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

Используемое программное обеспечение: операционная система Windows 7.

Теоретические сведения

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.

Редактор реестра в Windows является своеобразным «хранилищем» системы, которое содержит в себе настройки и параметры, как самой операционной системы, так и различных программ, установленных в ней, а также многого другого, необходимого для работы Windows. Редактор реестра содержит список его главных разделов (root keys, корневых ключей). Внутри них содержатся все значения реестра:

- 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.

Параметры (ключи) реестра бывают нескольких видов (параметры DWORD, QWORD, двоичные, строковые и многострочные параметры и др.) в зависимости от сведений, которые в них содержатся. Информацию с этих ключей Windows считывает главным образом во время запуска, поэтому для того чтобы внесенные в реестр Windows изменения вступили в силу, нужно перезагрузить компьютер.

Раздел Explorer, в который необходимо вносить изменения, отвечает за настройки экрана, рабочего стола и т.д. Создание раздела Explorer производится через свойства раздела Policies.

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

Для применения параметра необходимо изменить установленное по умолчанию значение параметра «0» на «1». После того, как все параметры добавлены, можно экспортировать всю директорию Explorer в отдельный файл, для удобства работы с реестром путем редактирование отдельного файла.

Настройка изолированной программной среды на АРМ

Для анализа динамики изменений зафиксируем исходный вид меню «Пуск» и рабочего стола АРМ.

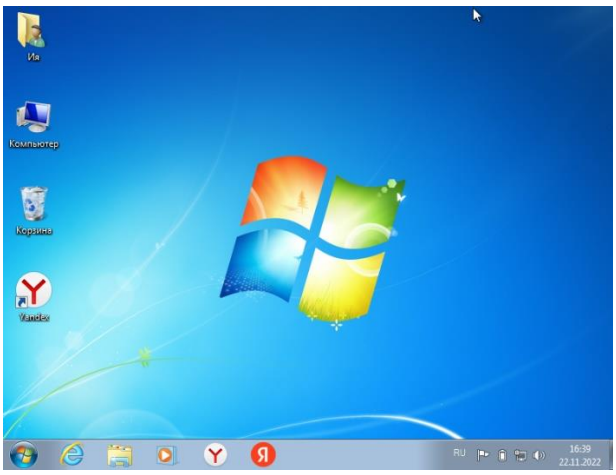


Рисунок 1 - Рабочий стол

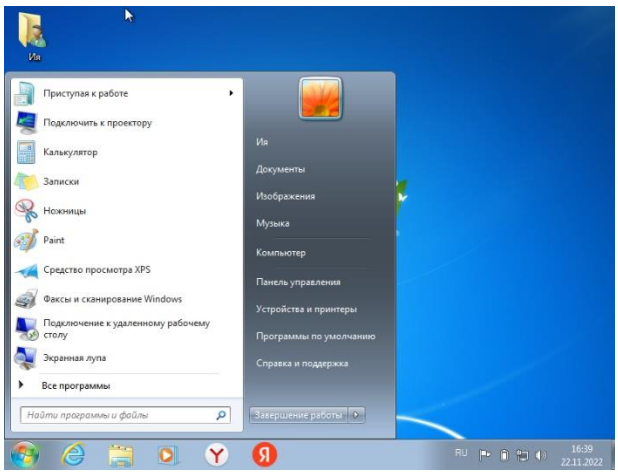


Рисунок 2 - Меню "Пуск"

1.1 Редактирование параметров реестра

Чтобы открыть редактор реестра нужно нажать сочетанием клавиш ***Win+R***, а после ввести ***regedit*** в окно поиска:

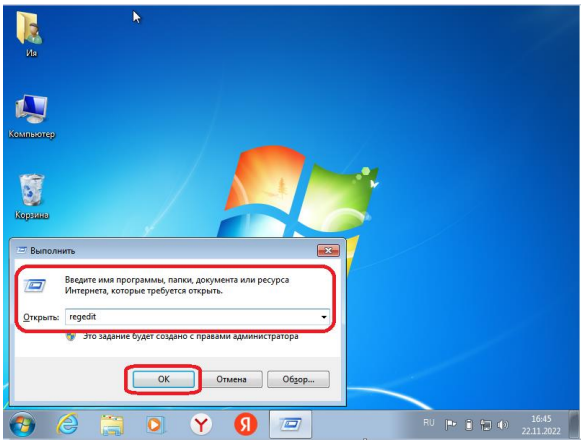


Рисунок 3 - Открытие редактора реестра

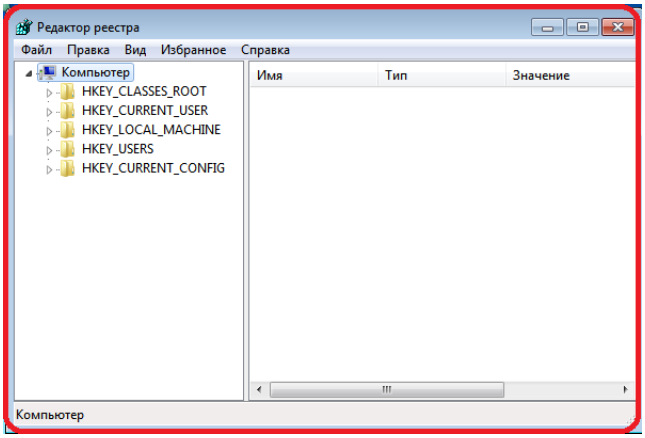


Рисунок 4 - Редактор реестра

1.1.1 Раздел реестра Policies

Далее перейдем в раздел реестра Policies. Для этого в редакторе реестра переместимся по следующим каталогам:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\

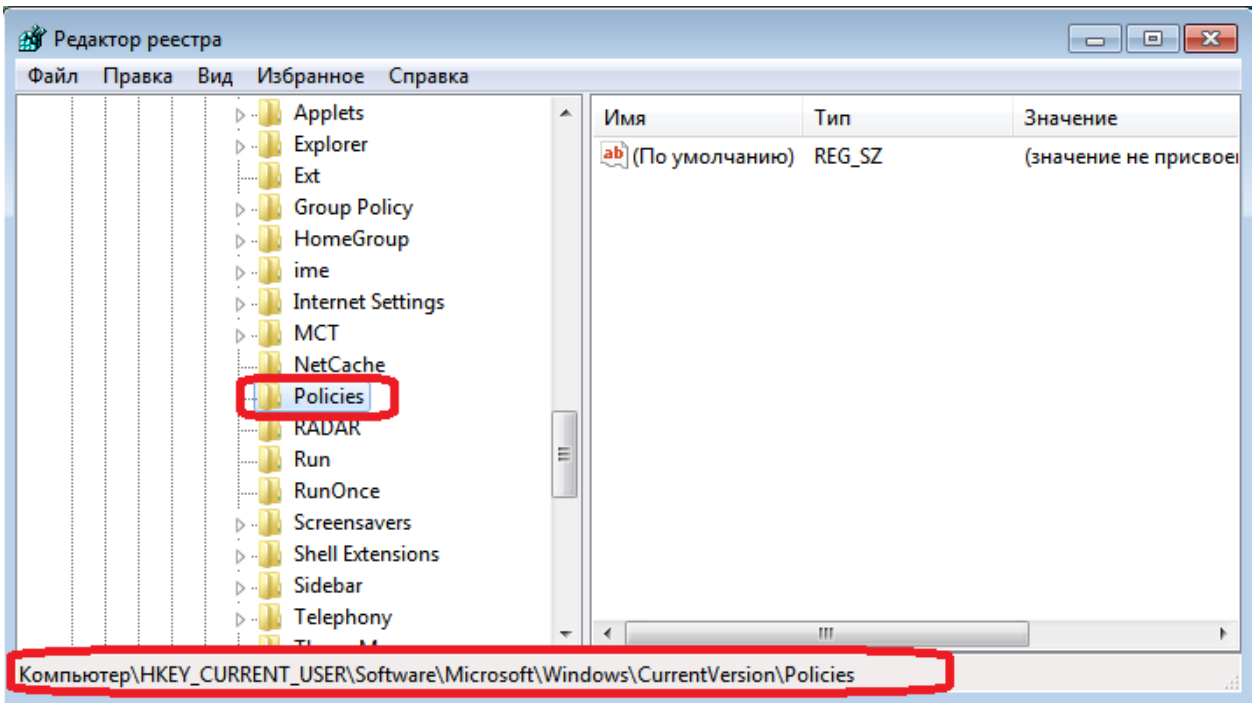


Рисунок 5 - Раздел policies

1.1.2 Создание раздела Explorer

Создадим раздел Explorer с целью настройки экрана, рабочего стола и т.д. Для его создания необходимо кликнуть правой кнопкой по ***policies***, выбрать ***создать***, выбрать ***раздел*** и присвоить имя ***explorer***:

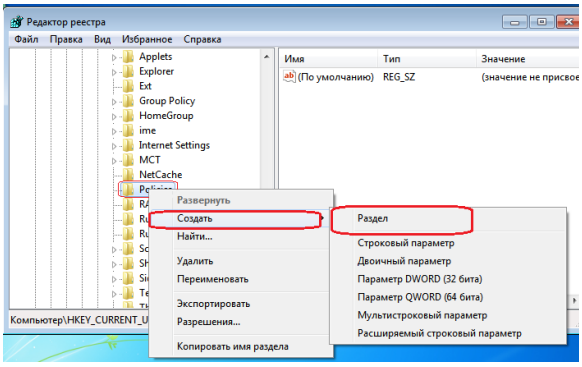


Рисунок 6 - Создание раздела

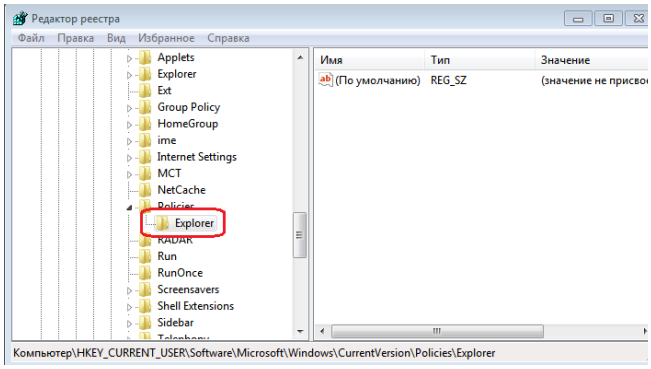


Рисунок 7 - Новый раздел

1.1.3 Создание параметра NoDesktop

Создадим в разделе Explorer новый параметр типа DWORD. Данные типа DWORD – это данные, представленные целым числом (4 байта, 32 бита). Присвоим имя созданному параметру – NoDesktop, и установим его значение равным 1. Этот параметр позволяет скрыть все элементы на рабочем столе с целью ограничения действия пользователя в установке лишних ярлыков на рабочем столе. Для создания необходимо кликнуть правой кнопкой по ***policies***, выбрать ***создать***, выбрать ***параметр DWORD 32 бита*** и присвоить

имя ***NoDesktop***. Для установки 1 необходимо дважды кликнуть по параметру ***NoDesktop*** и в открывшемся окне ***изменения параметра*** установить требуемое значение:

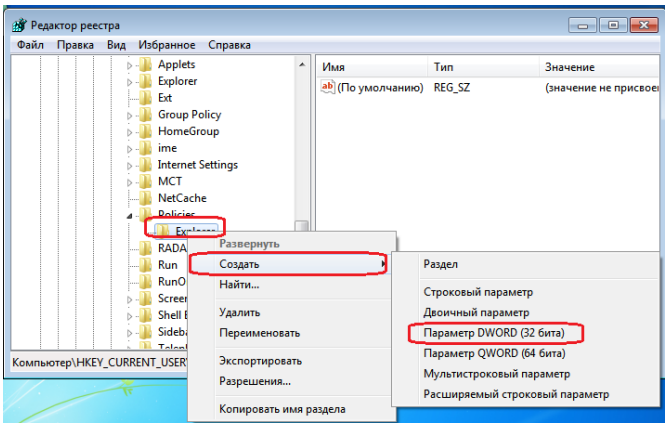


Рисунок 8 - Создание параметра NoDesktop

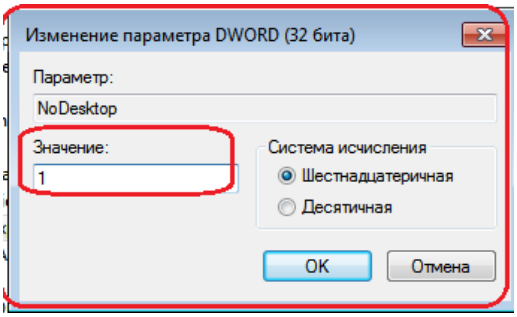


Рисунок 9 - Изменение значения параметра

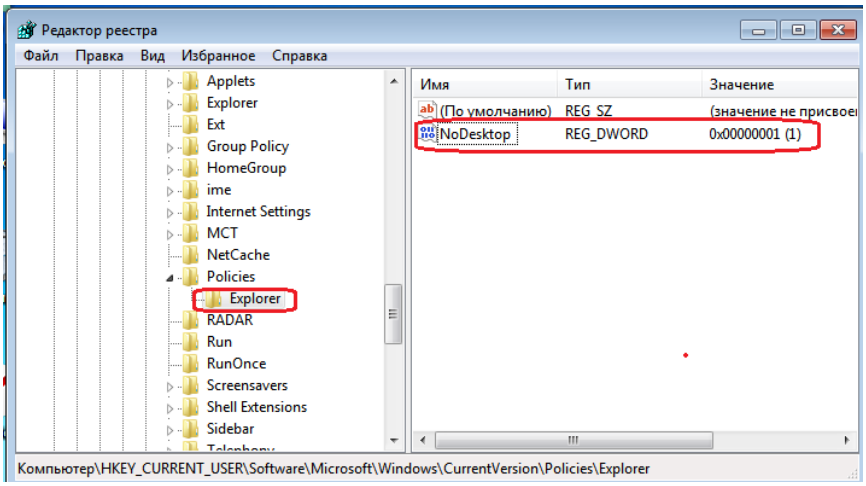


Рисунок 10 - Установленное значение

Теперь можно увидеть изменения:

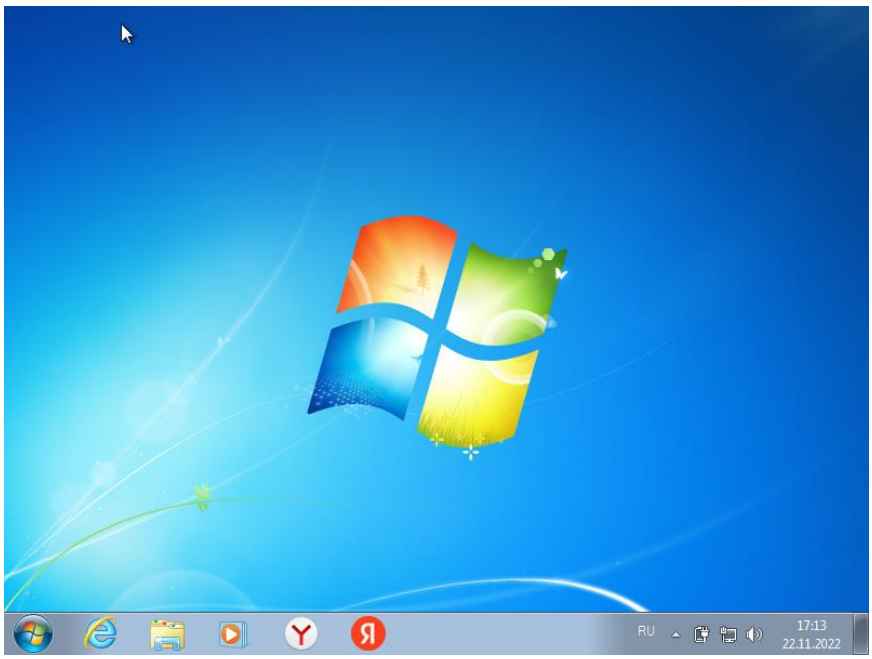


Рисунок 11 - Рабочий стол после изменений

Таким образом, ключ реестра *NoDesktop* не удаляет ярлыки и значки с рабочего стола пользователя, но запрещает их отображение. Пользователь не может редактировать содержимое рабочего стола, а также выносить на него свои ярлыки. Это необходимо, так как

Аналогичным образом настроим все остальные параметры раздела *Explorer*.

1.1.4 Создание параметра NoRun

Создадим параметр *NoRun* с целью скрытия пункта меню «Выполнить» кнопки Пуск.

1.1.5 Создание параметра NoFind

Создадим параметр *NoFind* с целью скрытия пункта меню «Найти» кнопки Пуск.

1.1.6 Создание параметра NoRecentDocsMenu

Создадим параметр *NoRecentDocsMenu* с целью скрытия пункта меню «Документы» кнопки Пуск.

1.1.7 Создание параметра NoFavoritesMenu

Создадим параметр *NoFavoritesMenu* с целью скрытия пункт меню «Избранное» кнопки Пуск.

1.1.8 Создание параметра NoSetFolders

Создадим параметр *NoSetFolders* с целью скрытия пунктов меню «Принтеры» и «Панель управления» из меню «Настройка» кнопки Пуск.

1.1.9 Создание параметра NoWindowsUpdate

Создадим параметр *NoWindowsUpdate* с целью скрытия пункта «WindowsUpdate» из меню Настройки кнопки Пуск.

1.1.10 Создание параметра NoSetTaskbar

Создадим параметр *NoSetTaskbar* с целью скрытия «Панели задач» и меню Пуск из меню «Настройка» кнопки Пуск.

1.1.11 Создание параметра NoSetActiveDesktop

Создадим параметр *NoSetActiveDesktop* с целью скрытия пункта «Рабочий стол ActiveDesktop» из меню Настройка кнопки Пуск.

1.1.12 Создание параметра NoChangeStartMenu

Создадим параметр *NoChangeStartMenu* с целью запрета контекстного меню кнопки Пуск

1.1.13 Создание параметра NoRecentDocsHistory

Создадим параметр *NoRecentDocsHistory* с целью очистки недавно открытых документов.

1.1.14 Создание параметра ClearRecentDocsOnExit

Создадим параметр *ClearRecentDocsOnExit* с целью очистки списка недавно открытых документов при выходе.

1.1.15 Создание параметра NoTrayContextMenu

Создадим параметр *NoTrayContextMenu* с целью запрета контекстного меню для Панели задач.

1.1.16 Создание параметра NoFolderOptions

Создадим параметр *NoFolderOptions* с целью запрета пункта «Свойства папок» из Меню настройка кнопки Пуск.

1.1.17 Создание параметра NoViewContextMenu

Создадим параметр *NoViewContextMenu* с целью запрета контекстного меню по правой клавише мыши на Рабочем столе.

1.1.18 Создание параметра NoCustomizeWebView

Создадим параметр *NoCustomizeWebView* с целью запрета настройки вида конкретных папок Меню Вид команда Настроить вид папки.

После создания всех параметров и установки значений раздел Explorer имеет вид:

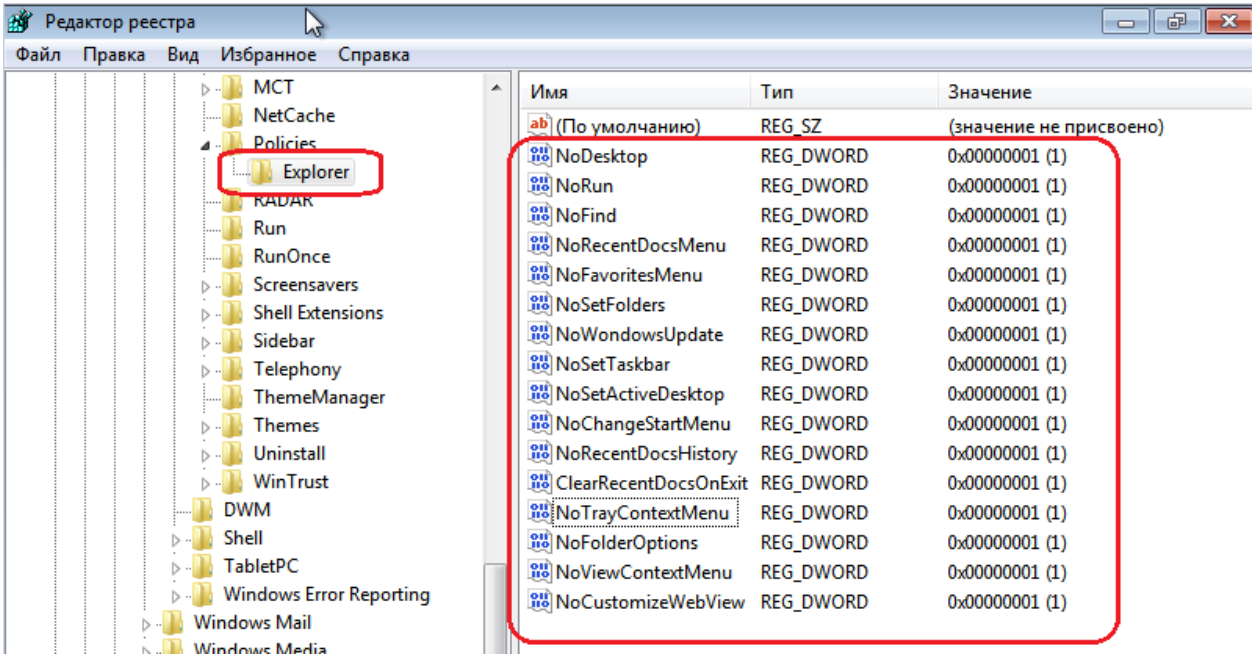


Рисунок 12 - Созданные параметры

1.2 Экспорт директории Explorer

Необходимо экспортировать директорию *Explorer* для сохранения значений параметров реестра в файл с целью возможности возврата к настроенным параметрам на данном АРМ и ускоренной настройки других АРМ. Для этого необходимо выделить раздел реестра ***Explorer***, в меню выбрать ***файл***, выбрать ***экспорт*** и место сохранения (в данном случае C:\):

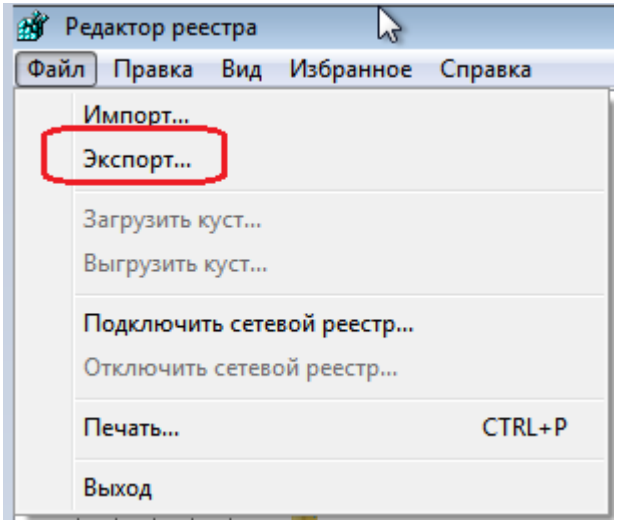


Рисунок 13 - Экспорт

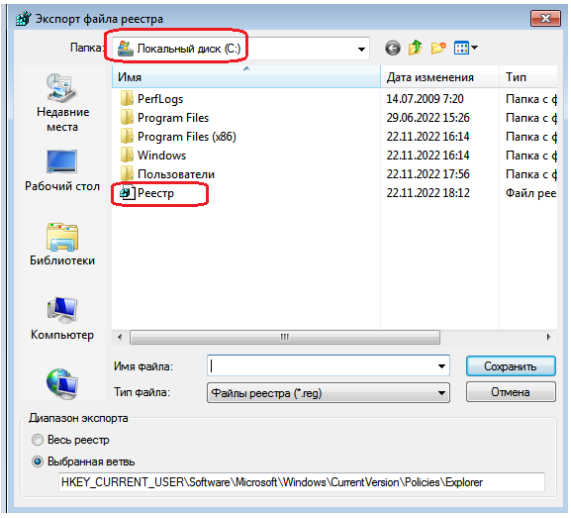


Рисунок 14 - Файл

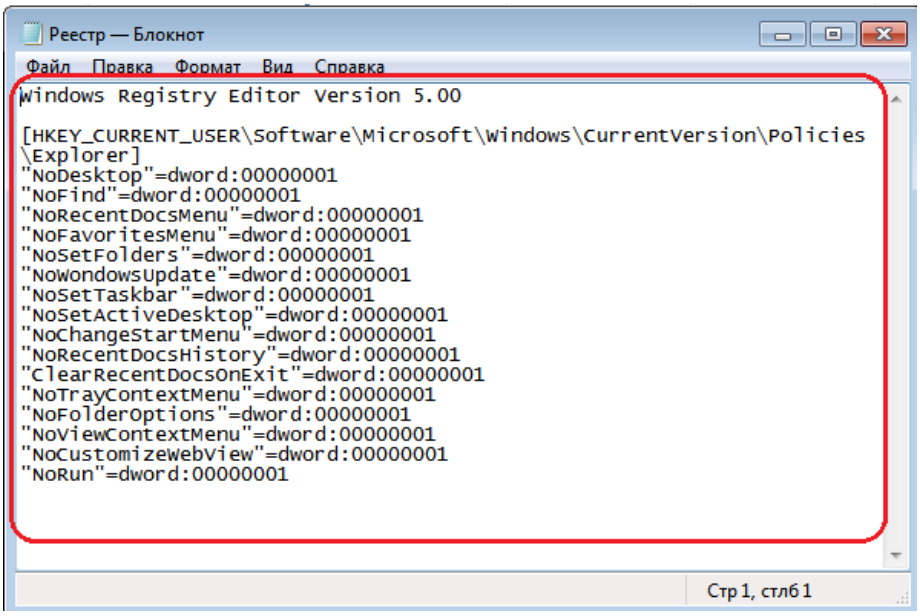


Рисунок 15 - Содержимое файла

1.3 Оценка изменений

Оценим изменения после настройки параметров реестра.

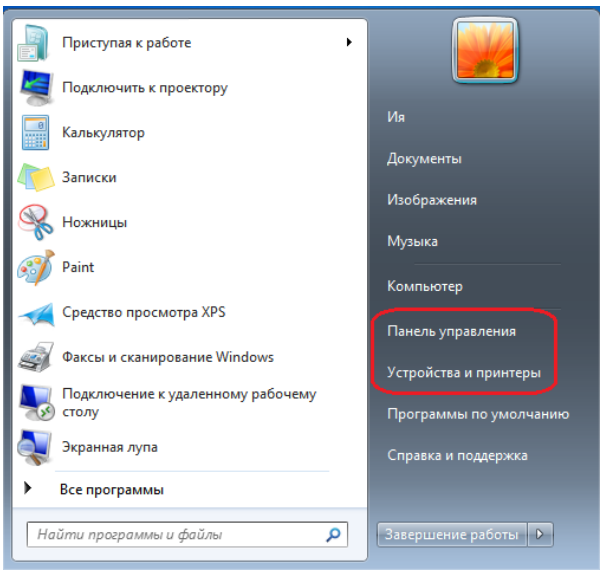


Рисунок 16 - Было

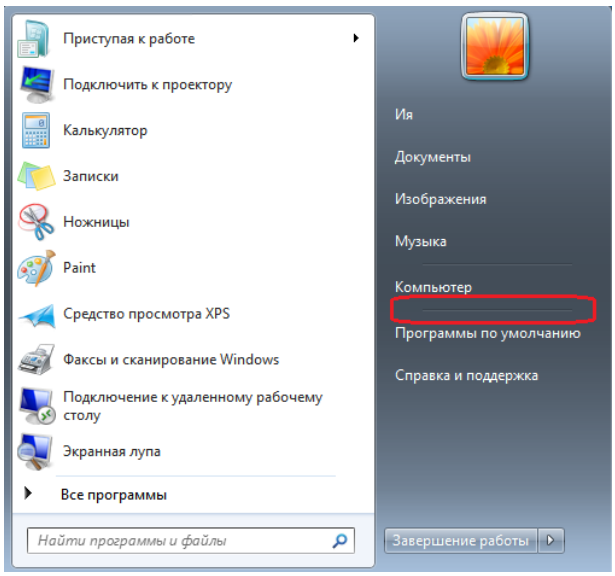


Рисунок 17 - Стало

Как видно, из меню «Пуск» скрылись пункты меню «Панель управления» и «Устройства и принтеры». Скрытие было настроено параметрами NoRun и NoSetFolders.

Пункт “Выполнить” меню Пуск скрыт, а доступ через сочетание клавиш Win+R приводит к ошибке – результат применения ключа NoRun:

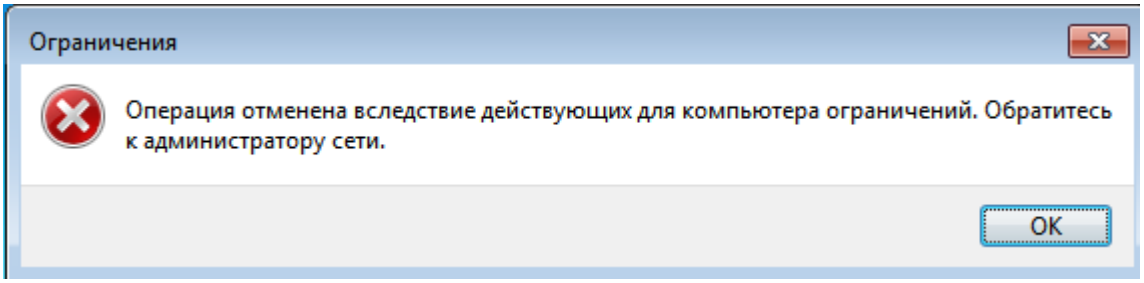


Рисунок 18 - Ошибка при Win+R

После применения настроек ключа реестра NoSetFolders из поиска нельзя увидеть и зайти в реестр в режим редактирования. Однако это по-прежнему можно сделать из C:\Windows.

Панель же управления доступна при поиске:

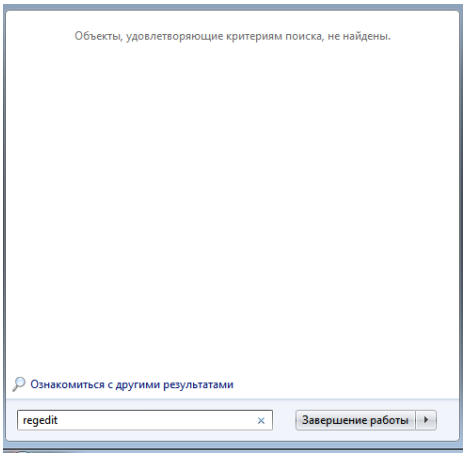


Рисунок 19 - Редактор реестра из поиска

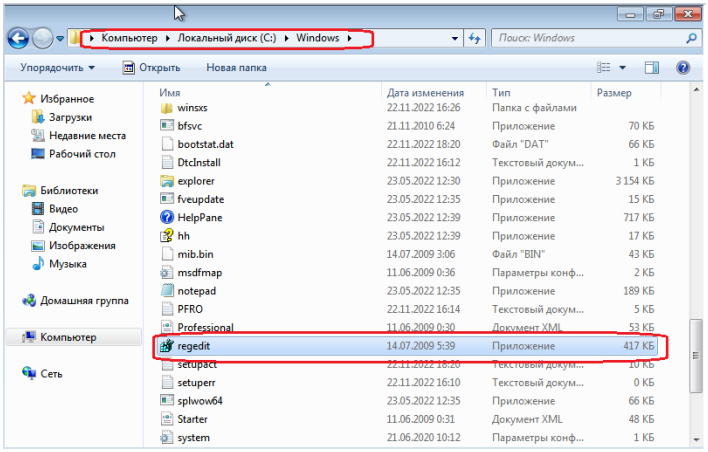


Рисунок 20 - Редактор реестра из C:\Windows

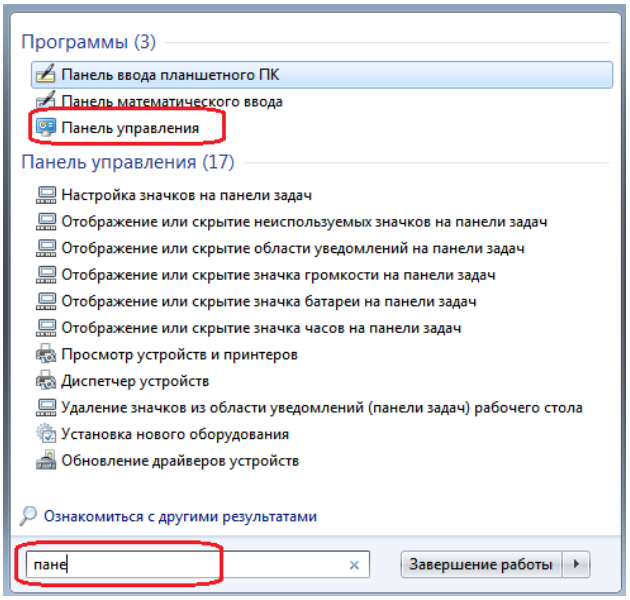


Рисунок 21 -Панель управления из поиска

1.4 Редактирование реестра для ограничения функционала «Панели управления»

Создадим следующие разделы:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop.

Подробные шаги для создания раздела были описаны выше. После создания получено:

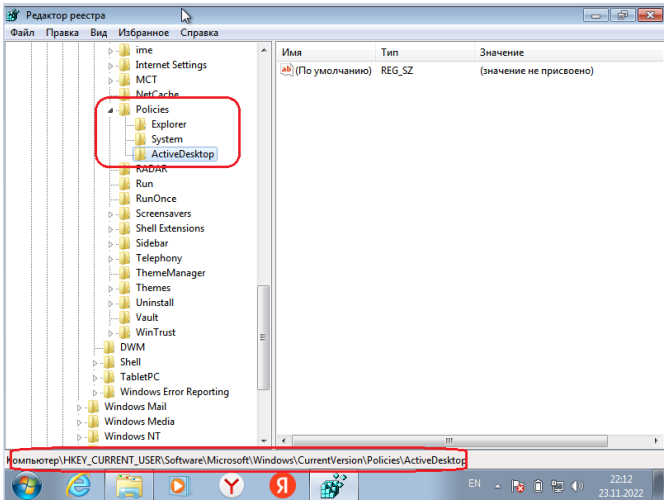


Рисунок 22 - Создание новых разделов

Аналогичным образом создадим следующие ключи:

1.4.1 Создание ключа NoDispCPL

Создадим параметр *NoDispCPL* в *System* с целью блокировки настройки пункта «Экран» в панели управления в целях обеспечения безопасности, так как настройками панели управления должен заниматься администратор, и удобства пользователя.

1.4.2 Создание ключа NoChanginigWallpaper

Создадим параметр *NoChanginigWallpaper* в *ActiveDesktop* с целью запрета изменения фонового изображения рабочего стола, 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).

Сравним результаты до изменения значений параметров и после:

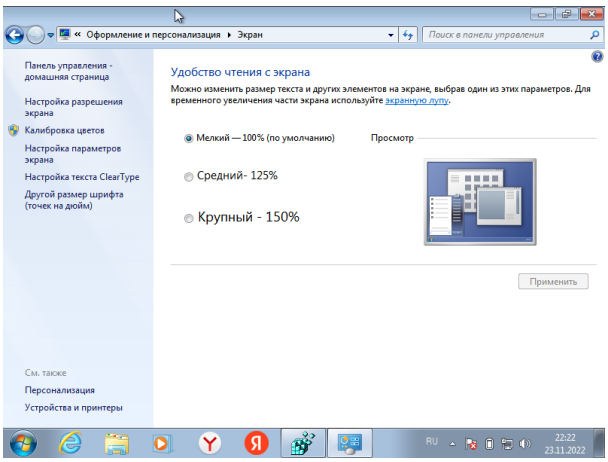


Рисунок 23 - Настройка экрана до изменений

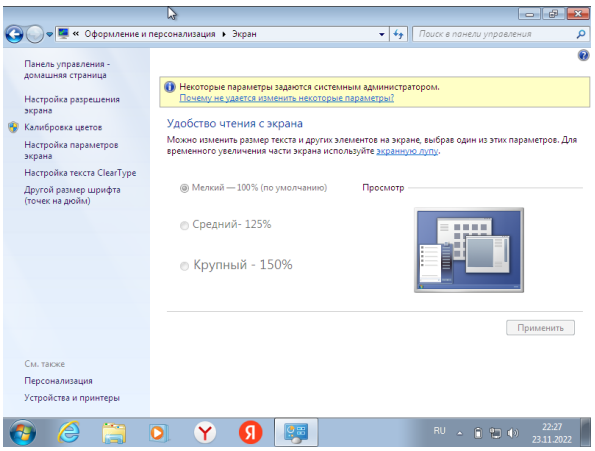


Рисунок 24 - Настройка экрана после изменений

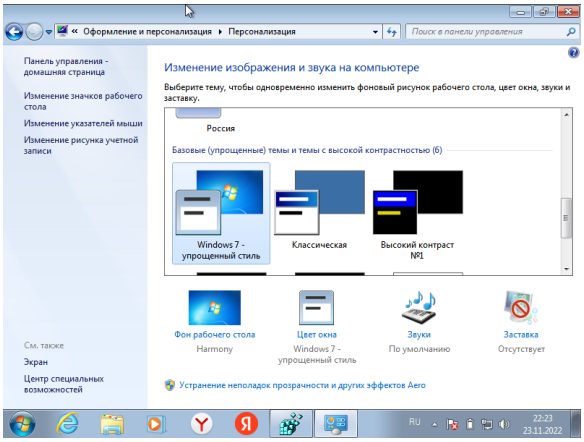


Рисунок 25 - Настройка обоев до изменений

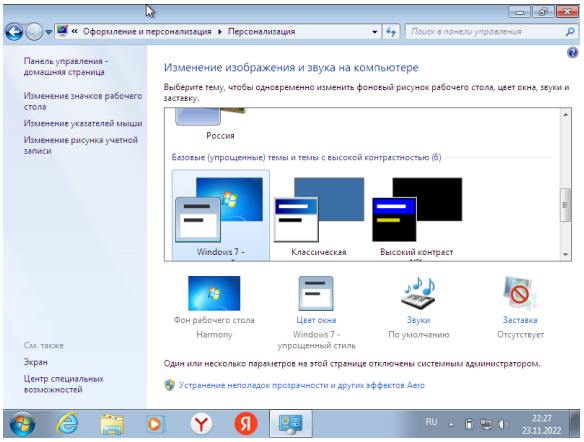


Рисунок 26 - Настройка обоев после изменений

Теперь пользователю недоступно изменение масштабирования экрана, а также появилось предупреждение о том, что некоторые параметры данной вкладки изменены системным администратором. Соответственно, и отменить данные ограничения также может только системный администратор.

Пользователю также недоступно изменение фона рабочего стола, соответствующий пункт неактивен, а также появилось предупреждение о том, что некоторые параметры данной вкладки изменены системным администратором. Соответственно, и отменить данные ограничения также может только системный администратор.

Отключим возможность использования «Панели управления» с целью ограничения возможности пользователя вносить изменения в систему. Для этого воспользуемся настройкой параметра *NoControlPanel*.

Убедимся в том, что у пользователя нет доступа к панели управления даже через поисковую строку:

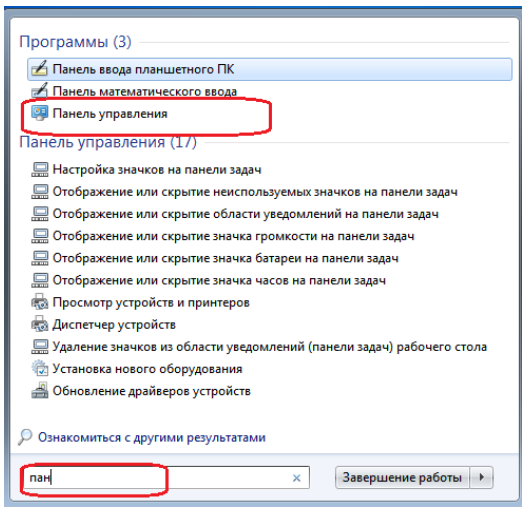


Рисунок 27 - Панель управления

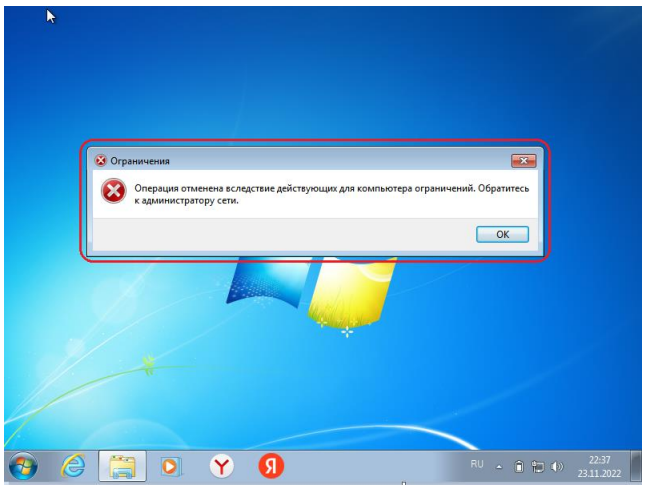
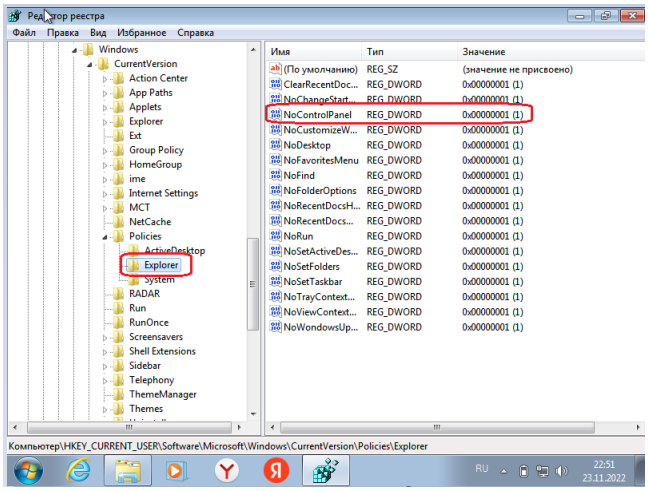


Рисунок 28 - Доступа к панели управления нет

1.5 Редактирование реестра для закрытия меню кнопки «Пуск» от редактирования

Закрытие меню кнопки «Пуск» от редактирования используется для того, чтобы зафиксировать доступные для работы пользователя приложения в соответствии с политикой конфиденциальности предприятия. Для этого следует: в разделе Explorer был ранее создан ключ *NoChangeStartMenu*:



Сравним изменения:

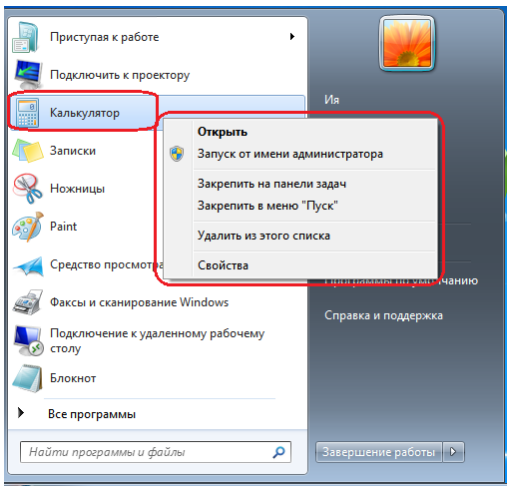


Рисунок 29 - До изменений

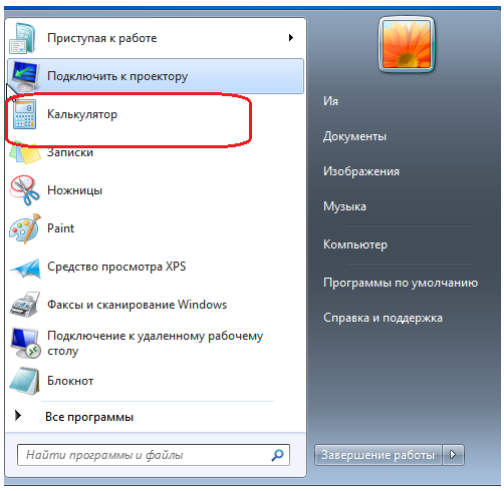


Рисунок 30 - После изменений

Как видно, теперь меню кнопки «Пуск» закрыто от редактирования.

Выводы: в ходе выполнения лабораторной работы были изучены и настроена изолированная программная среда (ИПС) на автономном автоматизированном рабочем месте (АРМ) пользователя средствами операционной системой Windows для защиты информации от несанкционированного доступа (НСД).

Был создан раздел *Explorer* с целью настройки экрана, рабочего стола и т.д. В рамках раздела *Explorer* были настроены следующие ключи:

- Ключ *NoRun* с целью скрытия пункта меню «Выполнить» кнопки Пуск.
- Ключ *NoFind* с целью скрытия пункта меню «Найти» кнопки Пуск.
- Ключ *NoRecentDocsMenu* с целью скрытия пункта меню «Документы» кнопки Пуск.
- Ключ *NoFavoritesMenu* с целью скрытия пункт меню «Избранное» кнопки Пуск.
- Ключ *NoSetFolders* с целью скрытия пунктов меню «Принтеры» и «Панель управления» из меню «Настройка» кнопки Пуск.
- Ключ *NoWindowsUpdate* с целью скрытия пункта «WindowsUpdate» из меню Настройки кнопки Пуск.
- Ключ *NoSetTaskbar* с целью скрытия «Панели задач» и меню Пуск из меню «Настройка» кнопки Пуск.
- Ключ *NoSetActiveDesktop* с целью скрытия пункта «Рабочий стол ActiveDesktop» из меню Настройка кнопки Пуск.
- Ключ *NoChangeStartMenu* с целью запрета контекстного меню кнопки Пуск
- Ключ *NoRecentDocsHistory* с целью очистки недавно открытых документов.

• Ключ *ClearRecentDocsOnExit* с целью очистки списка недавно открытых документов при выходе.

• Ключ *NoTrayContextMenu* с целью запрета контекстного меню для Панели задач.

• Ключ *NoFolderOptions* с целью запрета пункта «Свойства папок» из Меню настройка кнопки Пуск.

• Ключ *NoViewContextMenu* с целью запрета контекстного меню по правой клавише мыши на Рабочем столе.

• Ключ *NoCustomizeWebView* с целью запрета настройки вида конкретных папок Меню Вид команда Настроить вид папки.

Была экспортирована директорию *Explorer* с целю сохранения значений параметров реестра в файл и возможности возврата к настроенным параметрам на данном АРМ и ускоренной настройки других АРМ.

В рамках ограничения функционала *Панели управления* был создан ключ *NoDispCPL* в созданном разделе *System* с целью блокировки настройки пункта «Экран» в панели управления в целях обеспечения безопасности, так как настройками панели управления должен заниматься администратор. Также был создан ключ *NoChanginigWallpaper* в разделе *ActiveDesktop* с целью запрета изменения фонового изображения рабочего стола, 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).

В дальнейшем была рассмотрена возможность отключения возможности использования *панели управления* с целью ограничения возможности пользователя вносить изменения в систему. Для этого был настроен ключ *NoControlPanel*.

Для закрытия меню *Пуск* от редактирования с целью фиксирования доступных для работы пользователя приложений в соответствии с политикой конфиденциальности предприятия был создан ключ *NoChangeStartMenu*.