**SAFETY MANAGEMENT SYSTEMS**

Content:

[Explanatory note 4](#_Toc479693245)

 [Practical work SRSP-1 Study of Security Policy in Windows 7 6](#_Toc479693246)

 [Practical work SRSP- 2 Security Template Management in Windows 7 12](#_Toc479693247)

 [Practical work SRSP- 3 Separation of powers and access to the Unix operating system objects 16](#_Toc479693248)

[Practical work work SRSP-4 Configuring Windows 7 authentication parameters eighteen](#_Toc479693249)

 [Practical work work SRSP -5 User Rights Assignment with random access control in Windows 7 23](#_Toc479693250)

 [Windows 7 Practical work work SRSP- 6 Setting parameters and registration audit 29](#_Toc479693251)

 [Practical work SRSP- 7 Methods of cryptographic data conversion 36](#_Toc479693252)

 [Practical work work SRSP-8 Using the functions of the cryptographic interface (CryptoAPI) Windows operating system for information security. 40](#_Toc479693253)

 [Practical work SRSP- 9 Antivirus Software Packages 64](#_Toc479693254)

[Practical work SRSP-10 recovery of infected files. Prevention of penetration of "Trojans" 84](#_Toc479693255)

[List of recommended literature 89](#_Toc479693256)

 **SRSP**

# explanatory note

This paper provides guidance for practical work on discipline "Safety Management Systems"

The purpose of development: the direction and assistance to students in performing SRSP practical work on the subject "Safety Management Systems"To prepare students to conduct workshops on given topics (Practical work №2 and №9 take the form of discussions and summarize the material collected by students).

Practical work is done by students themselves during the learning process, according to calendar-thematic plan on the basis of regulations, guidelines, theoretical knowledge and experience.

Lessons - seminars allow students to independently engage in extracurricular work in preparation for the workshop, and increase the level of student activity. Seminars require students to serious independent work with additional materials: a new source of reading, comparison of materials, independent work with certain software packages, a selection of interesting facts. At the seminars is expected a higher degree of specialization of the educational material than is the case at the lecture.

Other practical work carried out in the computer lab and require specific training in the field of programming.

All practical work begins with the study of theoretical material and terminate registration of the report.

#

# SRSP practical work -1

# Security Policy Study of the Windows 7 operating system

**The purpose of lessons**: Examine the Windows 7 operating system security policy

**Methodical maintenance:** guidance for practical work

**theoretical information**

Windows 7 is based on Windows Vista security principles, meets the wishes of users to establish a more comfortable and controlled system and contains security enhancements required for data protection in a rapidly changing threat patterns. The most significant security improvements in Windows 7 are considered in four sections.

1. Secure platform. At the core of Windows 7 security enhancements are introduced with Windows Vista. In addition, it meets the needs of customers to establish a more convenient and manageable system.

2. Achieve universal access security. Windows 7 provides the appropriate security controls so that users at any time, from any location can access the data they need for the job.

3. Protecting Users and Infrastructure. Windows 7 provides flexible protection against malware and intrusions so that users get the right combination of security, control and efficiency.

4. Data protection from unauthorized viewing. Windows 7 extends BitLocker ™ Drive Encryption technology to protect data stored on portable media (eg, USB-devices, flash memory, USB hard drives), so only authorized users can read the data, even if the vehicle has been stolen, lost or used incorrectly.

Secure platform.

Fundamental security features:

 Kernel patch protection;

 limited service mode of operation;

 DEP;

 the random distribution of the address space;

 Integrity Levels continue to provide enhanced protection against malware and attacks.

This operating system meets the Common Criteria requirements for certification Evaluation Assurance Level 4 and Compliance FIPS 140-2. Based on the reliable Windows Vista security platform, Windows 7 makes significant improvements in the main event auditing security technologies and management of user accounts.

**Improved auditing.**

Windows 7 provides enhanced audit capabilities that simplify compliance with regulatory and operational requirements: Including realized a simplified approach to the audit configuration management, and carried out in the organization of tasks are described with greater clarity. For example, Windows 7 helps to get a clear idea of ​​who can access specific information, why a user was denied access to certain data, as well as find out about all the changes made by the user or group.

Support for security devices.

Windows 7 simplifies the process of connecting security devices to your PC and manage, and provides easy access to common tasks related to the use of devices. Never before has the use of safety devices was not so simple: during the initial installation and daily operation.

Storage device with enhanced security.

Extensive use of the flash USB-memory devices, and other personal storage devices leads to doubt the security of data on these devices. However, some users do not require the full capabilities of encryption BitLocker To Go ™ data. Windows 7 supports password protection and certificate-based authentication for the USB-storage devices that conform to the IEEE 1667. To preserve the confidentiality of data, you can use the ability to protect passwords, implemented in protection devices that support IEEE 1667 standard.

Storage device with enhanced security.

Extensive use of the flash USB-memory devices, and other personal storage devices leads to doubt the security of data on these devices. However, some users do not require the full capabilities of encryption BitLocker To Go ™ data. Windows 7 supports password protection and certificate-based authentication for the USB-storage devices that conform to the IEEE 1667. To preserve the confidentiality of data, you can use the ability to protect passwords, implemented in protection devices that support IEEE 1667 standard.

Ensuring universal access security.

Windows 7 provides the appropriate security controls so that users at any time, from any location can access the data they need for the job. Along with full support for existing technologies (such as Network Access Protection) Windows 7 provides a more flexible firewall, DNS Security support, and an entirely new concept of remote access.

Support DNSSec.

DNS - this is the main protocol that supports most daily tasks performed on the Internet, including e-mail delivery, Web browsing, and messaging. However, it should be noted that the DNS system was designed more than three decades ago, without taking into account today's security threats. DNS Security Extensions (DNSSEC) - a set of extensions to DNS that provide the security services required to operate on the Internet. In accordance with the requirements of RFC 4033, 4034 and 4035, Windows 7 support of DNSSEC documents, providing confidence in the authenticity of the organization domain name records and providing protection against malicious manipulation.

**The presence of multiple active firewall policies.**

Firewall Policy in Windows Vista is based on the type of network connection established: home, work, or general domain (this type is hidden). However, if the user is connected to the Internet through a "home" network that uses a VPN to access the corporate, it could create serious security problems. In such a case, the corresponding firewall settings to access the corporate network can not be applied as network type (and hence the firewall settings) has been set based on the first network to which the user is connected.

Windows 7 eliminates this problem by supporting multiple active firewall policies that allow computer users to obtain and use information about the domain firewall profile, regardless of other networks that can be connected to a PC. With these capabilities, which are among the main features requested by enterprise customers, IT professionals can simplify connectivity and security policies by maintaining a single set of rules for remote clients and clients that are physically connected to the corporate network.

**DirectAccess.**

With Windows 7, working outside the office becomes simpler. With DirectAccess, remote users can access the corporate network at any time if there is an Internet connection, without the need for additional action to install the VPN-connection. This increases employee productivity. DirectAccess provides IT professionals a more secure and flexible corporate network infrastructure to remotely update the users' PC and manage them. DirectAccess simplifies IT management by introducing constantly managed infrastructure, in which computers in the network and beyond, supported by an efficient and updated.

With DirectAccess, IT professionals can more precisely control the network resources that are accessed by users. For example, to control remote user access to enterprise applications, you can use Group Policy settings. DirectAccess separates Internet traffic from access to internal network resources, so that users can access on the public Web sites without generating additional traffic in the enterprise network. Furthermore, DirectAccess component supports industry standards (e.g., IPv6 protocols and IPsec), ensuring the protection and security of corporate data exchange.

**Protect users and infrastructure.**

Windows 7 provides flexible protection against malware and intrusions so that users can get the right value for the security, control and efficiency. The main improvements are the security component AppLocker ™ and Internet Explorer® 8 browser, which provide a new standard operating system security from invasion of malicious programs in Windows 7.

AppLocker.

Application Control Policies in Windows 7 are used in conjunction with the AppLocker tool - a flexible and easy to manage mechanism that allows IT professionals to specify the programs and components that can be run on the desktop. In addition, users can use applications, installation programs, and scripts that enhance their productivity. As a result, IT staff can carry out in the organization of standardization application that provides security and compliance, and improves productivity.

AppLocker provides a simple and effective rules of the structure and introduces publisher rules: rules based upon application digital signatures. Publisher rules make it possible to build rules that survive application updates through the ability to specify the application version as an attribute. For example, an organization can create a rule that allows the program Acrobat Reader all versions greater than 9.0 if they are signed by the software publisher Adobe. Now when Adobe updates Acrobat, it can be safely deployed without creating another rule for the new version of the application.

Internet Explorer 11.

Internet Explorer 11 provides improved protection against security and privacy threats, including the ability to determine the unreliable websites and blocking the download of malicious software. Protection is strengthened by the possibility to browse the web without saving the data on a public computer, as well as through advanced configuration parameters and controls how the Web sites can track user actions. In Internet Explorer 11 improved system of restrictions for ActiveX ® controls and improved management of add-ons. The web browser has a high reliability, which is provided by the function of automated failover and recovery tab, as well as enhanced support for accessibility.

Protecting data from unauthorized viewing.

Windows 7 includes data protection technologies available in Windows Vista: system supports the Encrypting File System (EFS), built-in technology Active Directory® Rights Management Services components and accurate control of USB-ports. Along with the updated versions of these technologies in Windows 7 provides several significant improvements to the popular BitLocker Drive Encryption technology.

BitLocker and BitLocker To Go.

Windows 7 solves all the more relevant data leakage with manageability and deployment updates to BitLocker Drive Encryption and BitLocker commissioning new facilities To Go, which provides enhanced protection against data theft and exposure by expanding BitLocker support to removable storage devices. Extended BitLocker support for FAT data volumes, a broader devices and range of disk formats including flash USB-memory devices, and removable drives. This allows users to deploy BitLocker with the need to ensure data protection.

When traveling with your laptop, sharing large files with a trusted partner, or work at home protection devices with BitLocker ensures that data can be read only by authorized users, even if the media is lost, stolen, or misused. BitLocker protection is easy to deploy and intuitive for the end user meets regulatory requirements and provides proper data security.

With BitLocker To Go, administrators can control the use of removable storage devices, and to establish the necessary level of protection. Administrators make a mandatory defense on any removable storage device, the data that users want to write data, allowing the use of unprotected devices to access read-only mode. In addition, there are special policies that require appropriate passwords, smart card, or domain user credentials to utilize a protected removable storage device. In addition, BitLocker To Go provides configurable support for removable devices with the ability to read older versions of Windows, enabling more securely share files with users who are still running Windows Vista and Windows XP.

Built on the Windows Vista® security principles, Windows 7 includes improved security features, giving users confidence in the reliable protection. Enterprises can take advantage of improvements designed for the safety of confidential data, for effective protection against malware and security of universal access to corporate resources and data. Consumers can enjoy the benefits of computers and the Internet knowing that thanks to embedded Windows 7 advanced security technology confidentiality of their personal data is protected. In addition, all users will appreciate the flexible and affordable options of Windows 7 security configurations that can be used to achieve a balance between security and usability.

**Exercise 1**

In Windows 7, set up account policy by setting the following parameters:

* maximum password age of 45 days;
* minimum password length of 8 characters;
* minimum password age of 5 days;
* Password must meet complexity requirements;
* Passwords should not be repeated;
* Passwords should be stored encrypted.

**task 2**

In Windows 7 operating system to configure account lockout policy setting the following parameters:

* lock the account for 60 minutes after 5 attempts to enter an incorrect password.
* charge counter attempts after 30 minutes.

#  practical work SRSP- 2

# Security Template Management in Windows 7

**The purpose of lessons**: See the possibilities of Windows 7 to manage security templates. The sequence of operations for operating system Windows 7. manage security templates to get practical skills to protect your computer is running Windows 7 operating system.

**Methodical maintenance:** guidance for practical work

**theoretical information**

Security Template Management in Windows 7 by using Security Templates Editor, implemented as MMC snap-in.

It is designed for creating and editing text of the Windows operating system security configuration files 7. These files are more easily transferred from one system to another than the corresponding safety data base.

By using the Security Templates snap-in text files stored on the hard disk and, if necessary, can be imported to the security database. In this case, all the stored security settings take effect.

The values ​​of safety parameters recorded in text files with the extension inf, called a security template.

*Note. New security templates do not change all the old security configuration parameters of the system, they only supplement them by increasing (incrementing) the degree of computer protection.*

**The task:**

Download editor security templates, edit the security template and save it with a new name.

**The algorithm performance.**

BUT). Download Security Templates snap-in.

Select the Start button on the taskbar.

Scroll to Run.

In the window that opens into the input box, type mmc.

This will open the mmc console.

On the Console menu, click Add or Remove Snap-in (Figure 1) and click the Add button.



Picture 1

In the snap-in, double-click Security Templates.

Click the Close button.

The list of selected snap-ins for the new console will be an element of security templates.

If the console does not need to add other snap-ins, then click OK.

To save this console, on the Console menu, click Save and specify the name of the Security Templates snap-in.

Close the Console window and then click Start and then All Programs.

Find a point to Administrative Tools, and then click the Security Templates subparagraph (now with the Security Templates snap-in is available in the Start menu).

To view the available templates in the snap values ​​window open, for example, security templates node, click to select compatws security template (Figure 2) and view the folder Account Policies, Local Policy, and others.



Figure 2

In addition to the disclosed security template compatws.inf there are other standard templates that are configured to receive a variety of safety system reliability.

B). Editing and saving a security template.

 Click on one of the default security template (for example, compatws), which you see in the box, the Security Templates snap-in.

If you want to modify any security settings, double-click on it and edit the parameter values ​​(Figure 3).



Figure 3

To save the corrected standard security templates with a different name, follow these steps.

Enter the corrected standard template (for example, compatws), and click the right mouse button.

In the context menu, click Save As.

Type a new file name (for example, custom). Default security templates are located in the directory% SystemRoot% \ Secunfy \ Templates.

Custom template will be added to the pre-defined security configuration and saved under the name you entered.

After configuring the security template for a PC, you can transfer it to other PC your working group. Security templates are flexible and convenient tool for setting up the operating system's security system.

**Tasks for independent work**

Established on the basis of an existing security template a new template, and give it a name PZ-8. After that, fix the template list by copying the screen image to the clipboard to send it to the teacher as a record.

**Control questions**

1. Why use security templates?
2. At what point are stored on disk (default) security templates?
3. Which sections includes a standard security template?

#

#  practical work SRSP- 3

# Separation of powers and access to the Unix operating system objects

**The purpose of lessons**: Examine the Windows 7 operating system security policy

**Methodical maintenance:** guidance for practical work

**theoretical information**

Concurrent access to objects in the operating systems Unix family - files, directories, PR and special files (character or block devices IO and named pipes) - is carried out based on the stored index corresponding object information about the owner of the object (UID) and his group ( GID), and the vector to the object.

- File Index - its control unit, which is stored in the index, the department ?? ennoy from the field files.

directory structure

Directory - file consisting of records included in the respective catalog file. Each entry consists of an index number associated with the file, and the file name. Ability to create multiple files associated with the same index, ᴛ.ᴇ. with the same external memory region (by means of so-called reference).

access vector

Is a list of fixed access control (rather than arbitrary, like Windows) to length. The first item in the list determines the access rights to the object of its owner, the second - the members of his primary group, and the third - Sun ?? ex ?? s other users of the system. Root user has full access to Sun ?? eat objects in the system. Each access unit vector has a length of 3 or 4 bits.

Types of access to the object

- There are three types of access to the object: reading (r), recording (w) and execute (x). For directory entry defines create, rename and (or) removal of the files, and execution - search for files in the given directory name.

- EXAMPLE vector file access:

rwxr-xr - (or 0754 in octal)

(Owned ?? ec file has the right to have full access to it, the owner of the group members - to read and execute the file, and the Sun ?? e other users - only to read the file).

*The reliability of access control to objects in Unix*

In order to use the system without a command to change the access rights to the object for a particular user, it is essential to have access to the area of ​​the file system indices that determine ?? enes in a special file (for example, / dev / root). But the index of this file is also stored in the index. For this reason, if not change the access rights to the Sun it ?? system objects that are set by default when you install the operating system (which can be done only by the superuser), then we can guarantee the safety of the access control subsystem.

*The extra bits in the access controls*

*If*the fourth bit is set in the vector element for the owner of the file (SUID), the program file to be executed in a session with any user rights of the owner of this file. This is extremely important, for example, when you call the command passwd user ?? eat to change your password. A normal user may have the right to change his password, but can not have write access to the password file.

*If*the fourth bit is set in the access for the vector element holder member group (SGID), then the program file to be executed in a session with the rights of any user group members of the owner of the file. If SGID is set in a vector of access to the directory, the Sun ?? e ?? it was built by users files in this directory will have the same identifier of the owner of the group, as well as a directory.

*If*the fourth bit is set in the element of the vector access to Sun ?? ex ?? s other users (Sticky), the operating system creates a special text software image file. Most often this bit is used for catalogs and determines the prohibition on deleting or renaming files to other users ?? s in this directory. This is particularly important for the / tmp and / usr / tmp, so that some users can not damage the work of others. Sticky bit for directories should only be installed by an administrator.

# Practical work work 4Configuring Windows 7 authentication parameters

**The purpose of lessons**: Learn some basic settings of the Windows operating system authentication mechanism 7. Examine the sequence of setting up user authentication options transactions at the entrance to the operating system. Acquire practical skills to protect your computer against accidental or intentional acts.

**Methodical maintenance:** guidance for practical work

**theoretical information**

In accordance with the certification requirements for the security systems of operating systems when connecting users must implement an authentication mechanism and \ or identification.

Identification and authentication are used to restrict access random and illegal subjects (users, processes) information systems to its objects (hardware, software, and information resources).

Identification - assigning subjects and objects of personal identifier to access and compare it with the set.

Authentication (authentication) - ownership of access to the subject against them ID and proof of its authenticity. In other words, authentication is to verify: whether the entity connects those for whom he claims to be.

Configuring authentication parameters considered operating system runs within the local security policy.

Attachments "Local Security Policy" is used to change the account policies and local policies on local computer.

With the help of snap "Local Security Policy" can be defined:

who has access to your computer;

what resources users can use on your computer;

Enable or disable recording of user actions or a group in the event log.

**The task:**

Configure the Local Security Policy of Windows 7 operating system.

**Algorithm performance**

To view or edit user authentication settings, follow these steps:

Select the Start button, taskbar.

Select Control Panel, Customize.

In the window that opens, select the shortcut Administration, Local Security Policy.



Figure 4

Select Account Policies (This item includes two sub-items: password policy and account lockout policy).

Open the sub-password policy. In the right pane displays a list of configurable parameters (Figure 5).



Figure 5

In the example shown, the password policy corresponds to the initial state of the security system after installing the operating system, in this case, none of the parameters are not set. The parameter values ​​given in Table 1.

Table 1

|  |  |
| --- | --- |
| Parameter | Value |
| 1 | 2 |
| Enforce password history. | Specifies the number of new passwords that must be associated with a user account before you can reuse an old password. This value must belong to a range of 0 to 24. |
| Maximum password age. | It specifies the amount of time (in days) during which the password can be used before the system requires the user to replace it. It can be set in the range from 1 to 999 days or take any limitation of validity, setting the number of days to 0. |
| Minimum password | It specifies the amount of time (in days) during which you must use a password before the user can replace it. You can specify a value from 1 to 999 days, or to allow an immediate change by setting the number of days to 0. |
| Minimum password length. | It specifies the minimum number of characters that may contain user account password. It can be set in the range of 1 to 14 characters or cancel use of the password by setting the number of characters to 0. |
| Password must meet complexity requirements. | Determines whether passwords must meet complexity requirements.If this policy is enabled, passwords must meet the following minimum requirements.Password can not contain the user's account name or any part of it. The password must contain at least six characters. The password must be present symbols of the three categories of the following four: capital letters of the English alphabet from A to Z; lowercase letters from a to z; decimal digits (0 to 9); characters do not belong to a set of alphanumeric (such as!, $, #,%).Verification of compliance with these requirements satisfied for changing or creating passwords. |
| Keep the passwords of all users in the domain using reversible encryption. | Determines whether Windows 2000 Server, Windows 2000, and Windows XP Professional store passwords using reversible encryption. This policy provides support for applications that use protocols that use authentication, you need to know the user's password. Store passwords, encrypted reversible methods - it's like to keep them in plain text. Therefore, this policy should be used only in exceptional cases, if an application needs are more important than password protection. |

Discover the properties of all the parameters.

Figure 3

To change the setting you want, select it and call its properties from the context menu when right-clicking (or double-click to change the parameters).

As a result of this action will be one of the windows shown in Figure 3.

Change the setting and click OK.

For example, (required to execute and save), select the Enforce password history and change its value to 1.

To configure the account lockout policies, select the sub-item and open it.

The values ​​of the parameters of this subparagraph Account Policies are summarized in Table 2.

table 2

|  |  |
| --- | --- |
| Parameter | Value |
| Lockout threshold | Defines the number of unsuccessful login attempts after which the user account is locked. Blocked account can not be used until then, until it is reset by an administrator or until the lockout interval has elapsed it. It can be set in the range from 1 to 999 or deny blocking this account, by setting the value 0. |
| Account ban | Specifies the number of minutes during which the account remains locked before it is automatically unlocked. This parameter can take values ​​from 1 to 99,999 minutes. If set to 0, the account will be blocked for the whole time until until an administrator unlocks it explicitly.If the lock threshold value is determined, the lock interval must be greater than or equal to the reset interval. |
| Reset lockout counter after | Specifies the number of minutes that must pass after a failed login attempts before the failed attempts counter is reset to 0. This parameter can take values ​​from 1 to 99,999 minutes.If the determined blocking threshold value, the reset interval should not be longer than the interval Account ban. |

Discover the properties of all the parameters.

To change the parameters, use the algorithm described in paragraphs 8-10.

**Tasks for independent work**

Change the "Password must meet complexity requirements" Password Policies to "Enabled" (Figure 3) and then try to change the password for your account. Secure all communication systems, analyze and enter a valid password. This password is the result of the execution of your job and should be sent to the teacher.

After successful completion of the first task, change the password for your account, as well as a new password, enter the old password. All messages secure, analyze and explain the behavior of the security system. The results of the analysis of present teacher.

Experiment with different parameters Account Policies.

**Control questions**

1. What is authentication and identification?
2. What are these mechanisms used?
3. That can be configured using the Local Security Policy snap-in.

**Description of the report form**

Performing quests for self-study and answers to test questions must be sent to check the teacher.

# Practical work work 5User Rights Assignment with random access control in Windows 7

**The purpose of lessons**: To view the features of Windows 7 operating system, security system intended user access rights. The sequence of operations to create new users and groups and assign them permissions. Acquire practical skills for managing access rights to the Windows 7 operating system.

**Methodical maintenance:** guidance for practical work

**theoretical information**

After performing identification and authentication security subsystem sets the permissions (set of rights) subject to follow-authorized use of objects of information systems.

Typically, the subject authority submitted a list of resources available to the user, and the rights of access to each resource in the list.

The delimitation of the access lists specified correspondence: each user - a list of resources and the rights of access to them, or every resource - the list of users and their access rights to the resource.

Lists let you set right up to the user. Lists are used in security subsystems operating systems and database management systems.

**The task:**

Create an account and a local group, change the user belongs to a local group and to block the user account.

**The algorithm performance.**

A) Create a new account.

Open the Computer Management under Administrative Tools Control Panel (Figure 1).



Picture 1

The snap-in Local Users and Groups, set the mouse pointer over the Users folder and right-click.

In the context menu, click New User (Figure 2). You will see a dialog box New user (Figure 3).



Figure 2

In the User field, enter the name of your new user, such as name.

Note. User name must be unique for the computer. It may contain up to 20 upper and lowercase characters. The following symbols, the use of which the user name is unacceptable: "/ \ [] :; =, + \* <>?

The user name can not consist entirely of dots and spaces.

In the Full Name field, type the full name of the user being created.



Figure 3

In the Description field, enter a description created by the user or his account, for example, "student ..........".

In the Password field, enter your user password and in Confirm, confirm that it is correct secondary input.

Note. Password length can not exceed 14 characters.

Check or uncheck the boxes:

* User must change password at next logon;
* User can not change password;
* password never expire;
* disable the account.

To create another user, click New and repeat steps 1 through 8. Click Start, and then click Close to complete the work.

B) Creating a local group.

In the snap-in Local Users and Groups, set the mouse pointer to the Groups folder and right-click.

In the shortcut menu, click New Group.

In the Group Name field (Figure 4), enter the new group name, for example, students.

Note. Name of the local group must be unique within the computer. It can contain up to 256 characters in upper and lower case.

In the Description field, enter a description of the new group.

In the group members can immediately add users and groups to be included in this group: it is necessary to press the Add button and select them in the list.



Figure 4

To complete, click Start, and then click Close.

To change the membership of the local group, follow these steps.

The snap-in Local Users and Groups, click the Groups folder.

In the right pane, set the mouse pointer to a modifiable group and click the right button.

 In the context menu select Add to group or properties.

To add new accounts to the group, click the Add button (Figure 5).



Figure 5

Follow the dialog box instructions Select Users or Groups.

In order to remove some of the group members in the group members (Figure 5) of the Properties window, select one or more accounts and click the Remove button.

Note: The local group can be added as a local user created on the computer, and users and global groups created in the domain to which the computer belongs or in trusted domains. Built-in groups can not be deleted. Deleted groups can not be restored. Deleting a group does not affect its constituent members.

B) Temporary account lockout.

Open Computer Management.

You can either select a desktop shortcut My Computer and click the right mouse button, and then click Manage context menu, or use the Administration section in the Control Panel.

In the opened snap-in, select Tools / Local Users and Groups (Figure 2).

Open the Users folder and select the Guest account.

Right-click and select Properties.

In the window that opens, uncheck the item Disable account (Figure 6).



Figure 6

Click OK, and then draw conclusions about the account status.

Follow step 5 and click the checkbox Account is disabled.

**Tasks for independent work**

Create an account PZ-7 by using the Print Screen keyboard, keep a copy of the screen with a list of your users on the computer (for this, after pressing the Print Screen paste the copied image into a new Word document, keys) for presentation as a teacher report.

Create a group of Information Security and, as in the first task, keep a window with a list of groups to represent your computer teacher.

Lock PZ-7, and then delete the account.

**Control questions**

1. What methods of access control do you know?
2. What is different mandatory access control by discrete?
3. whether the user name is valid PZ8 \ 44? Why?

# Practical work work 6Setting registration options and auditing in Windows 7

**The purpose of lessons**: See the possibilities of Windows 7 on the registration and audit security events. The sequence for setting up registration settings and security auditing operations. To acquire practical skills in the Windows 7 operating system analysis of security events.

**Methodical maintenance:** guidance for practical work

**theoretical information**

Registration is another mechanism for ensuring the security of information systems. This mechanism is based on the security systems of accountability, retaining all of the events related to security. The effectiveness of the security system is fundamentally improved in the case of registration mechanism supplements the audit mechanism. This allows you to quickly identify violations, identify weaknesses in the security system, analyze the system of laws, to evaluate the user experience, etc.

Audit - is the analysis of accumulated information held quickly, in real time or periodically (eg, once a day). Operational audit automatic response to the identified emergency situations is called active.

Practical means of registration and auditing are:

* various system utilities and applications;
* registration (or control system) magazine.

The first tool is usually in addition to monitoring carried out by the system administrator. An integrated approach to logging and audit provided using log.

Logbook - a chronologically ordered set of records system activities subjects results sufficient for recovery, viewing and analyzing the workflow surrounding or leading to the implementation of operations, procedures, or an event occurs, when the transaction for the purpose of control of the final result.

**The task:**

Activate mechanisms of the Windows 7 operating system logging and auditing and configure the folder view and file audit settings

**The algorithm performance.**

A) Activation mechanism of registration and auditing by using the Local Security Policy snap-in.

To enable auditing on a standalone computer, follow these steps.

1. Click the Start button, taskbar.

2. Open the menu Configure / Control Panel.

3. In the window that opens, select the shortcut Administration / Local Security Policy.

4 .Select click Audit Policy (Figure 1).



Picture 1

5. To enable or disable the audit settings, select the desired option and double-click the left mouse button.

6. For each option, you can specify whether to audit successes or failures, or not audit the event type (Figure 2).



Figure 2

7. Values ​​audit policy parameters are given in Table 1.

Table 1

|  |  |
| --- | --- |
| Parameter | Value |
| one | 2 |
| Audit logon events | It determines whether or not subject to audit each time a user attempts to log in or out of it on another computer, provided that the computer is being used to authenticate the account.If this policy setting is defined, you can specify whether to audit successes or failures, or not audit the event type. Success Audit generate an audit entry for each successful logon attempts. Failure Audit generate an audit entry for each unsuccessful logon attempts. |
| Audit account management | Determines whether the subject audit all events associated with the account management on a computer. Such events include the following events:creating, changing, or deleting a user or group account; renaming, disable or enable a user account; set or change the password.  |
| Audit directory service access | It determines whether to audit user access event is subject to an object in Active Directory, which is set to its own system access control list. |
| Audit logon events | It determines whether or not subject to audit each time a user attempts to log in or to leave it on the computer, or connect to it over the network. |
| Audit object access | It determines whether to audit user access event is subject to an object - such as a file, folder, registry key, printer, etc., - for which is given its own system access control list. |
| one | 2 |
| Audit policy change | It determines whether to audit each subject fact change user rights assignment policies, audit policies, or trust relationships policy. |
| Privilege Use Audit | It determines whether to audit user every attempt to be to take advantage of his entitlement. |
| Audit process tracking | It determines whether to audit events such subject as the activation of the program, completion of the process, the repetition of descriptors and indirect access to the object. |
| Audit system events | It determines whether to audit shall be restarting events or shutdown, as well as events that affect system security or the security log. |

By default, all audit policy settings are turned off.

Enable auditing for success and failure for all parameters.

To do this, point 5.

Click OK.

B) Set up and view the audit files and folders (available only on NTFS volumes).

To configure, view or modify audit settings files and folders, follow these steps.

Place the mouse pointer over the file or folder for which you want to audit, and then press the right button.

 In the shortcut menu, click Properties.

 In the properties file or folder, click the Security tab.

On the Security tab, click Advanced, and then click the Auditing tab.

If you want to set up auditing for a new user or group on the Audit tab, click Add.

A selection dialog box: User, Computer or Group.

Select the name of the user or group and click OK. Open Auditing Entry dialog box for. Here you can enter all the required audit settings.

In the Apply onto list, specify where you want to audit (this field is only available for folders I).

Under Access should specify what events should be monitored: graduated successfully (success) fail (failure) or both types of events.

Apply this to the audit objects and containers within this container only determines whether the subject entered the audit settings you make to files and folders that are located below the tree file system directories (is not checked). Otherwise, check the box (or select from the list Apply Only option for this folder. This will not perform an audit for the file system objects that are not of interest.

After the completion of the audit settings for a file or folder, click OK several times to close all dialog boxes.

If you want to view or modify audit settings for an existing user or group, click View / Edit. Appears Auditing Entry dialog box for. Here you will be able to carry out all the necessary changes to audit settings you selected user or group. Finished making changes, click OK.

Note. After you enable auditing of Windows 7 operating system begins to monitor developments related to security. The resulting information can be viewed using the Event Viewer snap-in. When viewing the event log, you can find out who attempted to perform unauthorized actions him.

*In order to be able to configure auditing for files and folders, you must have administrator rights.*

B) Viewing events in the event log.

To view events, follow these steps.

Select the Start button, taskbar.

Open the menu Configure / Control Panel.

In the window that opens, select the shortcut and then Administrative Tools Event Viewer.

In the new window, select Security (see Figure 3).

In the right half of the open window, a list of all registered events.



Figure 3

To view the required events, call its properties from the context menu or double-click on its name with left mouse button.

As a result, a window will appear as shown in Figure 4.



Figure 4

In the example shown, fixed success disable guest user account in Admin 08.05.04 18.28.31.

In the example shown in Figure 5, is fixed failure login user NT AUTHORITY \ SYSTEM (System account) 08.05.04 at 17:39:58 due to "unknown user name or password is incorrect."



Figure 5

Thus, the log viewer allows you to fully analyze the actions of users and processes.

**Tasks for independent work**

Enable auditing for success and failure of all the parameters (use the task A).

Log off and log on again to embark on an operating system with an incorrect password. Open the event log, find the entry screen and then copy to the clipboard (Print Screen) for submission to the teacher.

Remove the account you created earlier, the PP-7 and fix all syslog events associated with this action to represent the teacher report.

**Control questions**

* What is the difference in registration and auditing?
* What is the means of registration and auditing?
* What events are recorded in the system log?
* That fixes the system when an event occurs?

# List of recommended literature

**Main Sources:**

1. Anin, B. Yu protection of computer information / BJ Anin. - SPb .: BHV-St.-Petersburg, 2010. - 384 p.
2. Kaspersky researcher K. Notes computer viruses / K-Virus. - SPb .: Peter, 2006. - 316 p.
3. Kornyushin, PN Information security / PN Kornyushin, SS Kosterin. - Vladivostok: Publishing house of the Far Eastern State University, 2010. - 154 p.
4. Partyka TL Information security / TL Partyka, II Popov.- M .: FORUM: INFRA-M, 2012. - 432 p.

**Additional Sources:**

1. Asgarov TM Data protection and information security / TM Askerov. - M .: Publisher Plekhanov. Plekhanov, 2009. - 387 p.
2. Booths, VN Information security and data protection. Lecture notes / VN Booth. - Voronezh: VSU Publishing House, 2010. - 86 p.
3. Sychev, YN Fundamentals of Information Security / YN Sychev. - M .: Eurasian Open Institute, 2010. - 328 p.