

Университет ИТМО

Лабораторная работа №3

«Разграничение доступа к реестру»

По дисциплине «Информационная безопасность»

Вариант 10.

Выполнили: Ванцев А. О.

Есаков К. И.

Сорокин С. С.

Группа: Р3400

Преподаватель: Маркина Т. А.

2020 г.

Цель работы:

Целью работы является изучение инструментов для работы с реестром, разграничение доступа к реестру, изменение и создание полей, для изменения состояния системы.

Реестр – это база данных для хранения сведений о конфигурации компьютера и настроек операционной системы.

Программно-аппаратные средства используемые при выполнении работы:

Лабораторная работа выполнена на компьютере с установленной операционной системой «Windows 10». Все операции, совершаемые с реестром, выполнены при помощи программы «Редактор реестра».

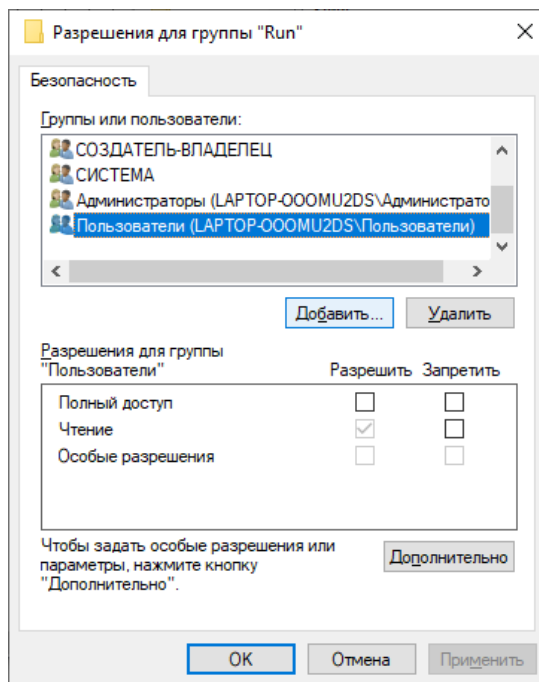
Основная часть:

1. Какие конкретно ветки и ключи доступны пользователю хотя бы на чтение; только Администратору, только System:

Для защиты ключей реестра в системе Windows используются списки контроля доступа (Access Control List, ACL). Она представляет собой базу данных с информацией о правах доступа к конкретным объектам операционной системы, в том числе и к ключам реестра.

Посмотреть какие права стоят у конкретной ветки можно при помощи «Редактора реестра», нажав на ветку правой кнопкой мыши и перейдя в меню «Разрешения...»

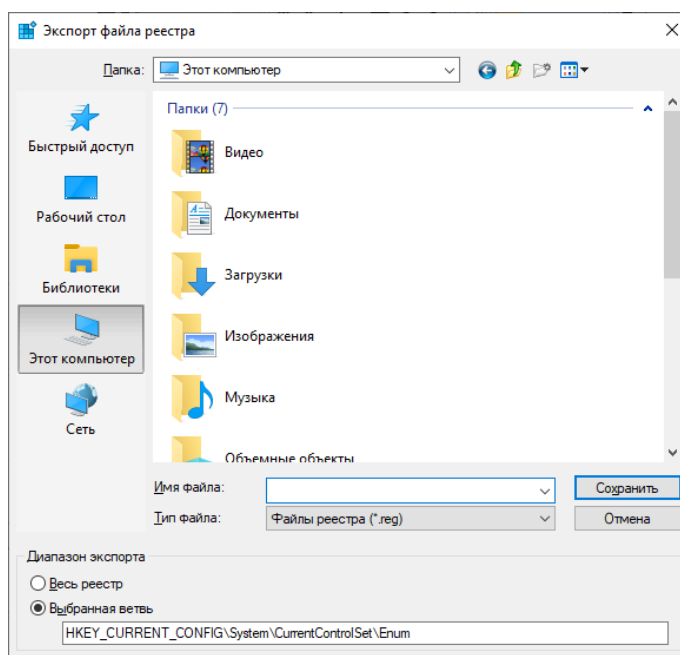
При помощи этого меню можно просматривать и изменять права для конкретных веток реестра.



2. Описание резервного копирования реестра:

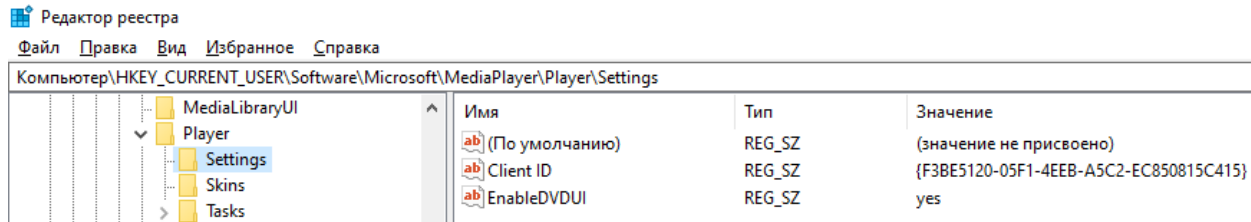
Перед тем как начать работу с реестром, рекомендуется создать резервную копию веток, которые требуется изменить.

Для того, чтобы создать резервную копию, необходимо нажать правой кнопкой мыши по ветке, копию которой вы хотите сделать, и перейти в меню «Экспортировать». После этого появится окно, где необходимо указать путь, куда сохранить резервную копию.



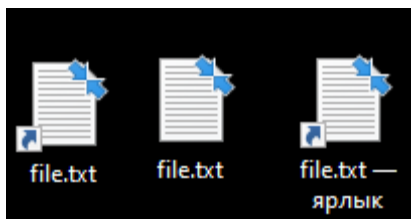
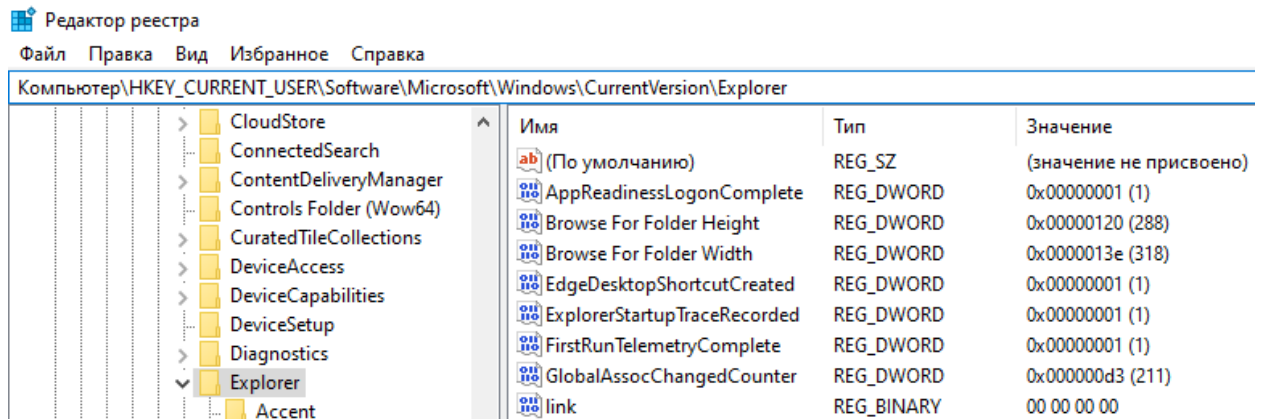
3. Задание по варианту:

- а) Включение доступа к настройкам DVD в Windows Media Player:
Для того, чтобы включить доступ к настройкам DVD в Windows Media Player, нужно создать строковый параметр «EnableDVDUI» в ветке HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\Settings и установить у него значение «yes».



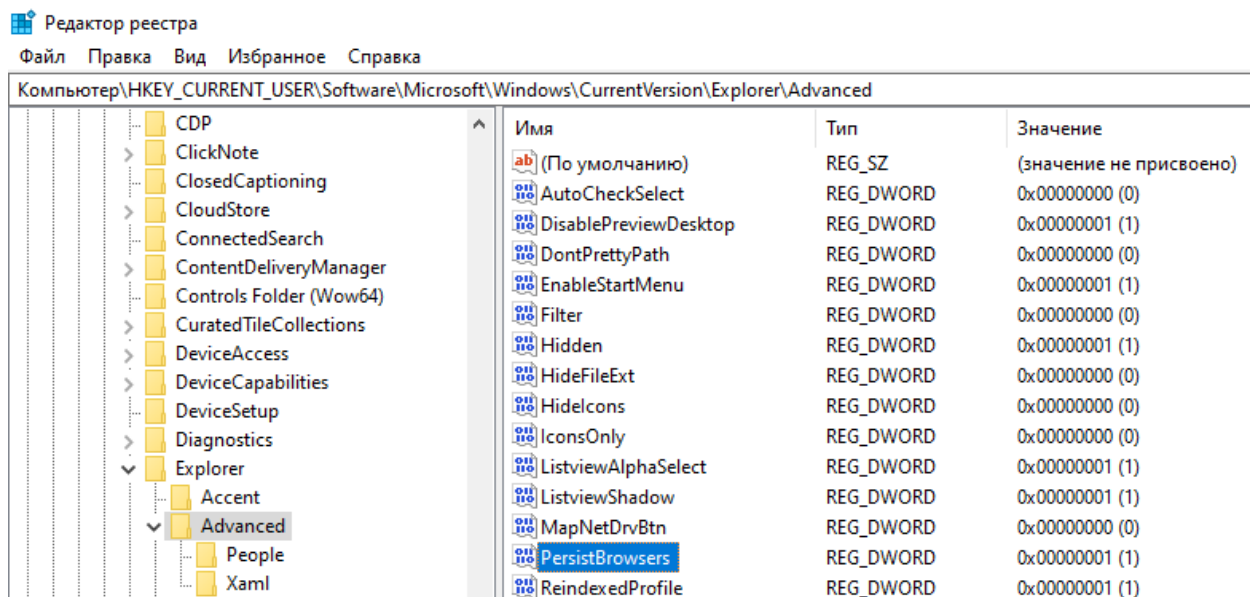
- б) Отключение добавления приставки «— ярлык» к названию ярлыков при их создании.

Для того чтобы отключить приставку в названии ярлыков, нужно изменить двоичный параметр «link» в ветке HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer на значение 00 00 00 00. После чего, чтобы изменения вступили в силу, необходимо перезапустить процесс «explorer».



- с) Включение автоматического открытия папок после загрузки системы, если они не были закрыты пользователем перед перезагрузкой.

Для того чтобы восстанавливать прежние окна папок при входе в систему, нужно создать параметр DWORD «PersistBrowsers» в ветке HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced и установить значение 0x00000001.



Выводы:

В ходе выполнения данной лабораторной работы, мы познакомились с понятием реестр в операционной системе «Windows». Узнали, как просматривать и изменять права доступа к разделам реестра для разных групп пользователей. Научились изменять параметры системы при помощи реестра. Данный навык является крайне полезным, так как далеко не все параметры можно изменять привычными способами, используя графический интерфейс.