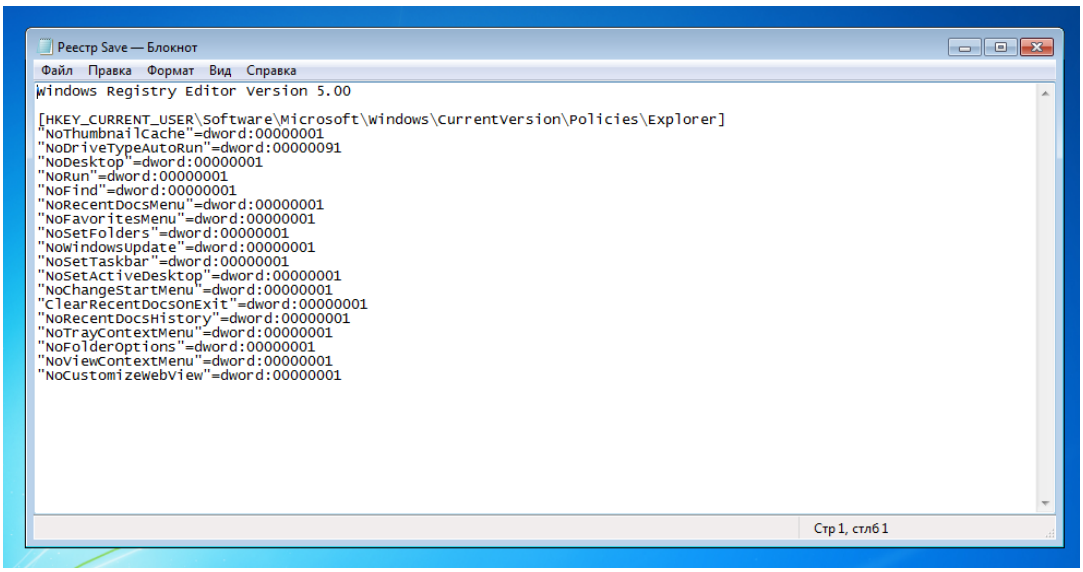

Рис.9 – настройки реестра в Блокноте

Для восстановления значения какого-либо раздела реестра по имеющейся копии, достаточно два раза щелкнуть мышью по REG-файлу — его содержимое будет автоматически добавлено внутрь реестра. Кроме того, при запущенном редакторе реестра можно в его строке меню выбрать Файл → Импорт, а затем указать REG-файл, который требуется импортировать.

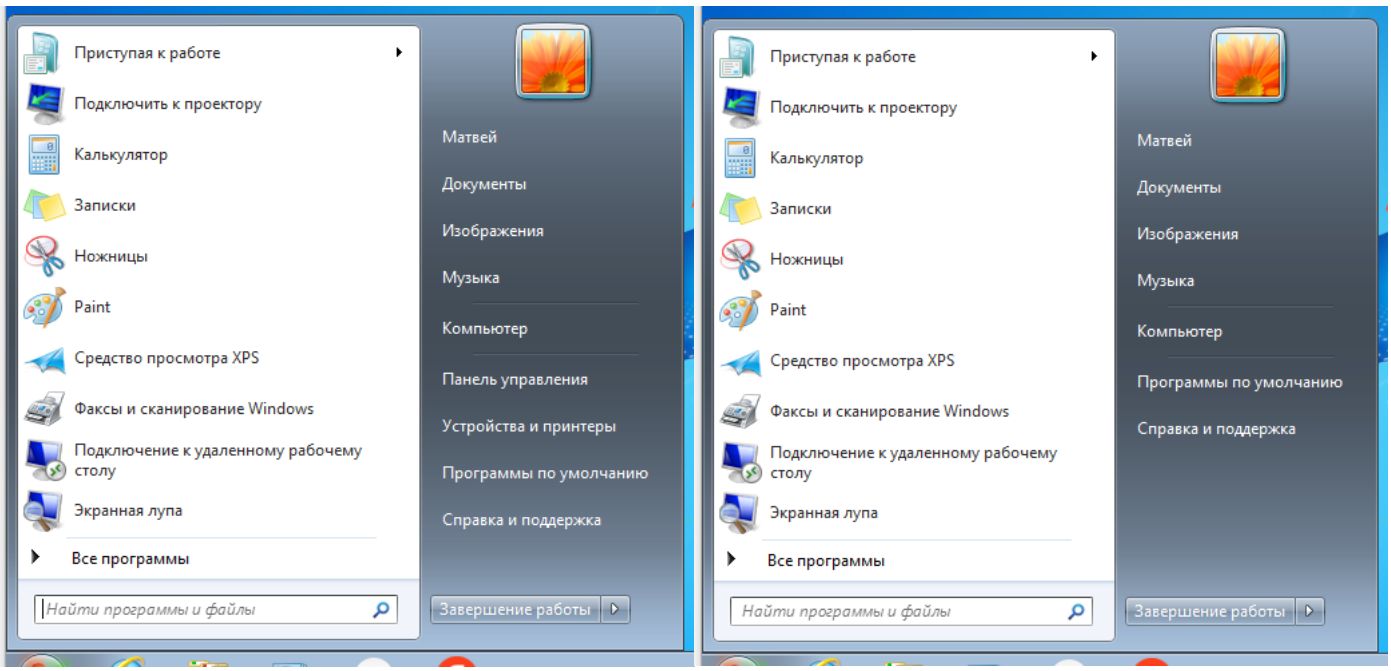

Рис.10 – меню Пуск до и после редактирования реестра

До применения параметров существовала возможность запустить редактор реестра через поиск меню «Панель управления» из меню «Настройка» кнопки Пуск и через меню «Выполнить» кнопки Пуск. Проверим недоступность редактора реестра через меню «Панель управления» из меню «Настройка» кнопки Пуск. После применения параметров это осуществить нельзя: пункт «Выполнить» меню Пуск скрыт, а доступ через сочетание клавиш Win+R приводит к ошибке – результат применения ключа NoRun (рис. 11).

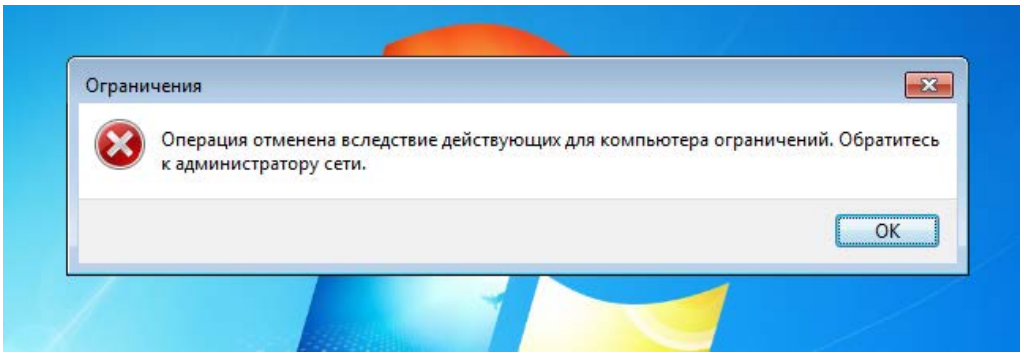

Рис.11 – сообщение об ограничении прав

После применения настроек ключа реестра NoSetFolders из поиска нельзя увидеть и зайти в реестр в режим редактирования (рис. 12). Такой способ защиты информации можно использовать в корпорациях или компаниях, чтобы сотрудники, у которых не должно быть доступа изменения настроек, не смогли этого сделать.

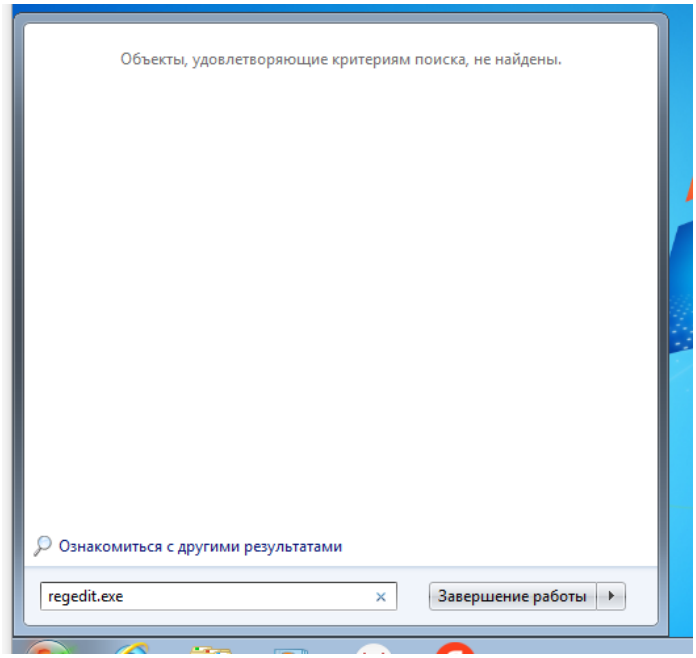

Рис.12 – результат применения параметра NoSetFolders

Также до применения настроек через кнопку Пуск можно было вызвать контекстное меню. После применения параметров реестра это действия стало невозможным, поэтому при нажатии правой клавиши мыши в меню Пуск ничего не происходит.

Однако, при этом следует помнить, что редактор реестра может быть запущен из командной строки Windows, если не принять дополнительных мер защиты. Открыть тот же редактор реестра можно напрямую запустив его exeфайл, расположенный по адресу *C:\Windows\regedit.exe.* Следовательно, можно сделать вывод, что для полного ограничения возможностей пользователя по запуску редактора реестра необходимо также ограничить доступ пользователя к содержимому диска С.

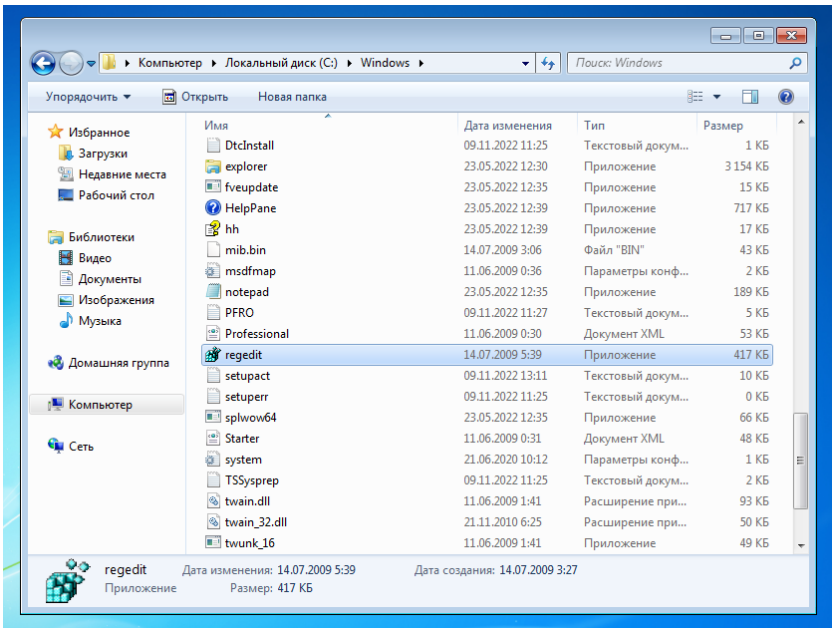

Рис.13 – приложение regedit.exe

Кроме того, «Панель управления», которая была скрыта из меню «Настройка» кнопки Пуск, доступна через поисковую строку (рис. 14).

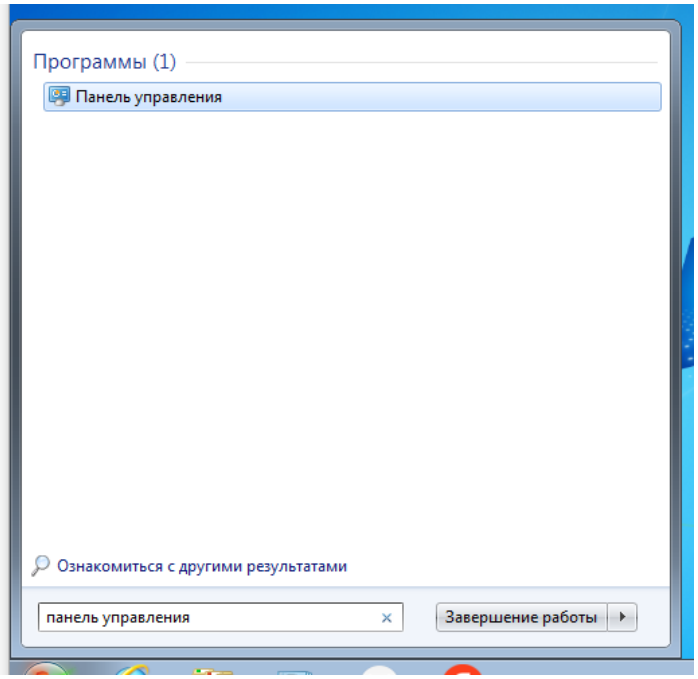

Рис.14 – панель управления в поиске

Поскольку в результате применения предыдущих настроек доступ к самой «Панели управления» у пользователя остался, несмотря на то, что она была скрыта в функционале меню кнопки Пуск - в целях безопасности ограничим функционал «Панели управления». Для этого следует создать в директории Policies новые разделы *System и ActiveDesktop*.

В качестве примера заблокируем настройки пункта «Экран» панели управления - параметр NoDispCPL (рис. 15) и заблокируем возможность изменения обоев рабочего стола пункта «Персонализация» панели управления - параметр NoChangingWallpaper (рис. 16). Первое сделано для удобства пользователя, второе – чтобы пользователь не мог установить на АРМ собственные обои, которые, например, будут включать изображение пароля от какой-то базы данных, с которой работает пользователь (вынесенное на рабочий стол поскольку пользователь не может его запомнить).

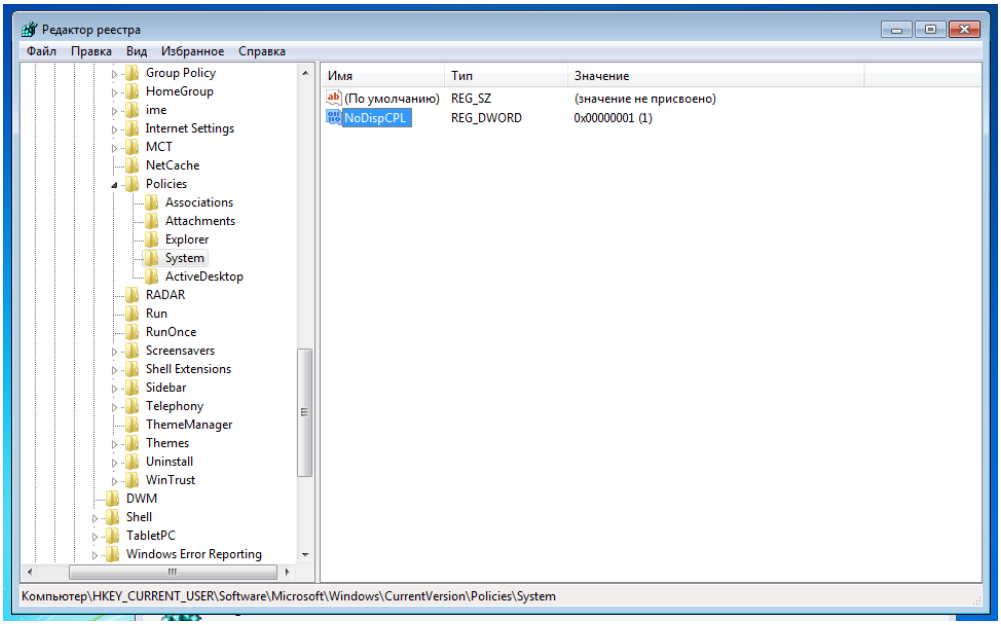

Рис.15 – новый параметр в папке System

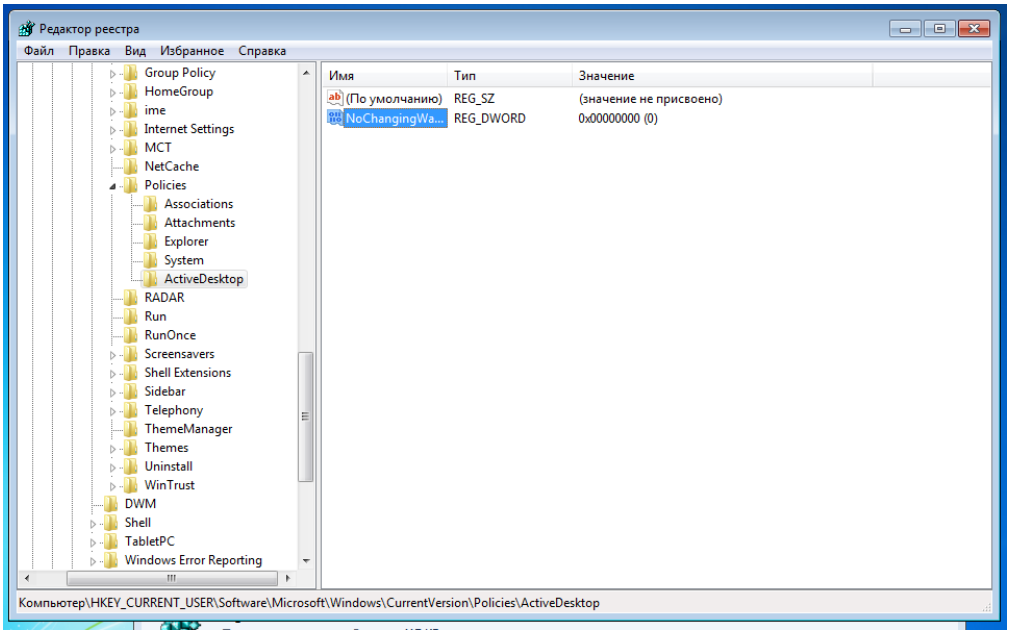

Рис.16 – новый параметр в папке Active Desktop

После внесения новых параметров и перезагрузки компьютера проверяем функционал (рис. 17 и 18).

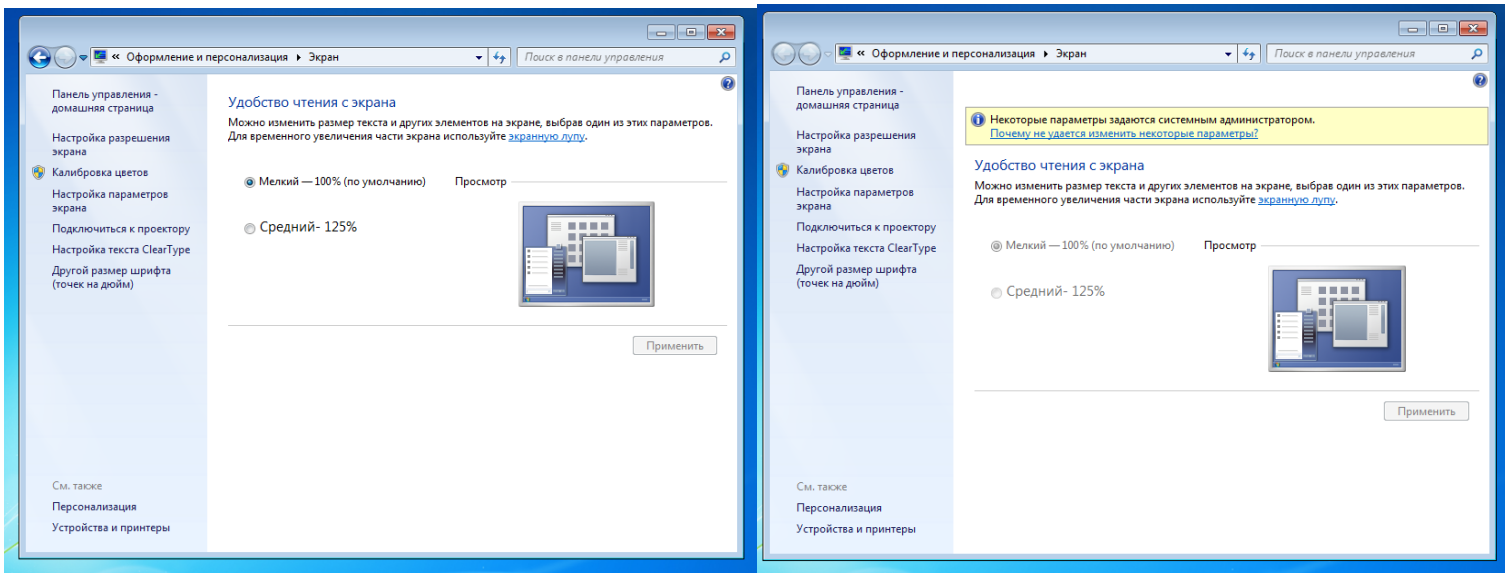

Рис.17 – настройки экрана до и после внесения изменений

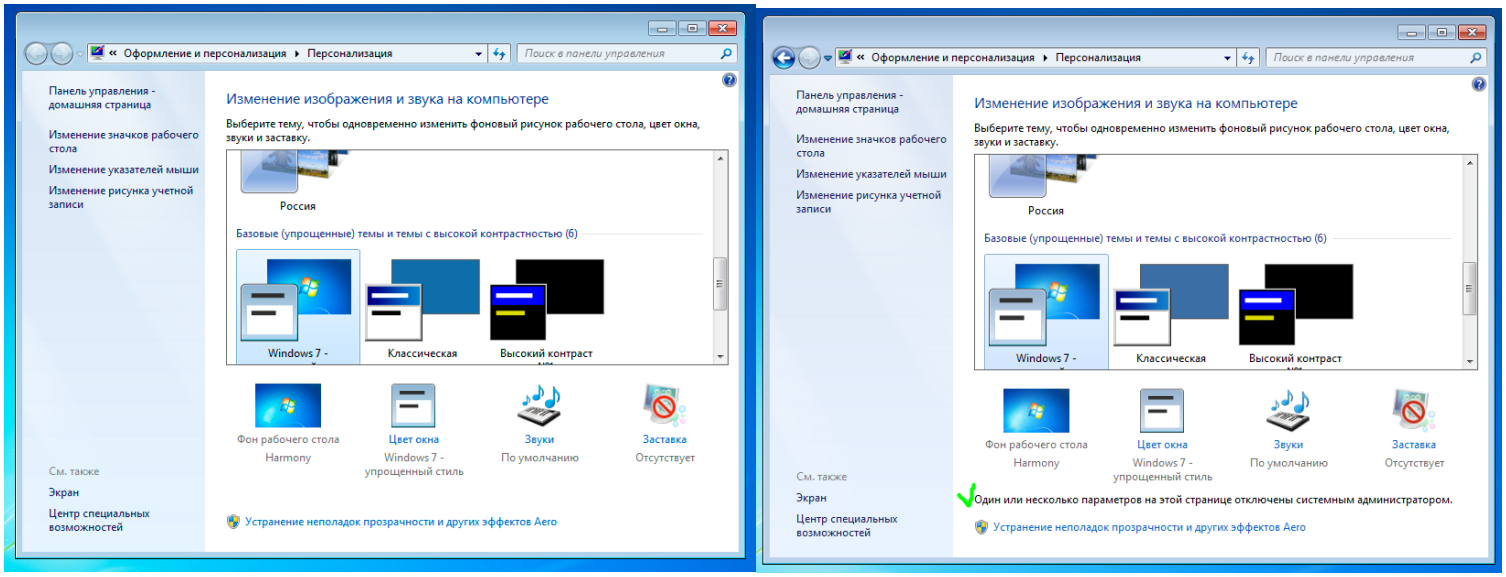

Рис.18 – настройки персонализации до и после внесения изменений

Изменения очевидны: теперь пользователю недоступно изменение фона рабочего стола и изменение масштабирования экрана, соответствующие пункты неактивны, а также появились предупреждения о том, что некоторые параметры данных вкладок изменены системным администратором. Соответственно, и отменить данные ограничения также может только системный администратор.

Рассмотрим еще один пример. Отключим возможность использования «Панели управления». Для этого воспользуемся настройкой параметра NoControlPanel (рис. 19).

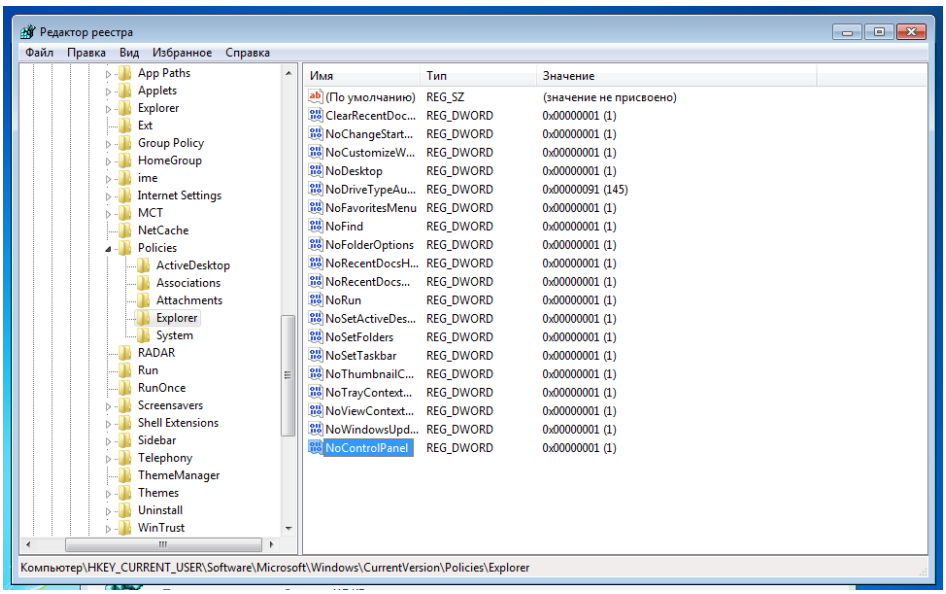

Рис.19 – параметр NoControlPanel в папке Explorer

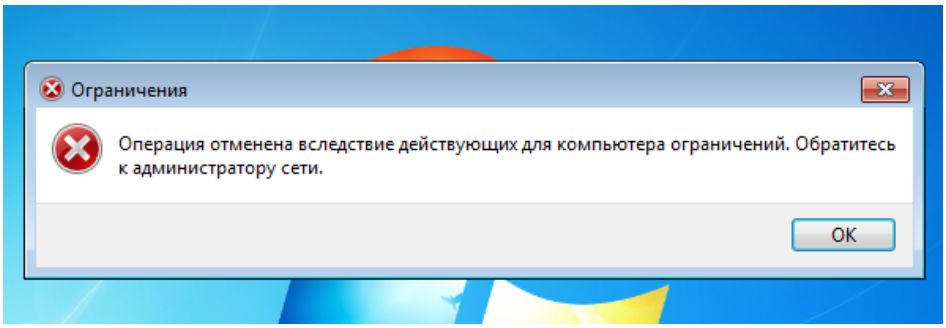

Рис.20 – вызов панели управления после редактирования реестра

Таким образом, ограничение функционала «Панели управления» произведено успешно.

Вывод:

В данной лабораторной работе была изучена и настроена изолированная программная среда на АРМ закрытого контура ИС средствами ОС Windows 7 с целью защиты от НСД. Были изучены: способ вызова реестра для настройки безопасности сети, добавление параметров в разделы реестра, установка значений для параметров, экспортирование настроек реестра. Было произведено редактирование ключей реестра раздела Explorer для ограничения функционала рабочего стола и меню «Пуск» пользователя, редактирование реестра для ограничения функционала «Панели управления» пользователя и редактирование реестра для ограничения функционала меню «Пуск» пользователя.

Использование параметров редактора реестра существенно способствует увеличению безопасности системы, поскольку работа с редактором доступна только системному

администратору. В то же время ИПС создает определенные сложности в администрировании защищаемой системы. Неправильная настройка параметров может привести к некорректной работе операционной системы.

Введение данных ограничений помогает частично выполнить требование к классу защищенности 3Б по обеспечению целостности программных средств и обрабатываемой информации.