Цель работы:

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.

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.

Механизм ИПС позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска. Перечень программ, разрешенных для запуска, может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей.

Организация ИПС средствами ОС Windows осуществляется сокрытием от пользователя части элементов интерфейса путём присвоения параметрам реестра ОС определенных значений (например, скрытие элементов рабочего стола, скрытие пункта меню «Выполнить» кнопки «Пуск», запрет контекстного меню кнопки «Пуск», запрет контекстного меню для «Панели задач» и др.). При этом параметры реестра различных версий ОС Windows могут значительно различаться.

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. 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.

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.

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».

После того, как все параметры добавлены, можно экспортировать всю директорию Explorer в отдельный файл, для удобства работы с реестром путем редактирование отдельного файла.

Тип ИС закрытого контура в соответствие с вариантом – **2Б**

Требования к классу защищенности 2Б:

Подсистема управления доступом:

Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и 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;
- результат попытки входа: успешная или неуспешная (при НСД);
- должен проводиться учет всех защищаемых носителей информации с помощью их 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 во время обработки и (или) хранения защищаемой информации;
- 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, предусматрива ющие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Подсистемы и требования	Класс 2Б
1. Подсистема управления доступом	
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
в систему	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-
к программам	-
к томам, каталогам, файлам, записям, полям записей	-
1.2. Управление потоками информации	
2. Подсистема регистрации и учета	
2.1. Регистрация и учет:	
входа (выхода) субъектов доступа в (из) систему (узел сети)	+
выдачи печатных (графических) выходных документов	-
запуска (завершения) программ и процессов (заданий, задач)	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-
изменения полномочий субъектов доступа	-
создаваемых защищаемых объектов доступа	-
2.2. Учет носителей информации	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-
2.4. Сигнализация попыток нарушения защиты	-
3. Криптографическая подсистема	
3.1. Шифрование конфиденциальной информации	-

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-
4. Подсистема обеспечения целостности	
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+
4.3. Наличие администратора (службы) защиты информации в АС	-
4.4. Периодическое тестирование СЗИ НСД	+
4.5. Наличие средств восстановления СЗИ НСД	+
4.6. Использование сертифицированных средств защиты	-

Ход выполнения 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».

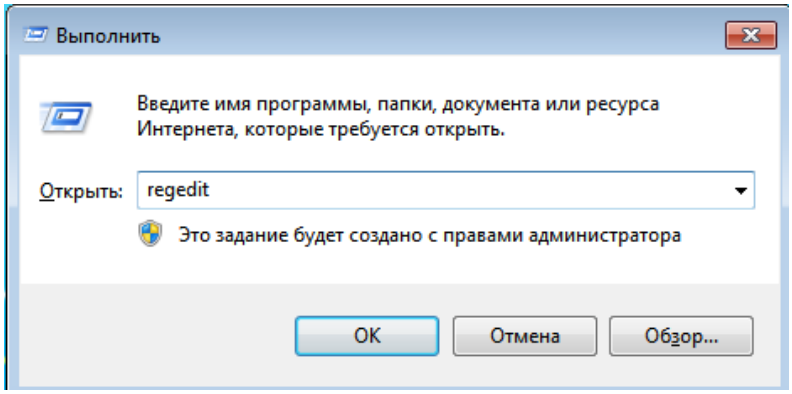

Рисунок 1 – Вызов редактора реестра

Для работы нам 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.

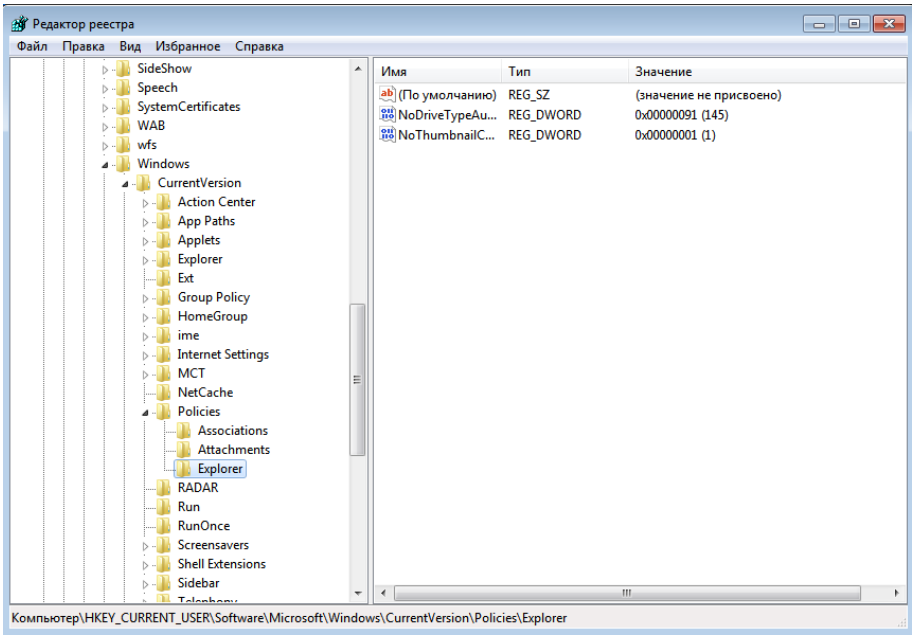

Рисунок 2 – Папка Explorer

Как видно из Рисунка 2, в папке Explorer уже есть несколько параметров, но они нас сейчас не интересуют, оставим их без изменения и начнем создавать свои параметры.

Сделать это очень просто: *Выделить раздел реестра Explorer → ПКМ → Создать → Параметр DWORD (32 бита)*.

На скриншоте ниже приведена визуальная инструкция для создания.

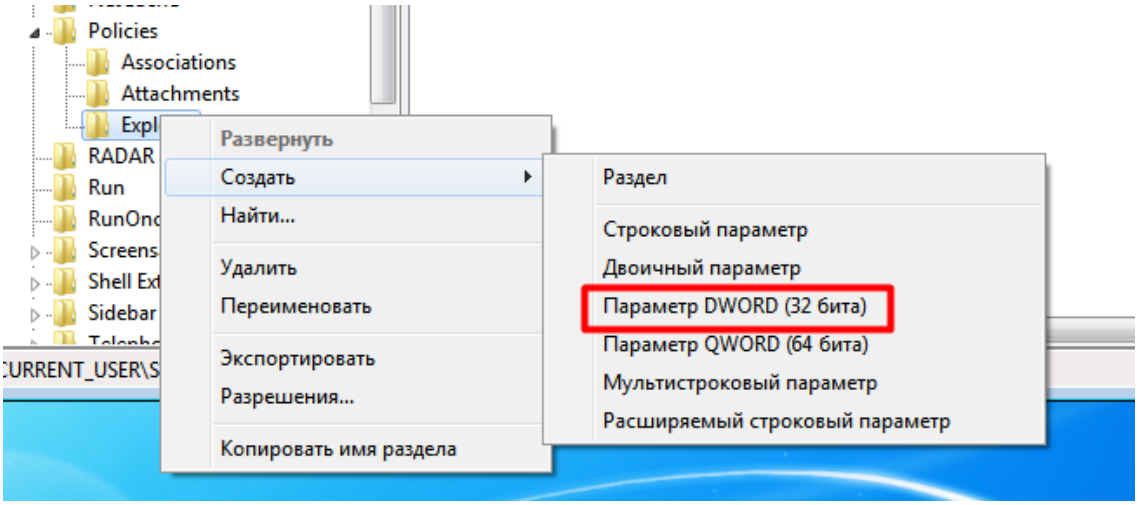

Рисунок 3 – Создание собственного параметра

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».

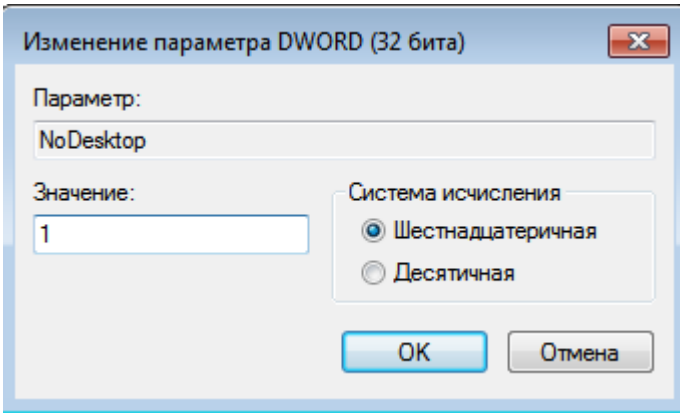

Рисунок 4 – Изменение параметра

Параметр «NoDesktop» позволяет скрыть все элементы («ярлыки») на рабочем столе. Данная мера ограничивает действия пользователя в установке лишних ярлыков на рабочем столе.

После перезагрузки видим следующую картину:

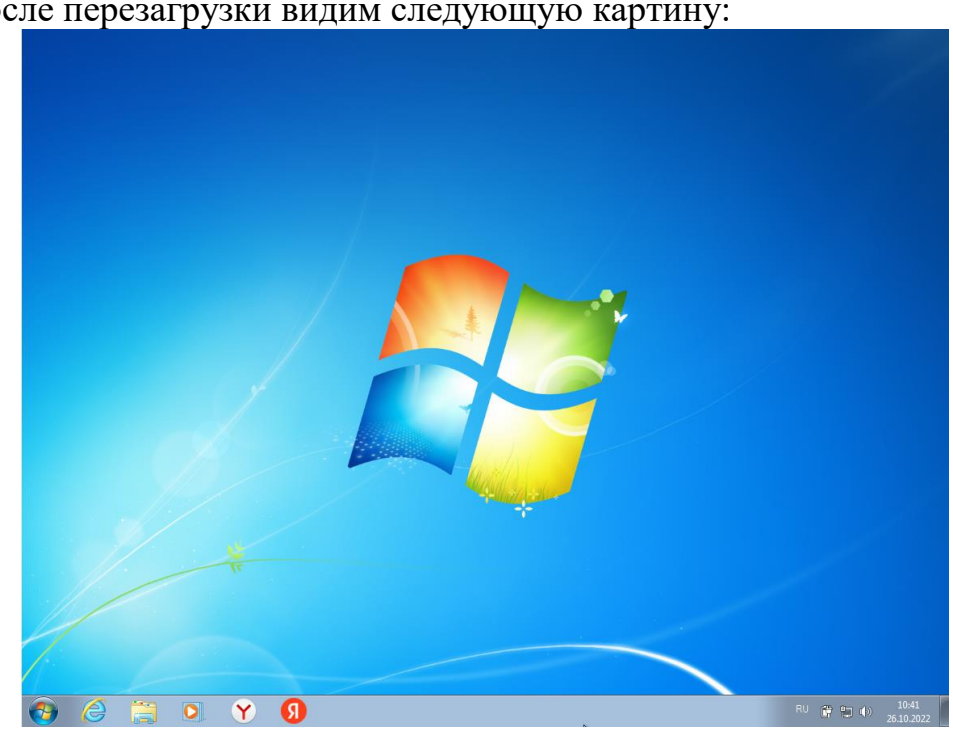

Рисунок 5 – Демонстрация изменения реестра

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»

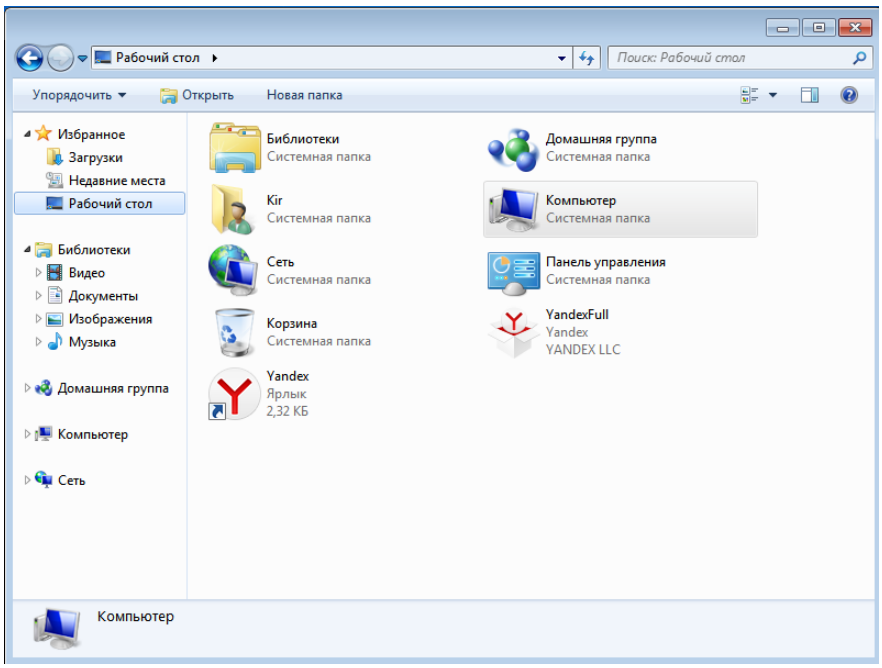

Рисунок 6 – Содержимое рабочего стола

Внесем в реестр остальные нужные параметры. Для удобства все параметры были объединены в одну таблицу.

Таблица 1: Параметры реестра

Название параметра	**Тип**	**Значение**	**Описание**
NoDesktop	DWORD	1	Скрытие элементов рабочего стола
NoRun	DWORD	1	Скрыть пункт меню «Выполнить» кнопки Пуск
NoFind	DWORD	1	Скрыть пункт меню «Найти» кнопки Пуск
NoRecentDocsMenu	DWORD	1	Скрыть пункт меню «Документы» кнопки Пуск
NoFavoritesMenu	DWORD	1	Скрыть пункт меню «Избранное» кнопки Пуск
NoSetFolders	DWORD	1	Скрытие пунктов меню «Принтеры» и «Панель управления» из меню «Настройка» кнопки Пуск
NoWindowsUpdate	DWORD	1	Скрытие пункта «WindowsUpdate» из меню Настройки кнопки Пуск
NoSetTaskbar	DWORD	1	Скрытие «Панели задач» и меню Пуск из меню «Настройка» кнопки Пуск

NoSetActiveDesktop	DWORD	1	Скрытие пункта «Рабочий стол ActiveDesktop» из меню Настройка кнопки Пуск
NoChangeStartMenu	DWORD	1	Запрет контекстного меню кнопки Пуск
NoRecentDocsHistory	DWORD	1	Очистка недавно открытых документов
ClearRecentDocsOnExit	DWORD	1	Очистка списка недавно открытых документов при выходе
NoTrayContextMenu	DWORD	1	Запрет контекстного меню для Панели задач
NoFolderOptions	DWORD	1	Запрет пункта «Свойства папок» из Меню настройка кнопки Пуск
NoViewContextMenu	DWORD	1	Запрет контекстного меню по правой клавише мыши на Рабочем столе
NoCustomizeWebView	DWORD	1	Запрет настройки вида конкретных папок Меню Вид команда Настроить вид папки

После создания новый параметров, папка Explorer выглядит так:

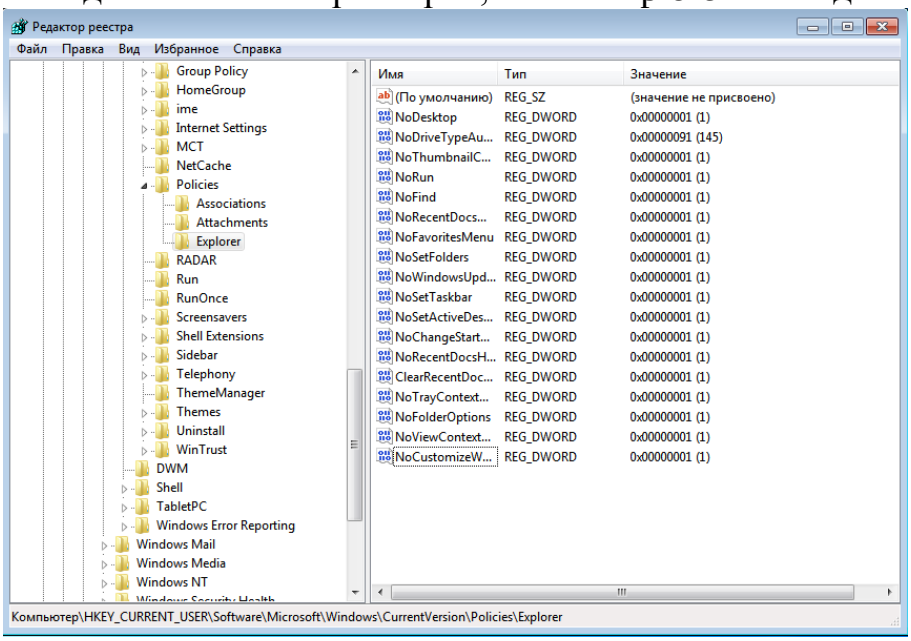

Рисунок 7 – Содержимое папки Explorer

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*

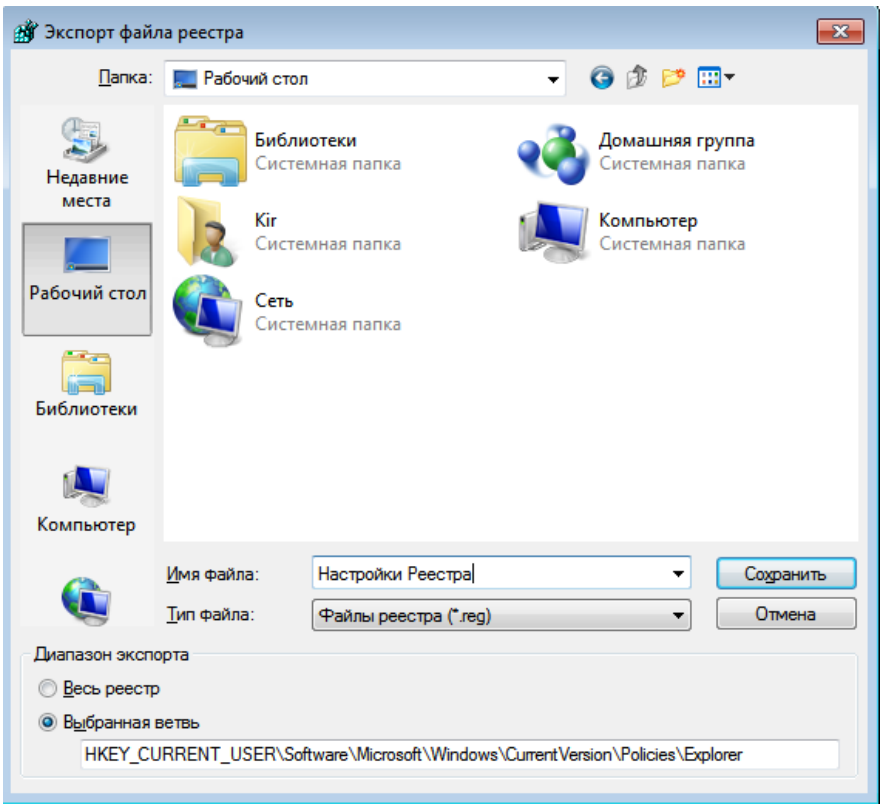

Рисунок 8 – Место сохранения файла реестра

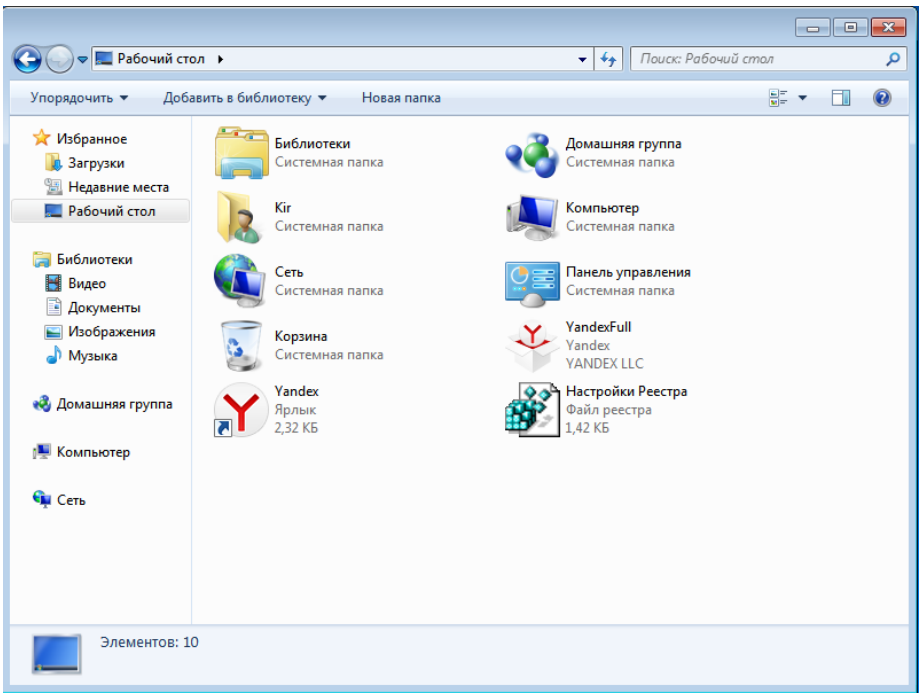

Рисунок 9 – Файл реестра на рабочем столе

После экспортирования раздела реестра с REG-файлами, которые он содержит, можно работать, как с обычным текстовым файлом, используя для этого стандартные текстовые редакторы, например, «Блокнот».

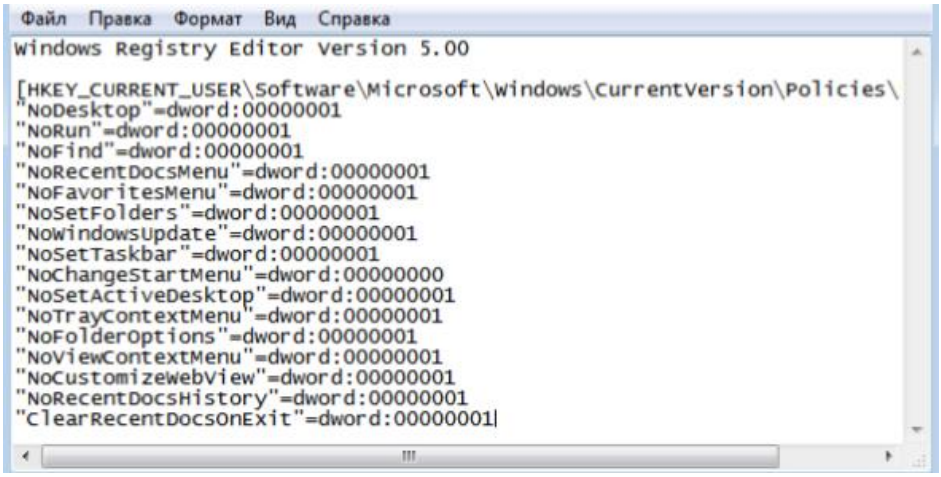

Рисунок 10 – Файл реестра в блокноте

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.

После редактирования реестра полезно будет проанализировать изменения.

Например, вот что произошло с меню «Пуск» после редактирования реестра.

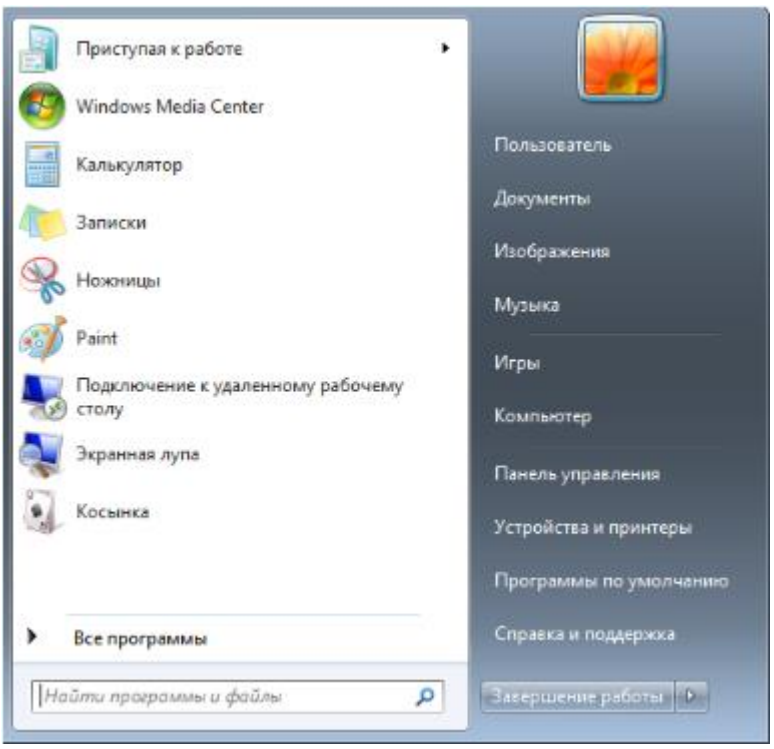

Рисунок 10 – Меню «Пуск» до редактирования

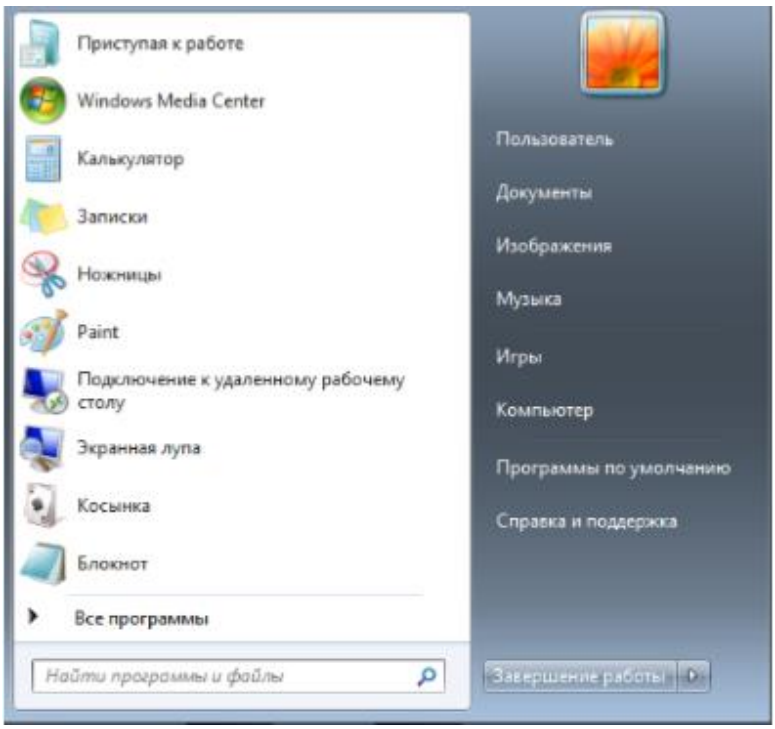

Рисунок 10 – Меню «Пуск» после редактирования

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.

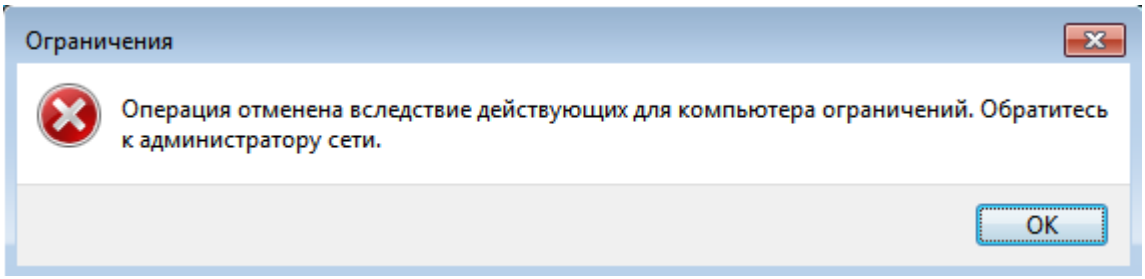

Рисунок 11 – Сообщение об ограничении прав

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

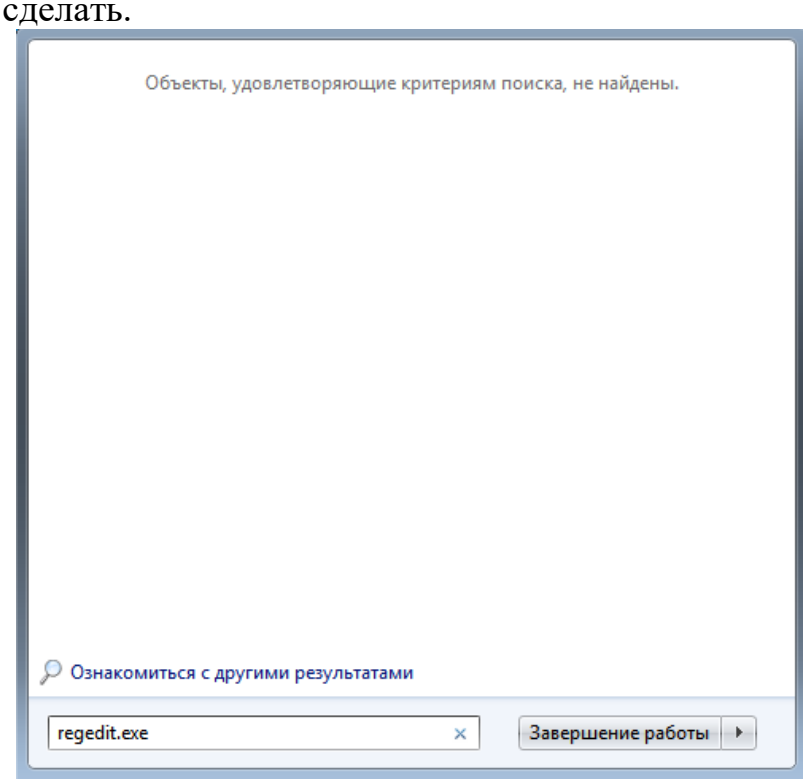

Рисунок 12 – Результат применения параметра NoSetFolders

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 exe-файл, 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 C.

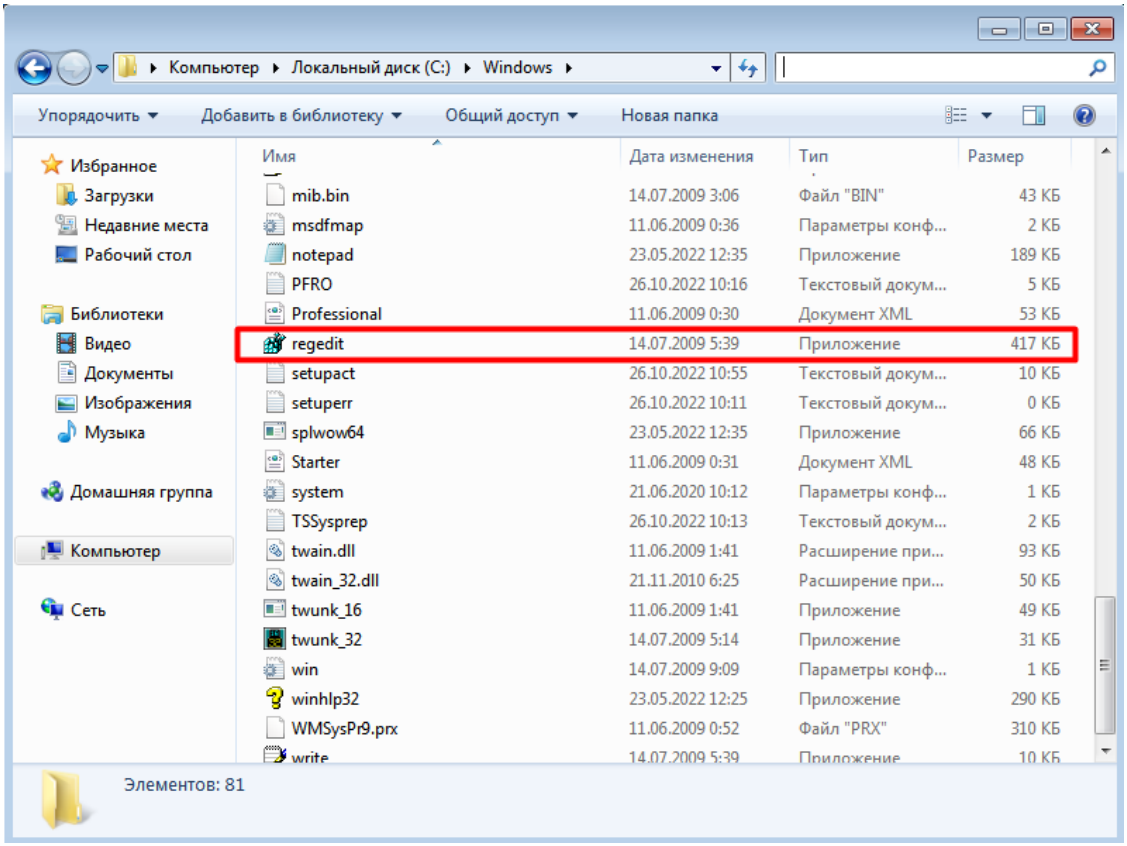

Рисунок 13 – Приложение regedit.exe

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

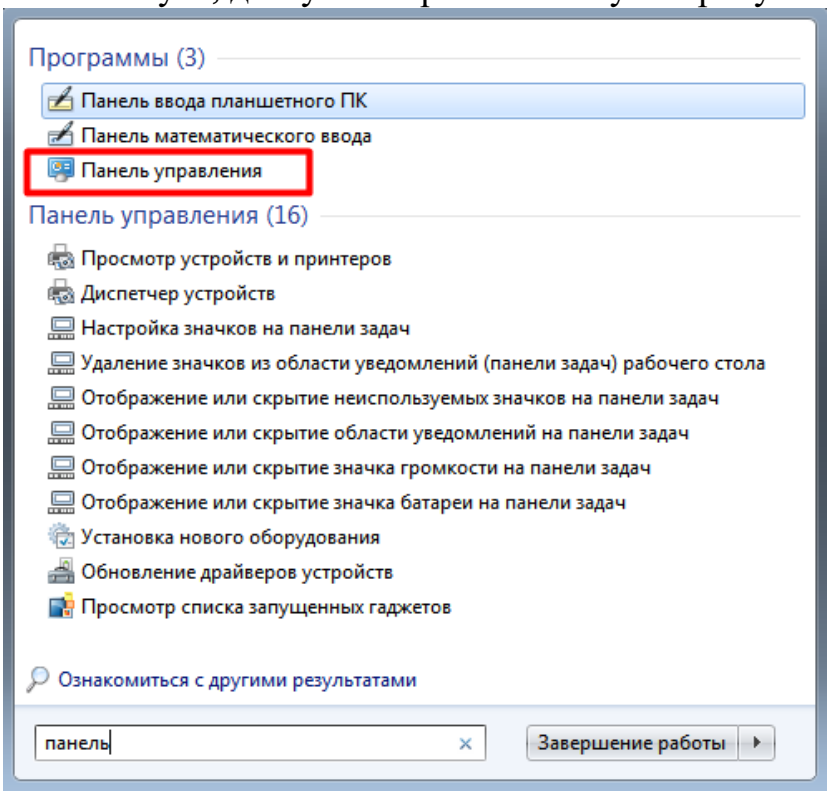

Рисунок 14 – Панель управления в поиске

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».

В качестве примера заблокируем настройки пункта «Экран» (параметр NoDispCPL) панели управления и заблокируем возможность изменения обоев рабочего стола пункта «Персонализация» панели управления (параметр NoChangingWallpaper). 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).

Для этого следует создать в директории Policies новые разделы *System и ActiveDesktop*:

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

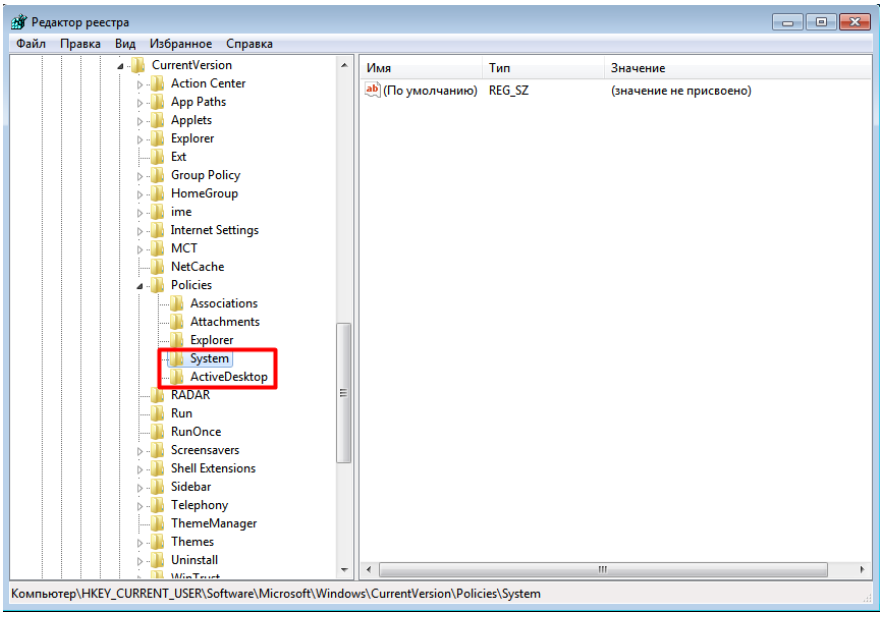

Рисунок 15 – Новые папки System и ActiveDesktop

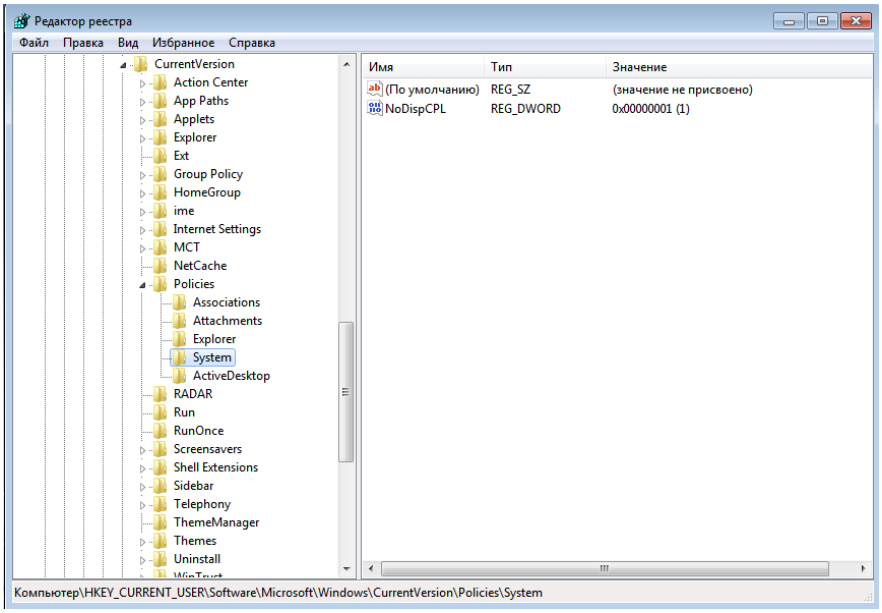

Рисунок 16 – Новый параметр в папке System

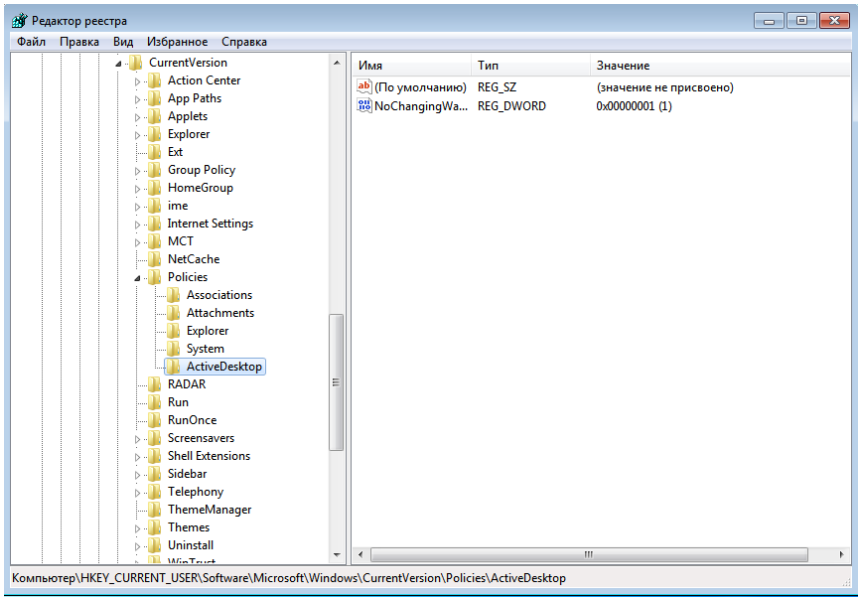

Рисунок 17 – Новый параметр в папке Active Desktop

После внесения новых параметров и перезагрузки компьютера проверяем функционал.

Настройки экрана до внесения изменений:

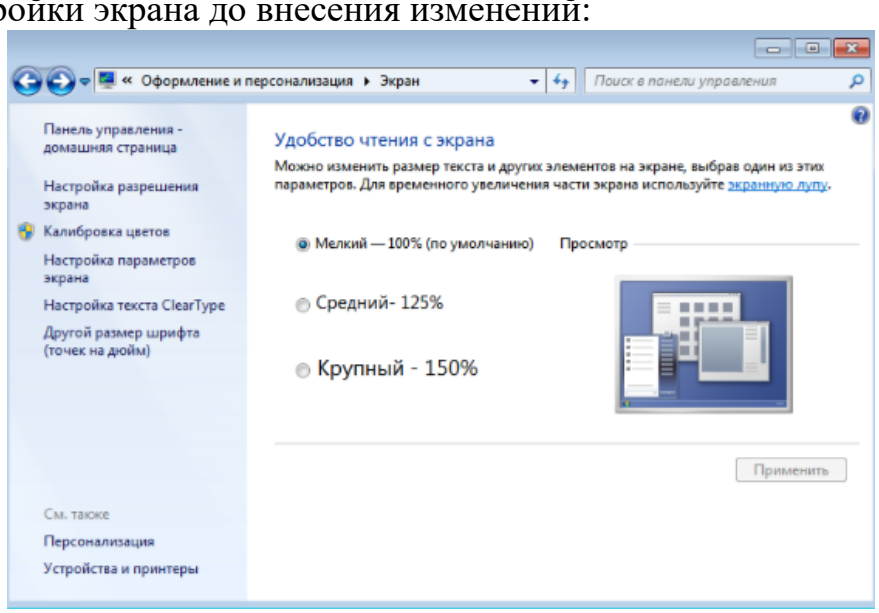

Рисунок 18 – Настройки до внесения изменений

Настройки экрана после внесения изменений:

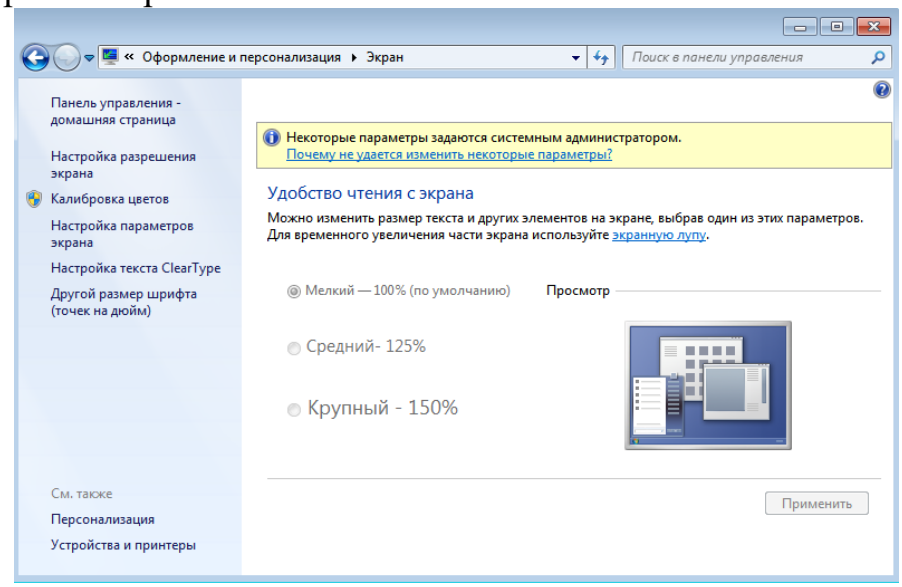

Рисунок 19 - Настройки после внесения изменений

Настройки персонализации до внесения изменений:

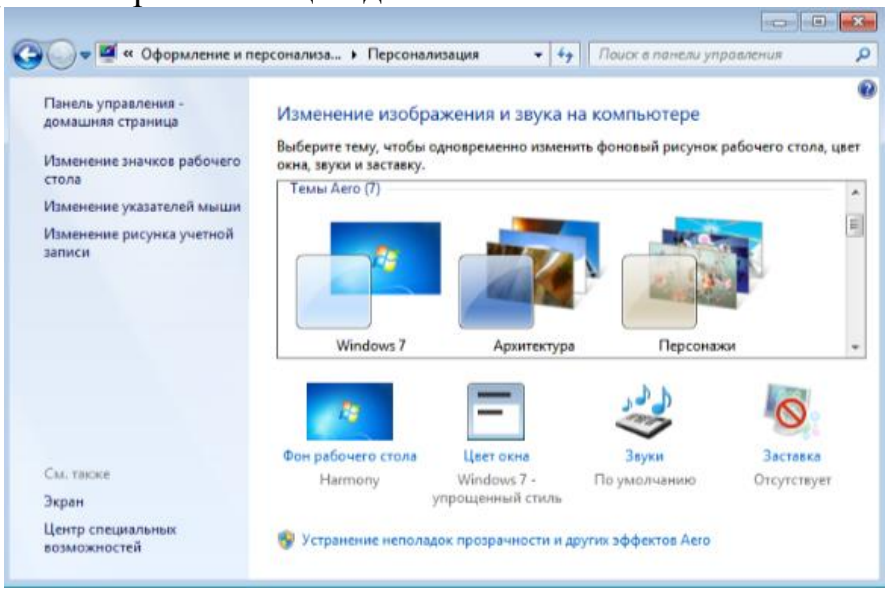

Рисунок 20 - Настройки до внесения изменений

Настройки персонализации после внесения изменений:

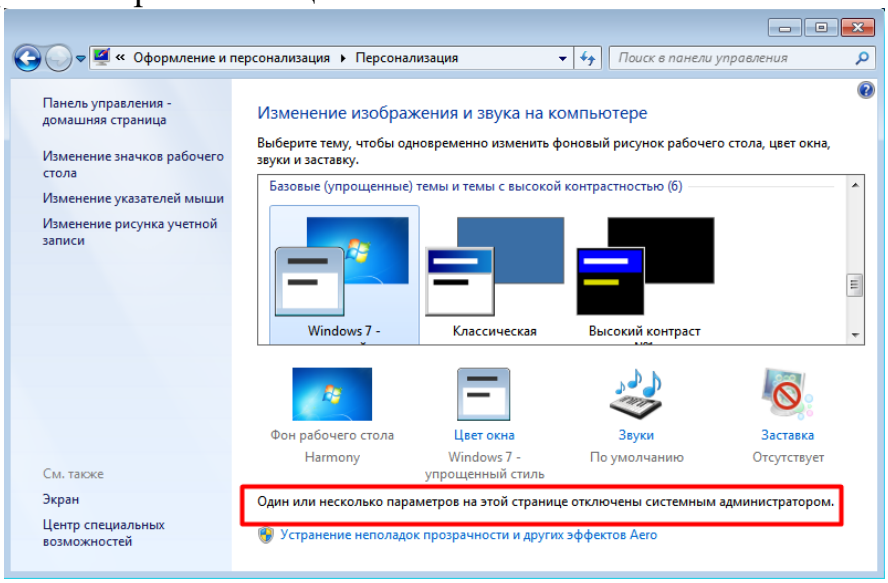

Рисунок 21 - Настройки после внесения изменений

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:

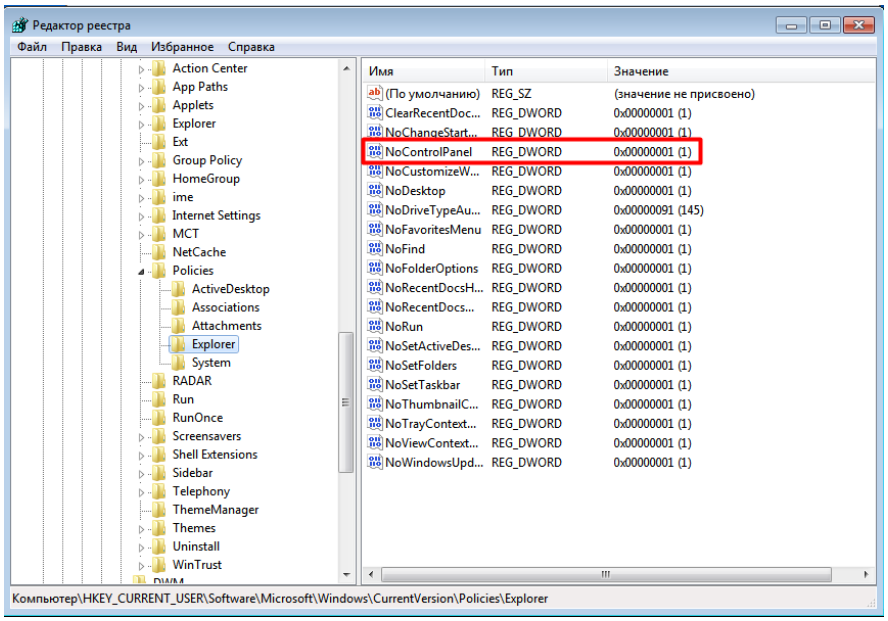

Рисунок 22 – Новый параметр в папке Explorer

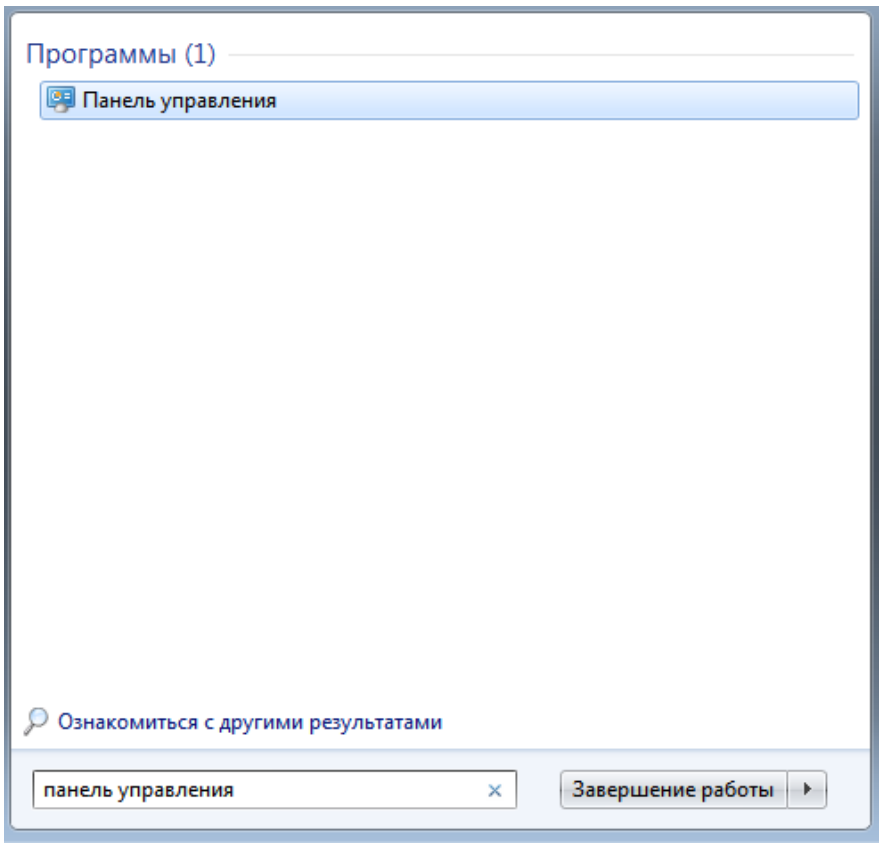

Рисунок 23 – Вызов панели управления до редактирования реестра

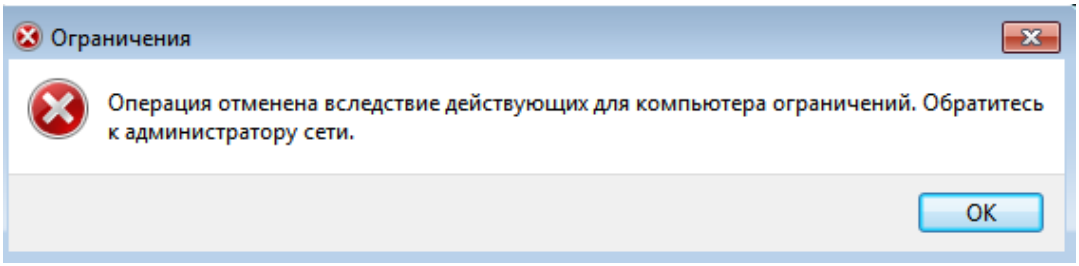

Рисунок 24 – Вызов панели управления после редактирования реестра

В качестве ещё одного примера, можно показать, что раньше пользователь имел больше функционала в меню «Пуск».

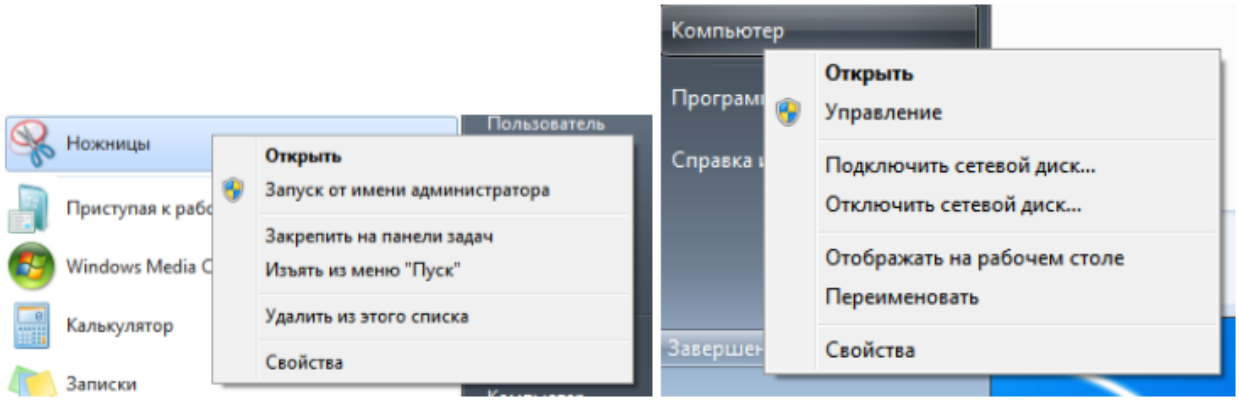

Рисунок 26 – Функционал до редактирования реестра

После редактирования использование кнопки ПКМ стало не доступно.

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

Выводы:

В лабораторной работе была изучена и настроена изолированная программная среда на АРМ «закрытого» контура ИС средствами ОС Windows 7 с целью защиты АРМ от НСД. В ходе данной лабораторной работы было изучено следующее:

- как вызывать реестр для настройки безопасности сети;
- как добавлять параметры в разделы реестра;
- как устанавливать значения для конкретных параметров реестра;
- как экспортировать настройки реестра для последующего упрощения конфигурации.

В частности, были осуществлены следующие настройки:

- Редактирование ключей реестра раздела Explorer для ограничения функционала рабочего стола и меню «Пуск» пользователя;
- Редактирование реестра для ограничения функционала «Панели управления» пользователя;
- 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.

Проведенные настройки реестра значительно ограничивают работу пользователя в системе. С точки зрения защиты от НСД к АРМ усложняется работа злоумышленника при успешном внедрении в систему. Например, злоумышленник лишен возможности просмотреть недавно открытые файлы пользователя, а также воспользоваться возможностями пункта меню «Выполнить» кнопки «Пуск» для открытия нужных ресурсов и так далее. После настройки ИПС ни пользователь, ни злоумышленник не смогут получить доступ к закрытым данным и/или повлиять на работу системы в целом. Изолированная программная среда существенно повышает защищенность системы от программных закладок, т.к. вредоносное ПО чаще всего нарушает работу ОС путем редактирования реестра.

В то же время ИПС создает определенные сложности в администрировании защищаемой системы. Неправильная настройка параметров может привести к некорректной работе операционной системы. Например, при установке нового программного продукта администратор обязан модифицировать списки разрешенных программ для пользователей, с учетом того, что они должны иметь возможность работать с этим программным продуктом.

Что же касается требования ФСТЭК к классу защищенности 2Б, ограничения прав пользователей базы данных помогает выполнить пункт **4.1.** «Обеспечение целостности программных средств и обрабатываемой информации».