ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

Способы добавления в автозагрузку

Пакулов Артур

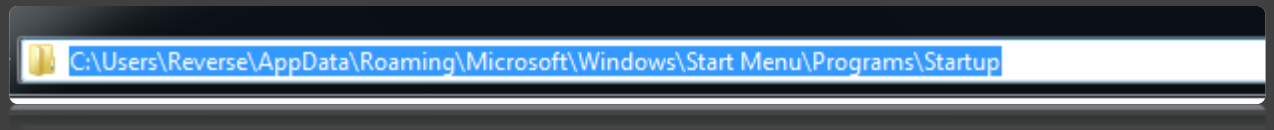
- Постоянный запуск после рестарта OS Windows
- Одноразовый запуск после рестарта OS Windows
- Косвенный автозапуск

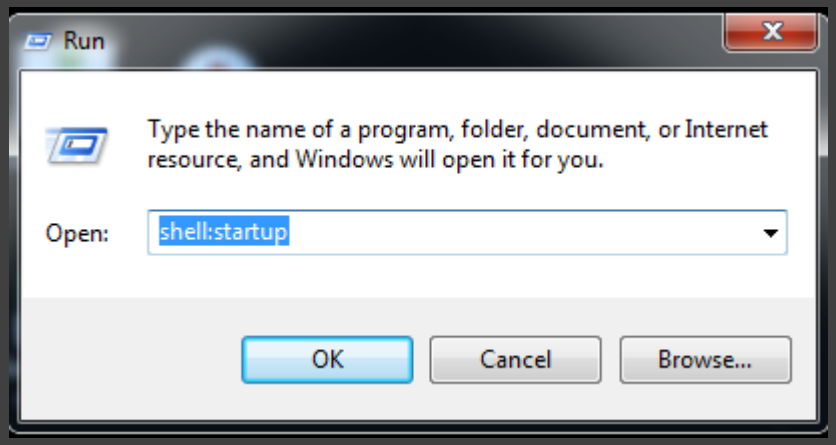
1

Стандартные техники

Папка «автозапуска»

```
WIN+R shell:startup
```





Определение пути

`GetSpecialFolderPath – получить путь к «специальной» папке`

SHGetSpecialFolderPathA function

12/05/2018 • 2 minutes to read

[**SHGetSpecialFolderPath** is not supported. Instead, use ShGetFolderPath.]

Retrieves the path of a special folder, identified by its CSIDL.

Syntax

C++

```
BOOL SHGetSpecialFolderPathA(
  HWND  hwnd,
  LPSTR pszPath,
  int   csidl,
  BOOL  fCreate
);
```

Определение пути

CSIDL_ALTSTARTUP - id пути дириктории с автозапуском

CSIDL (constant special item ID list)

```
#ifndef CSIDL_LOCAL_APPDATA
#define CSIDL_LOCAL_APPDATA             0x001c        // <user name>\Local Settings\Applicaiton Data (non roaming)
#endif // CSIDL_LOCAL_APPDATA

#define CSIDL_ALTSTARTUP                0x001d        // non localized startup
#define CSIDL_COMMON_ALTSTARTUP         0x001e        // non localized common startup
#define CSIDL_COMMON_FAVORITES          0x001f

#ifndef _SHFOLDER_H_
#define CSIDL_INTERNET_CACHE            0x0020
#define CSIDL_COOKIES                   0x0021
#define CSIDL_HISTORY                   0x0022
#define CSIDL_COMMON_APPDATA            0x0023        // All Users\Application Data
#define CSIDL_WINDOWS                   0x0024        // GetWindowsDirectory()
#define CSIDL_SYSTEM                    0x0025        // GetSystemDirectory()
#define CSIDL_PROGRAM_FILES             0x0026        // C:\Program Files
#define CSIDL_MYPICTURES                0x0027        // C:\Program Files\My Pictures
#endif // _SHFOLDER_H_
```

Пример кода

GetSpecialFolderPath – получить путь к «специальной» папке

```c
#include <Windows.h>
#include <Shlobj.h>
#include <stdio.h>

#pragma comment(lib, "Shell32.lib")


int main()
{
    bool status;
    char path[MAX_PATH];
    status = SHGetSpecialFolderPathA(NULL, path, CSIDL_ALTSTARTUP, false);
    printf("%s\n", path);
    system("pause");
    return 0;
}
```

Пример кода

Расположение этой папки определяется из реестра в слудющих разделах

HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\explorer\Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\explorer\User Shell Folders

Значение Common Startup можно переопределить

Ветка RUN

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

- запрос на вход

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- **Папка «Автозагрузка»**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

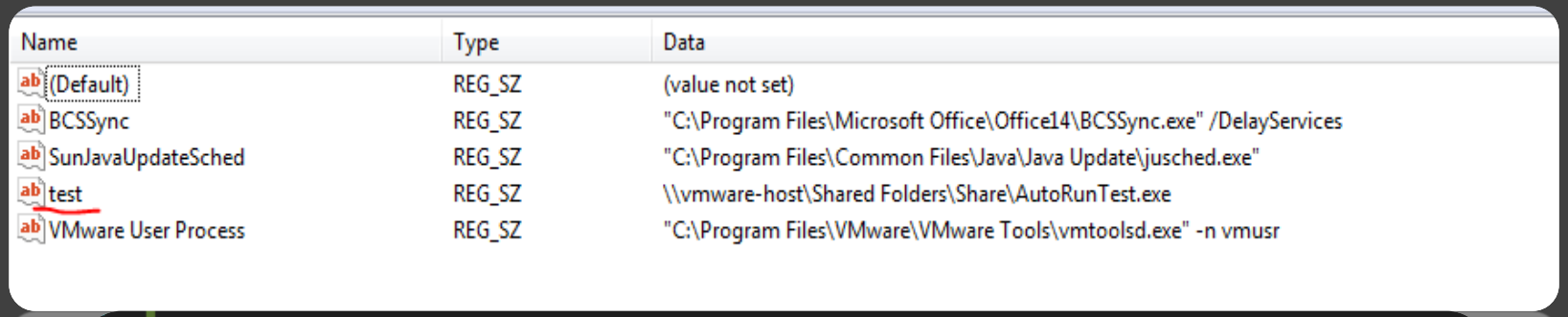
Пример кода (без проверок)

Последовательность вызовов:


```
10  void AddToRun()
11  {
12      HKEY newValue;
13      CHAR myPath[MAX_PATH];
14
15      GetModuleFileNameA(NULL, myPath, MAX_PATH);
16
17      RegOpenKeyA(HKEY_LOCAL_MACHINE, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", &newValue);
18
19      RegSetValueExA(newValue, "test", 0, REG_SZ, (LPBYTE)myPath, strlen(myPath));
20
21      RegCloseKey(newValue);
22  }
```

Пример кода

Результат:



Name	Type	Data
(Default)	REG_SZ	(value not set)
BCSSync	REG_SZ	"C:\Program Files\Microsoft Office\Office14\BCSSync.exe" /DelayServices
SunJavaUpdateSched	REG_SZ	"C:\Program Files\Common Files\Java\Java Update\jusched.exe"
test	REG_SZ	\\vmware-host\Shared Folders\Share\AutoRunTest.exe
VMware User Process	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

```
10  void AddToRun()
11  {
12      HKEY newValue;
13      CHAR myPath[MAX_PATH];
14
15      GetModuleFileNameA(NULL, myPath, MAX_PATH);
16
17      RegOpenKeyA(HKEY_LOCAL_MACHINE, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", &newValue);
18
19      RegSetValueExA(newValue, "test", 0, REG_SZ, (LPBYTE)myPath, strlen(myPath));
20
21      RegCloseKey(newValue);
22  }
```

Пример кода

OTUS

NgrBot

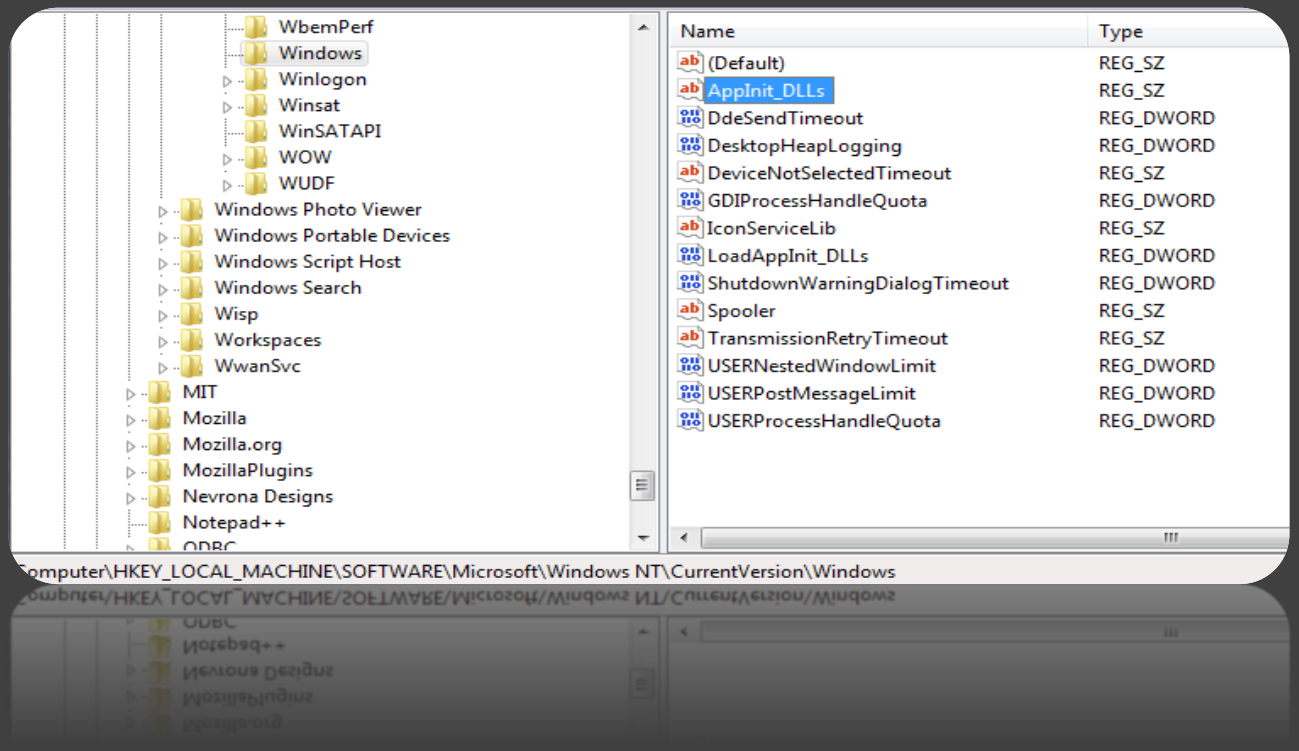
```
0457ED21: 68E0B35B04        push        0045BB3E0 ;'Wtfmfi' --↓7
.0457ED26: FFD3             call        ebx
.0457ED28: 8B0D98B95B04     mov         ecx,[0045BB998] --↓3
.0457ED2E: 50               push        eax
.0457ED2F: 68E0B35B04       push        0045BB3E0 ;'Wtfmfi' --↓7
.0457ED34: 51               push        ecx
.0457ED35: E80637FFFF       call        .004572440 --↑8
.0457ED3A: 68805B5804       push        004585B80 ;'Software\Microsoft\Windows\CurrentVersion\Run' --↓9
.0457ED3F: E84C49FFFF       call        .004573690 --↑A
.0457ED44: 8B1594B95B04     mov         edx,[0045BB994] --↓4
.0457ED4A: 83C404           add         esp,4
.0457ED4D: 50               push        eax
.0457ED4E: 680C2E5804       push        004582E0C ;'Software\Microsoft\Windows\CurrentVersion\Run' --↓B
.0457ED53: 52               push        edx
.0457ED54: E8E736FFFF       call        .004572440 --↑8
.0457ED59: 6850AC5B04       push        0045BAC50 ;'C:\Users\' --↓C
.0457ED5E: FFD3             call        ebx
.0457ED60: 50               push        eax
.0457ED61: A19CB95B04       mov         eax,[0045BB99C] --↓5
.0457ED66: 6850AC5B04       push        0045BAC50 ;'C:\Users\' --↓C
.0457ED6B: 50               push        eax
.0457ED6C: E8CF36FFFF       call        .004572440 --↑8
.0457ED71: 6A00             push        0
.0457ED73: 6A00             push        0
.0457ED75: 6890B95B04       push        0045BB990 --↓1
.0457ED7A: 6870E75704       push        00457E770 --↑D
.0457ED7F: 6A00             push        0
.0457ED81: 6A00             push        0
0457ED83: FFD6              call        esi
```

2

AppInit DLLs

Подгрузка DLL в контекст прцессов

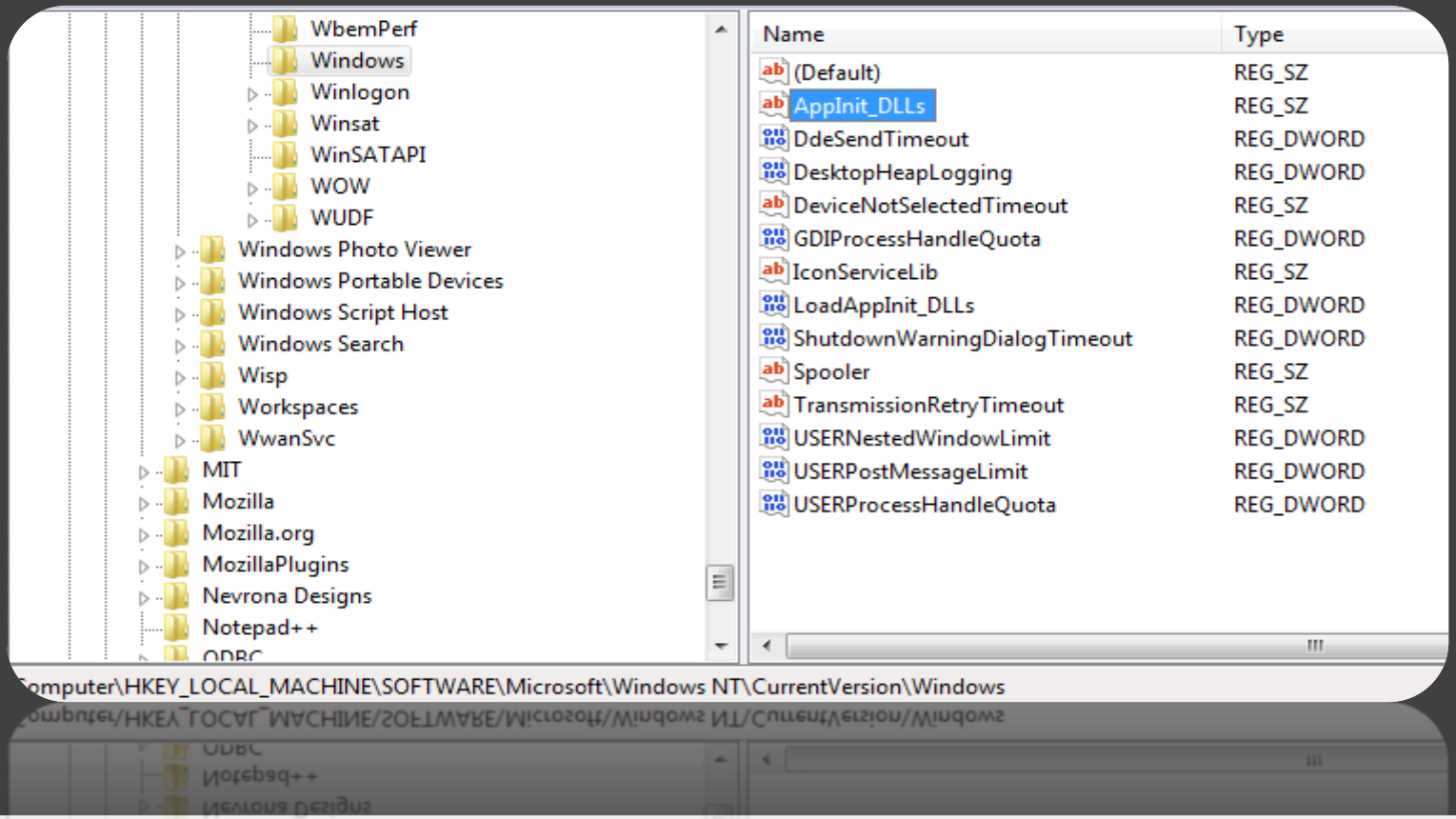
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs



Если в начало имени дописать нулевой байт, то его не будет видно

Подгрузка DLL в контекст прцессов

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs = 1

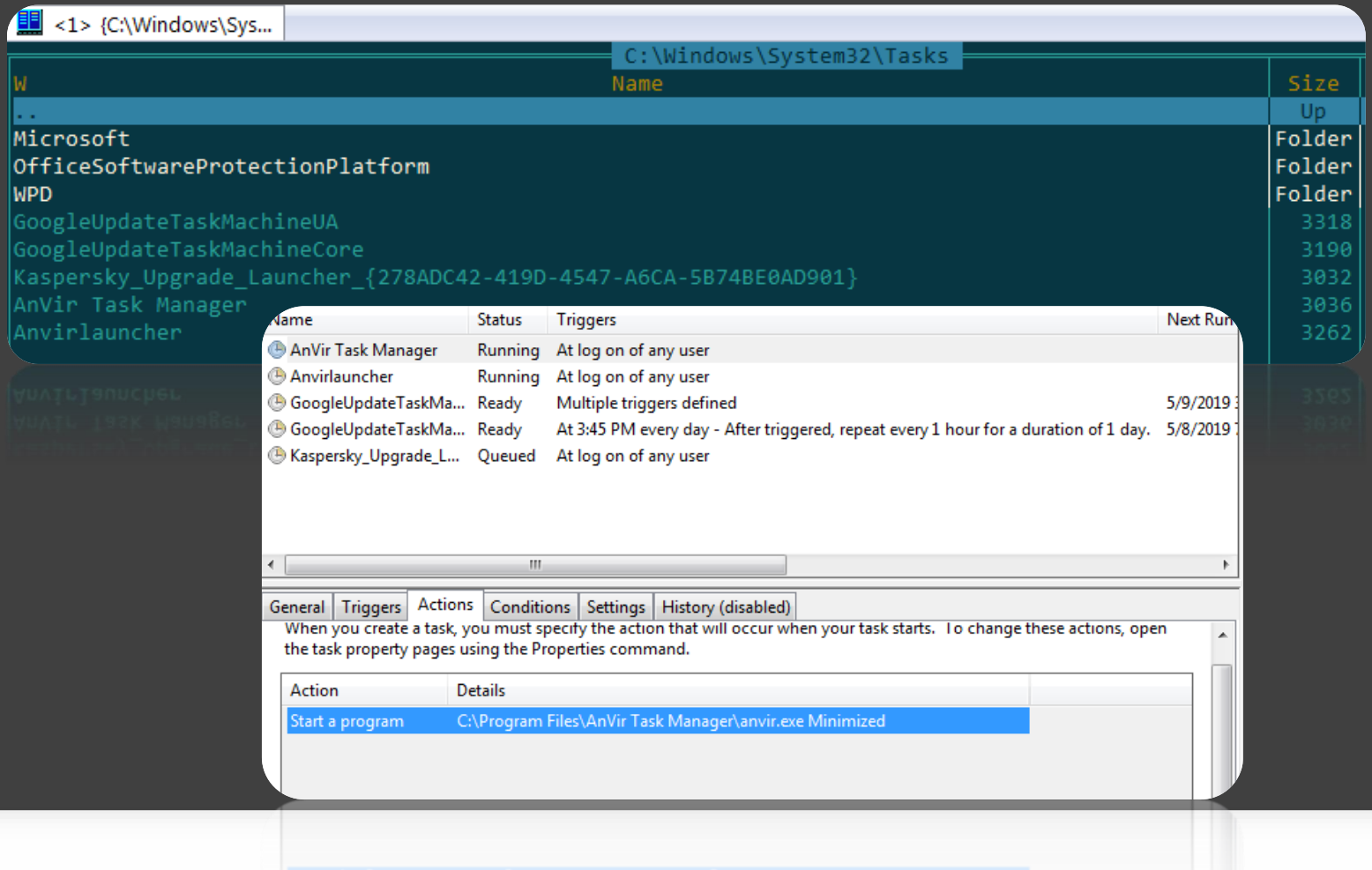


4

Task Scheduled

Task Scheduled

cd %Windir%\System32\Tasks



Задача описывается в XML файле

OTUS

```
C:\Windows\System32\Tasks\Kaspersky_Upgrade_Launcher_{278ADC42-419D-4547-A6CA-5B74BE0AD901}
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo />
  <Triggers>
    <LogonTrigger id="Trigger1">
      <Enabled>true</Enabled>
      <Delay>PT5H</Delay>
    </LogonTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <GroupId>Users</GroupId>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>5</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Program Files\Common Files\AV\Kaspersky Lab\upgrade_launcher.exe</Command>
      <Arguments>/waitUpgrade</Arguments>
    </Exec>
  </Actions>
</Task>
```

4

Image File Execution Options

Image File Execution Options (IFEO)

Используется для отладки. Позволяет запустить другую программу вместо конкретной

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\{name of the executable}

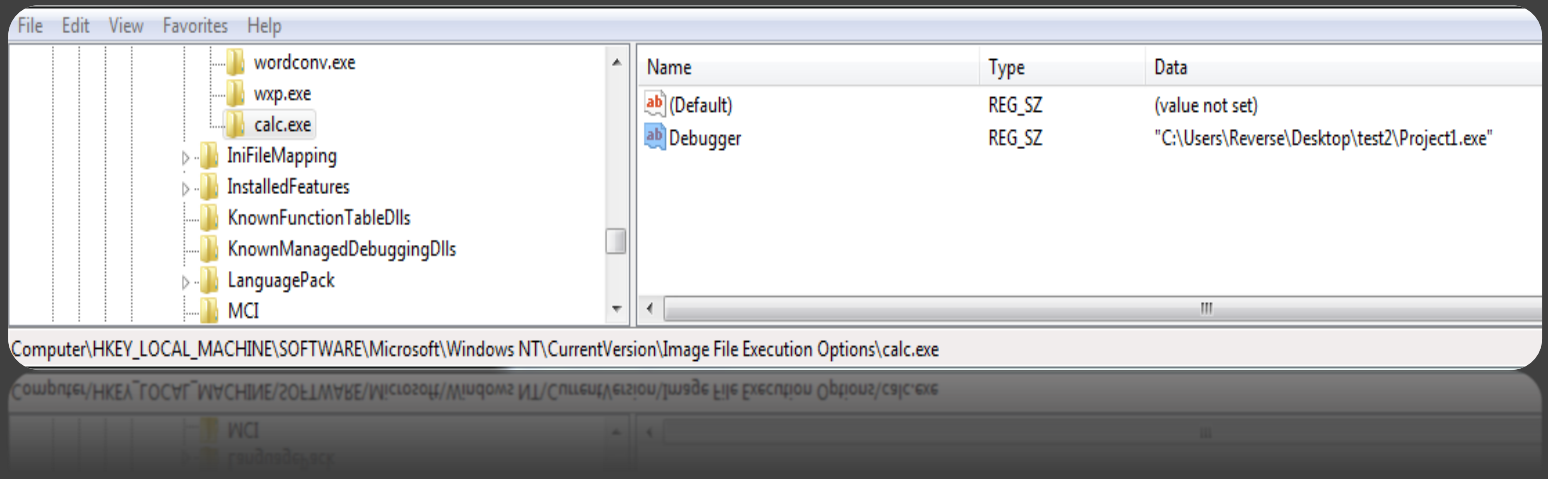
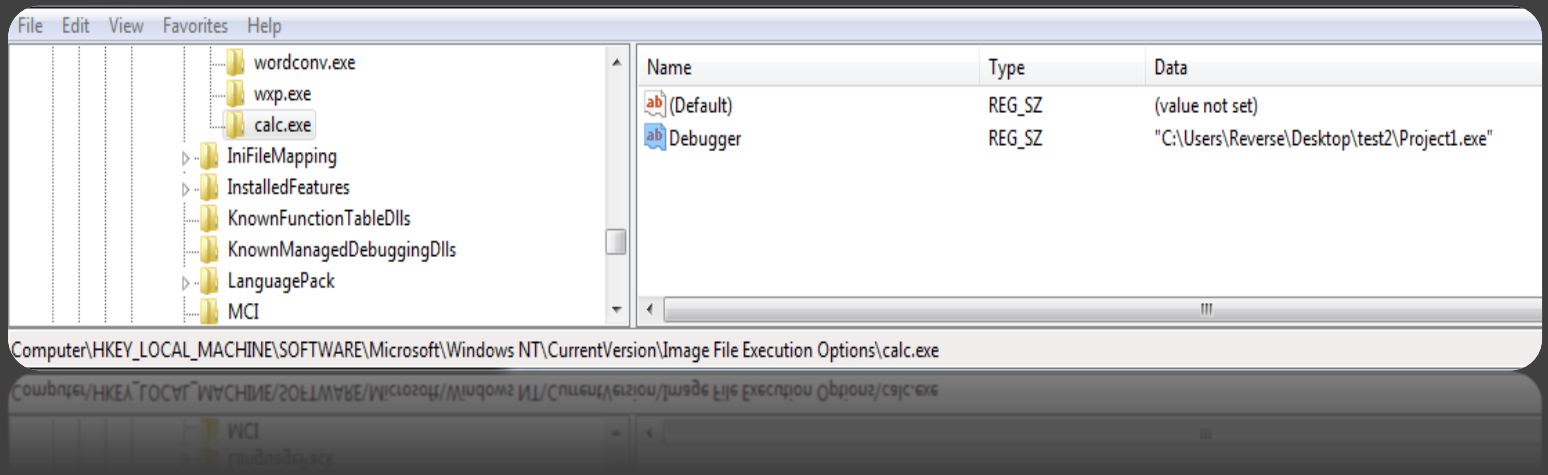


Image File Execution Options (IFEO)

Для этого создаётся параметр с именем “Debugger” со значением пути другой программы

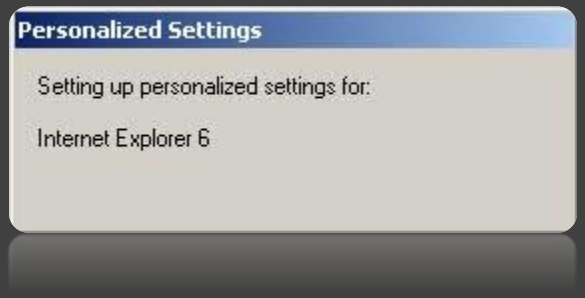


5

Active Setup

Что такое **Active Setup?**

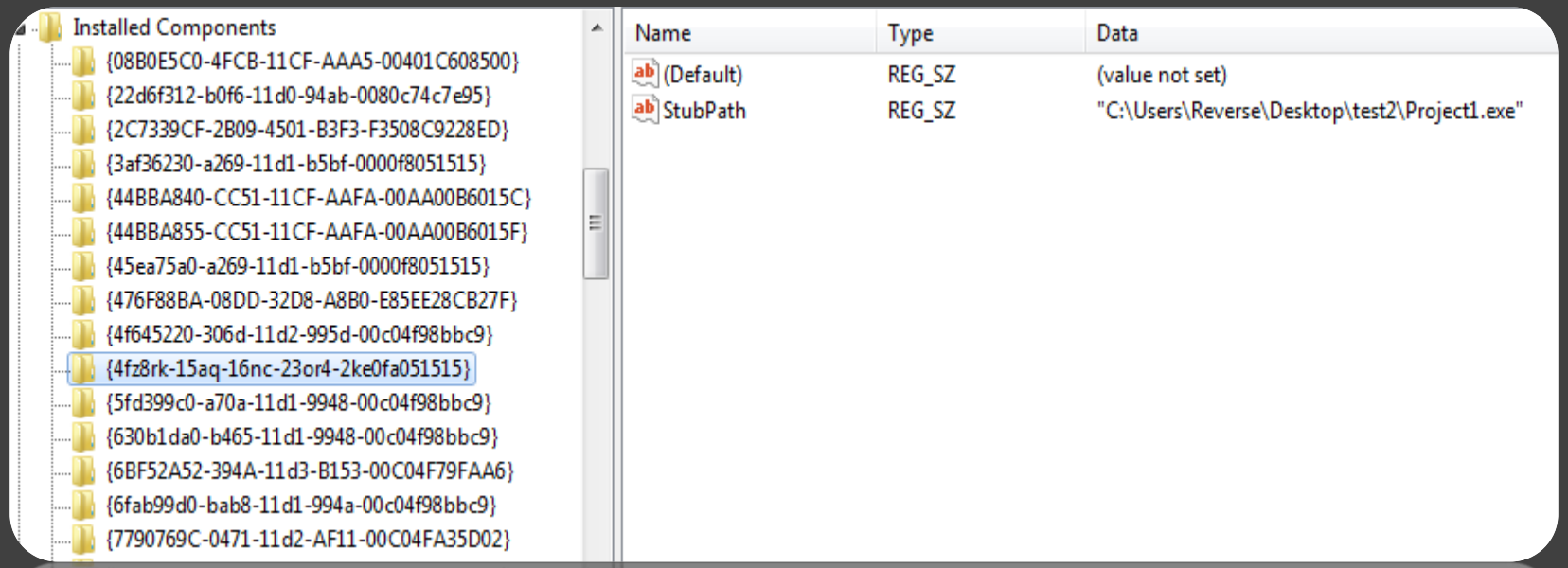
Применение настроек различных программных продуктов (Microsoft Office, Internet Explorer и тд) при первом пользовательском входе в систему



Настройки **Active Setup**

Настройки Active Setup находятся в реестре, в разделе
HKLM\Software\Microsoft\Active Setup\Installed Components

Для каждого компонента есть отдельный раздел с именем, состоящим из уникального идентификационного номера (GUID)



StubPath — команда, которая должна быть выполнена
Version — версия компонента в текстовом формате, элементы

При входе пользователя система сравнивает содержимое разделов

HKCU\Software\Microsoft\Active Setup\Installed Components

HKLM\Software\Microsoft\Active Setup\Installed Components

Если есть различия, то происходит вызов программы в **StubPath** и добавления в первую ветку

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!