METHODS AND PROBLEMS OF UPDATING THE MICROSOFT WINDOWS 7 OPERATING SYSTEM TO MICROSOFT WINDOWS 10 IN THE ENERGY ENTERPRISE

Zhidkov D.A., Kuligina N.O., Pavlycheva T.N.

Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Dzerzhinsk,
e-mail: deniska1792@bk.ru

This article addresses the issue of updating Microsoft Windows 7 operating systems to Microsoft Windows 10 at an energy enterprise. The authors propose 6 different methods and analyze each according to different criteria to find the most rational method. The authors considered such possible upgrade methods as PC replacement and standard installation of updates using Acronis software products or Microsoft software products such as System Center Configuration Manager, Microsoft Deployment Toolkit and Windows Server Update Service. The possibility of both updating the operating system locally and using the domain infrastructure of the enterprise using the software products described above is considered. Based on the results obtained, the average update time per user workstation was established, and the percentage of successful updates by each method was revealed. The main aspects of this article are illustrated by graphs and charts. The authors also compiled a table with the results of each method, which is presented. As a result, the most rational method for updating the operating system of user workstations at the energy company was chosen. The main aspects of this article are illustrated by graphs, drawings and diagrams.

Keywords: operating system, Microsoft Windows, update, methods of installation, Acronis, SCCM, MDT, WSUS, software

The problems of current software in the modern industry are very acute. This issue hasn't been ignored by the power industry. Not updating software products and operating systems on a time basis leads to incorrect operation of IT-Infrastructure services of the enterprise, the lack of new software features, outdated data processed by the services, and creates a threat to the information security of the enterprise.

An example of such problem is the installed Microsoft Windows 7 SP1 OS on users' automated workstations. On January 14, 2020, the Microsoft officially stopped supporting and updating Microsoft Windows 7 OS [1].

The management of the company and IT service immediately made the decision to transfer the users on automated workstations to a more current OS. Three possible OS options were discussed in details – OS based on the Linux kernel, OS Microsoft Windows 8.1 and OS Microsoft Windows 10. The advantages of Linux OS are its free ware distribution(there isn' necessity to purchase a license) and low system requirements. The disadvantages –incompatibility with IT services of the enterprise infrastructure. The OS Microsoft Windows 8.1 was rejected due to complicated user's interface and numerous problems with hardware and software compatibility. Microsoft Windows 10 is the most relevant OS from Microsoft; it has better compatibility with the enterprise IT-infrastructure, habitual user's interface and constant OS updates, expanding its functionality and increasing its security. The disadvantages of Microsoft Windows 10 – high system requirements and lack of certificates of compliance from the FSTEC and FSB.

A comparative analysis of operating systems has shown that the most rational option is to transfer users on automated workstations to Microsoft Windows 10. The appropriate licenses for using this software product were bought by the enterprise, so the issue of licensing won't be considered any further in this article.

This article discusses updating the OS with an **MBR** condition (master boot record, MBR). All x86-based and x64-based computers running Windows can use the partition style known as master boot record (MBR). The MBR partition style contains a partition table that describes where the partitions are located on the disk [2]. The MBR also contains executable code to function as a loader for the installed operating system – usually by passing control over to the loader's second stage or in conjunction with each partition's volume boot record (VBR). This MBR code is usually referred to as a boot loader.

Before updating the OS, the computer inventory was updated by 97.6%. All updated PCs have similar characteristics – Intel Corei3-6100 (4 MB cache, 3.80 GHz clock speed); RAM 4 GB, hard disk 500 GB. All PC data devices are absolutely identical.

Purpose of the study

The purpose of this study is to update the operating system of all personal computers of the enterprise using various methods and perform a comparative analysis of the methods to choose the most rational.

Material and research methods

The company's computer inventory consists of 410 users on automated workplace. The time limit for performing OS updates is

60 days. The network and domain infrastructure are developed on the enterprise. The company's IT-service has approved the following methods for updating users on automated workplace to Windows 10:

– Replacing the users' workstations with a more modern one with pre-installed Windows 10 with an OEM license (from the hardware manufacturer;

– Standard installation of Windows 10 OS from an external storage device;

– Creating and deploying an OS image using Acronis software products;

– Deploying an OS image using System Center Configuration Manager 2012 over a network infrastructure;

– Deploying an OS image using the Microsoft Deployment Toolkit via PXE network boot;

– Updating Windows 7 to Windows 10 via the update server Windows Server 3.0 update service.

After analyzing the technical characteristics of the fleet of computers and OS update methods, a diagram of the distribution of users on automated workstations, depending on the update methods, was compiled. Depending on the technical characteristics of the PC and their physical distance, the most rational methods of updating were chosen. A detailed diagram is shown on the Fig. 1.

It is necessary to consider each method separately to justify the rationality of the distribution of methods.

Replacing a PC is the simplest method of implementation from a technical point of view. As a result of the analysis, it was revealed that there were 10 automated workplace systems not supporting Windows 10, so it was decided to perform a complete replacement for more modern and productive PCs. The company purchased new PCs with pre-installed Windows 10 OS with a license from the manufacturer. The PCs were placed on the workstations of the specified users, connected to the LAN of the enterprise, and entered into the domain infrastructure. The disadvantages of this method are its cost and time spent on removing additional software products from the hardware supplier and installing enterprise software. The average update time for this method was 30 minutes.

Standard installation of Microsoft Windows 10 on the user's computer is the most trivial method of updating the OS. The factory image of the OS integrates the drivers of automated workplace devices that will be installed on Windows 10. A standard tool from Microsoft – DISM – is used for driver integration. **Deployment Image Service and Management Tool (DISM)** – is a command-line tool that is used to mount and service Windows images before deployment. You can use DISM image management commands to mount and get information about Windows image (.wim) files or virtual hard disks (VHD) [3]. Its features include mounting and unmounting images, querying installed device drivers in an offline image, and adding a device driver to an offline image. The time spent on driver integration is 60 minutes. Then the image is written to an external USB drive. This drive is physically connected to the local PC to download the OS installer. Windows 10 is being installed on the user's automated workstation. The automated workstation is entered in the domain. A standard package of enterprise software products is installed. The disadvantages of this method are the mandatory physical presence of an IT employee, manual configuration of the workstation, and configuration of the OS. The average OS update time is 77 minutes (including driver integration and OS configuration).

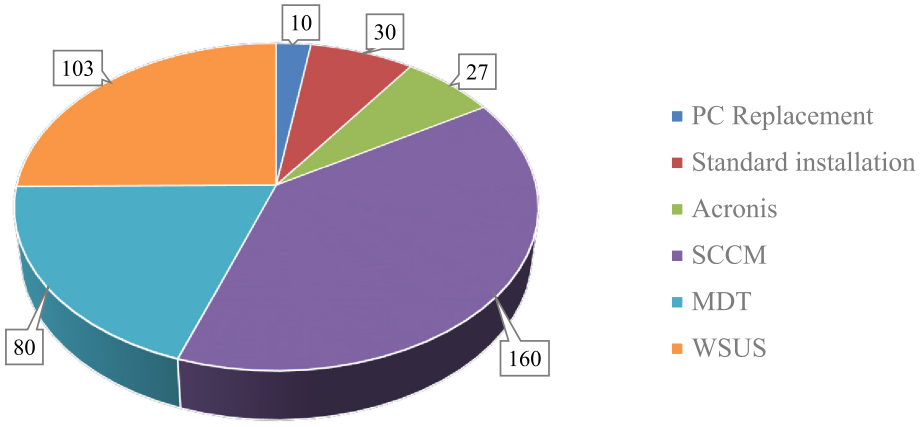

Fig. 1. Distribution of the number of automated workspace depending on the update method

Acronis True Image is a software product produced by Acronis that provides data protection for personal users including backup, archive, access, and recovery for Windows, macOS, iOS, and Android operating systems. As disk imaging software, True Image can restore the previously captured image to another disk, replicating the structure and contents to the new disk while allowing disk cloning and partition resizing, even if the new disk is of a different capacity [4]. This software is a commercial product and requires the purchase of a license to use it. The principle of its operation is based on copying the image of the reference OS with already installed drivers and software products, and further restoring from this image to the user's automated workstation. In the future, this image . can be used to restore the OS in the shortest possible time. Creating a reference image similar to the standard installation of Windows 10 (77 minutes), the time spent on creating the archive .tib – 16 minutes(without using sector-by-sector mode). The disadvantages of this method are the use of additional memory on an external storage device, the mandatory physical presence of an IT-employee, and resetting various service IDs for Windows 10 to work correctly in the enterprise domain infrastructure. The average time to deploy the image to the user's workstation was 24 minutes(including the creation of the reference image and the creation of the .tib archive).

Microsoft Endpoint Configuration Manager (Configuration Manager, also known as ConfigMgr or SCCM), formerly System Center Configuration Manager and Systems Management Server (SMS) is a member of the Microsoft System Center suite of management solutions, System Center 2012 Configuration Manager increases IT productivity and efficiency by reducing manual tasks and letting you focus on high-value projects, maximize hardware and software investments, and empower end-user productivity by providing the right software at the right time. Configuration Manager helps you deliver more effective IT services by enabling secure and scalable software deployment, compliance settings management, and comprehensive asset management of servers, desktops, laptops, and mobile devices [5]. Updating the OS with this method is the most automated and perfect for updating on remote user workstations. A System Center Configuration Manager specialist creates an image of an OS update in the server part of this product, as well as installs drivers and enterprise software using process automation scripts. Windows updates are performed directly using the enterprise network architecture. After the update manual entry of the workstation into the domain infrastructure of the enterprise is not required. The disadvantages of this method are the purchase of licenses to use this product, the requirements of special knowledge on working with this product, and a large number of unsuccessful updates on the users' automated workstations. The average update time, including pre-preparation, takes about 140 minutes.

The update method via Microsoft Deployment Toolkit (MDT) is similar to the update method via System Center Configuration Manager. **MDT** is a unified collection of tools, processes, and guidance for automating desktop and server deployment. You can use it to create reference images or as a complete deployment solution. MDT is one of the most important tools available to IT professionals today [6]. The principle of operation of this method is based on installing MDT on one of the free enterprise servers, configuring the server and configuring network equipment, creating a reference OS image with installed enterprise software products and drivers. This image is also installed over the network infrastructure using PXE technology. **Preboot Xecution Environment (PXE, most often pronounced as "pixie")** specification describes a standardized client-server environment that boots a software assembly, retrieved from a network, on PXE-enabled clients. On the client side it requires only a PXE-capable network interface controller (NIC), and uses a small set of industry-standard network protocols such as DHCP and TFTP. [7]. The advantages of this method are remote update of Windows OS, free license of MDT software product, high level of successful update among users on automated workspaces. The disadvantages of this method are high requirements for the enterprise's IT-infrastructure, the availability of special knowledge to implement this method, and the partial physical presence of an employee of the enterprise's IT-service to configure the network load and then enter the domain on the automated workstation. The average OS update time using this method was 160 minutes (taking into account the preparation of the enterprise's IT-infrastructure, server configuration, image creation, and configuration on automated workstations).

The last method of updating OS Microsoft Windows 7 to Microsoft Windows 10 is Windows Server Update Services (WSUS) 3.0. **WSUS** is a Windows Server role available in the Windows Server operating systems. It provides a single hub for Windows updates within an organization. WSUS allows companies not

only to defer updates but also to selectively approve them, choose when they're delivered, and determine which individual devices or groups of devices receive them. WSUS provides additional control over Windows Update for Business but does not provide all the scheduling options and deployment flexibility that Microsoft Endpoint Configuration Manager provides [8]. The advantages of this method are a completely remote automated OS update process, the ability to automatically roll back updates in the event of a failed installation of Windows 10, the existing infrastructure to ensure the operation of WSUS in the enterprise, the continued use of WSUS as an OS update server, and free use of this service. The principle of operation of this method is approving the necessary updates to transfer the user's on automated workspaces from Windows 7 to Windows 10 in the management console for this role, download updates from Microsoft servers, distribute and install the specified update on the user's automated workstation in real time or on a schedule. The enterprise has already deployed WSUS 3.0 with an external database running Microsoft SQL Server 2014. In order for the OS update to work correctly, you also need to make changes to the role of the Internet Information Services (IIS) web server that provides WSUS3.0. You must add permission to the IIS MIME-type parameters .esd (archive for installing Windows 10). Permission to update the OS version is automatically configured in the Windows 7 registry using group policies (GPO) and automation scripts. You must have a server running Microsoft Windows Server 2012 R2 or later OS versions. In previous versions of server OS, it isn't technically possible to upgrade Windows 7 to Windows 10. In the future, you can use this service to install cumulative update packages for Windows 10 and upgrade the build version of Windows 10. The disadvantages of this method are the need for a separate update of the enterprise software package, and low compatibility of device drivers. The average update time for this method was 120 minutes (including downloading the necessary updates and updating the enterprise software package).

Research results and discussion

Given the average OS update time of a single user's workstation, you can create a diagram to determine the fastest update method. The fastest way is a complete replacement of the user's automated workstation (30 minutes). The results are shown on the Fig. 2.

Also, in almost every case, there was an incorrect Windows update process. The failure of the update process was caused by various technical reasons-from a malfunction of the automated workstation to incorrect shutdown of the PC by the user. Updating a problematic automated workstation was solved by PC diagnostics and the method of standard installation of Windows 10.

In particular, we considered how successfully each of the following methods executed – replacing a PC, standard installation of OS, restoring from a backup using Acronis, SCCM, MDT, and WSUS .Knowing the total number of automated workstations planned for updating by a particular method, and the number of problematic PCs, you can deduce the percentage of success of updates by each method. This ratio is shown in detail on the Fig. 3.

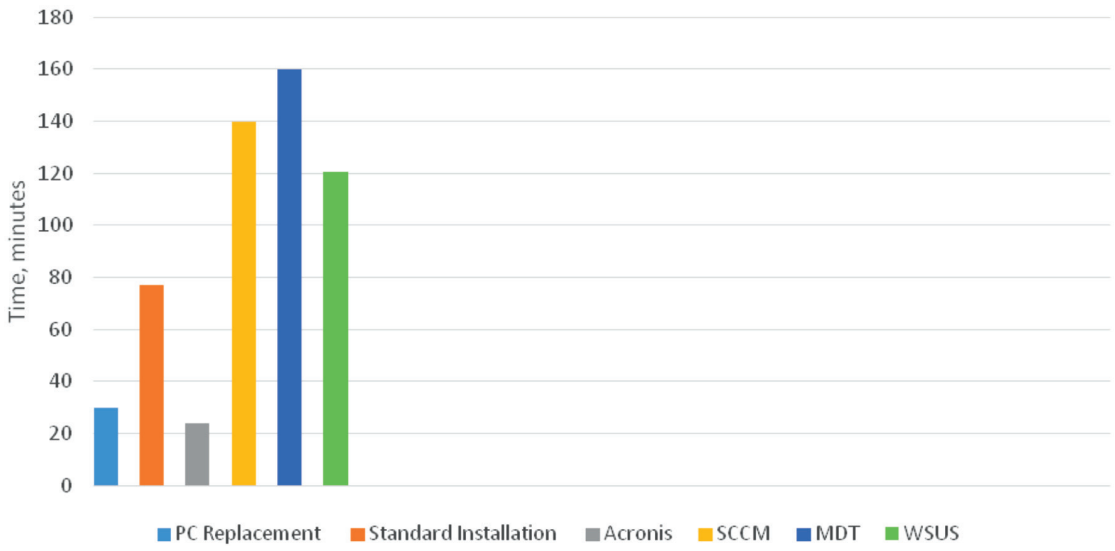

Fig. 2. The average installation time of updates

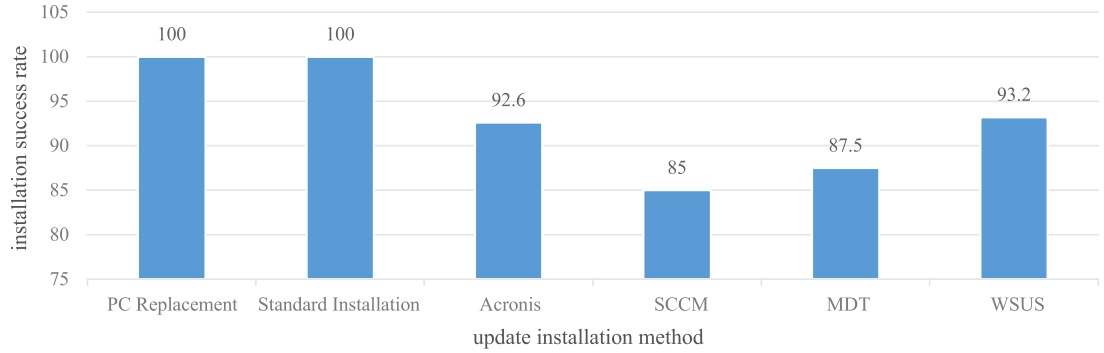

Fig. 3. Percentage of correct installation of updates on the automated workspaces by diferent methods

Criteria of methods for upgrading Microsoft Windows 7 to Windows 10

Method	Success rate, %	Time, min	Installation-complexity	License	Remotein-stallation	Hightechnical-requirements
PC Replacement	100	30	low	no	no	no
Standard Installation	100	77	low	no	no	no
Acronis	92,6	24	low	yes	no	no
SCCM	85	140	high	yes	yes	yes
MDT	87,5	160	high	no	partially	yes
WSUS	93,2	120	medium	no	yes	yes

By analyzing the data obtained, you can create a table of criteria for methods to select the most optimal method for updating the OS. The data is presented in the table.

Conclusion

So many power plant facilities are located remotely that the most rational method is to update them via WSUS 3.0.

As a result of the project to upgrade Microsoft Windows 7 to Microsoft Windows 10, 6 methods were used at the power plant. In the course of using the methods, the advantages and disadvantages of each method were identified, the most optimal and reliable method was the implementation of OS updates via WSUS 3.0. The project was implemented within 60 days in accord with the technical task order. At the moment, all users on automated workstations are running the most up-to-date Windows 10 operating system from Microsoft.

References

1. Data from the official website of Microsoft [Digital resource].: access mode: URL: https://www.microsoft.com/en-gb/windows/windows-7-end-of-life-support-information (date of the application: 26.10.2020).

2. Master Boot Record [Digital Resource].: Microsoft Docs. – access mode: URL: https://docs.microsoft.com/en-us/windows/win32/fileio/basic-and-dynamic-disks#master-boot-record (date of the application: 26.10.2020).

3. Deployment Image Servicing and Management [Digital Resource].: Microsoft Docs. – access mode: URL: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/dism---deployment-image-servicing-and-management-technical-reference-for-windows (date of the application: 26.10.2020).

4. Acronis True Image [Digital Resource].: Wikipedia. The free encyclopedia. – access mode: URL: https://en.wikipedia.org/wiki/Acronis_True_Image (date of the application: 26.10.2020).

5. System_Center_Configuration_Manager [Digital Resource].: Microsoft Docs. – access mode: URL: https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg682140(v=technet.10) (date of the application: 26.10.2020).

6. Microsoft Deployment Toolkit [Digital Resource].: Microsoft Docs. – access mode: URL: https://docs.microsoft.com/en-gb/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit (date of the application: 26.10.2020).

7. Preboot_Execution_Environment [Digital Resource].: Wikipedia. The free encyclopedia access mode: URL: https://en.wikipedia.org/wiki/Preboot_Execution_Environment (date of the application: 26.10.2020).

8. Windows Server Update Service [Digital Resource].: Microsoft Docs. – access mode: URL:https://docs.microsoft.com/en-gb/windows/deployment/update/waas-manage-updates-wsus (date of the application: 26.10.2020).