Belarusian State Technological University
Department of Information Systems and Technology

Pavel Urbanovich

INFORMATION PROTECTION.

Part 2: BASIC METHODS

pav.urb@yandex.by, p.urbanovich@belstu.by

General Methods of Information (Data) Protection

Information (Data) protection covers three basic areas:

a) protection against **loss of Inf. (Data),**

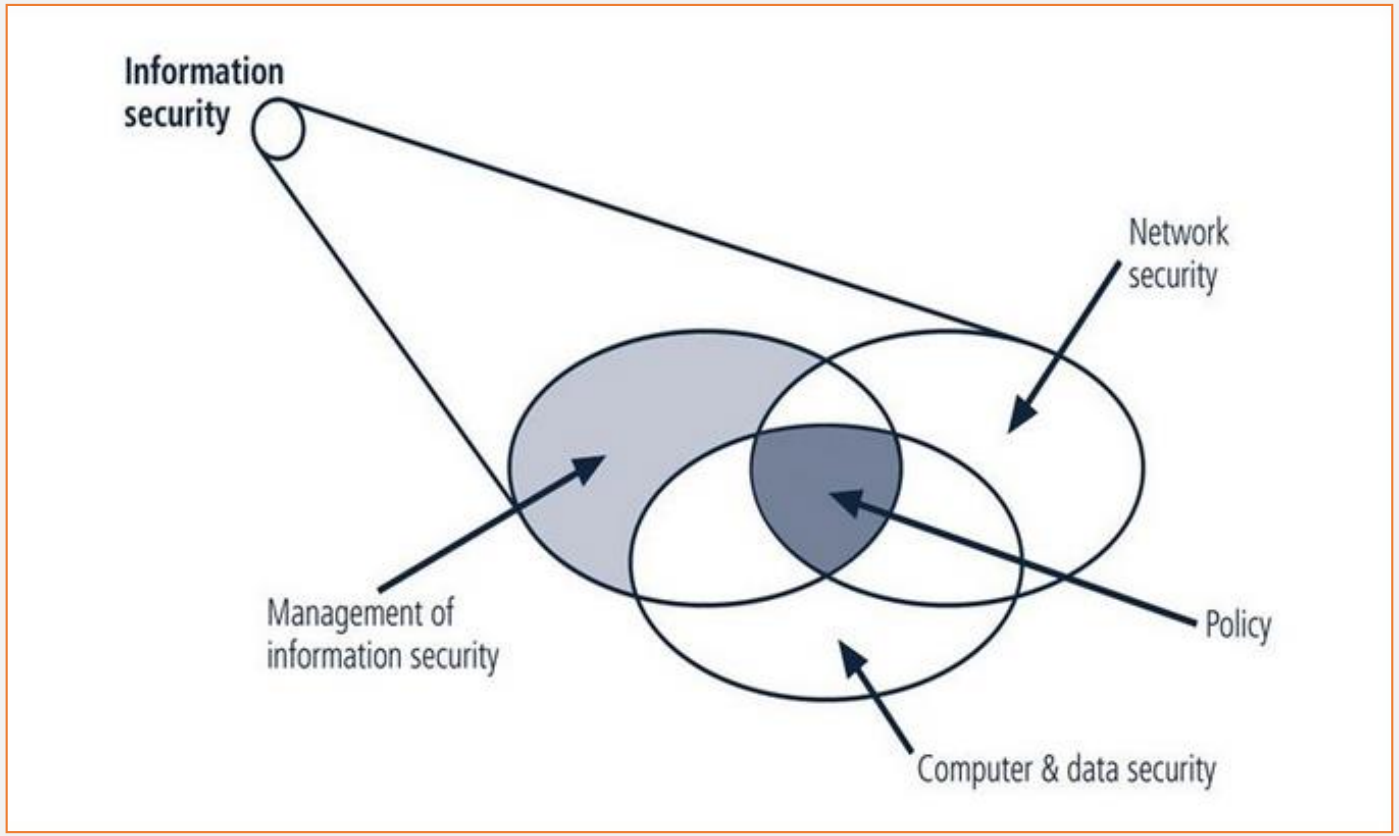
b) protection against **Inf. (Data) processing interruptions** (eg. in a bank: a transaction saved on one account and not shown on the other),

c) protection against **unauthorized access**.

Information (Data) protection procedures usually include:

- creation and securely storage of **back up** of your data, so you can quickly recover your lost data,
- backups of company operating data should be made **weekly** (to problem *a*),
- controlling the **access to data** in the system and **to equipment** (problems *a*, *c*),
- **anticipating threats** to the system and data, and developing preventive recommendations.

Information Protection (IP) as well as Information Security (IS) - one of the main challenges in IT - (today - **CyberSecurity**).



Information Security components

All different methods and used measures can be divided into **three classes:**

1. Legislation and regulations (the judiciary)
2. Organizational and technical means and methods
3. Hardware, programming, hardware and software methods and means

• Certificates, such as **ISO / IEC 27001**, include the requirements for ***Information Security Management Systems***.

• Three levels of security:
I. Security institution
II. Security of hardware and software in the institution
III. Security systems institutions

• On each level you specify:
- ❖ goal (intentions, end effect),
- ❖ strategy (how to achieve the goal),
- ❖ policy (concrete methods of strategy implementation).

A document with a sample company security policy:
www.securitum.pl/baza-wiedzy/publikacje/przykladowa-polityka-bezpieczenstwa

Legislations and Regulations

Constitution of The Republic of Belarus

Статья 25. Государство обеспечивает свободу, неприкосновенность и достоинство личности. Ограничение или лишение личной свободы возможно в случаях и порядке, установленных законом.

Статья 28. Каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

Статья 34. Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации….. Пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав.

Convention on CyberCrime

Convention established by the Council of Europe
-30 states sign Convention at opening ceremony in Budapest in 2001.

- **First international treaty on cyber crimes**, dealing particularly with:

- infringements of copyright,
- computer-related fraud,
- child pornography,
- violations of network security,
- racism.

- Contains a series of powers and procedures such as search of computer networks and interception.

- Main objective is to pursue a common criminal policy aimed at protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

The EU's Data Protection Directive

Data Protection Directive (*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*)

- **Every year on 28 January**, the European Commission celebrates **European Data Protection day**.
- 2016 was a historical year for data protection in the EU. **The EU agreed on a data protection reform** that will help stimulate the **Digital Single Market** in the EU by fostering consumer trust in online services and by providing legal certainty for businesses based on clear and uniform rules.
- **The European Commission** is now working to ensure that the rules work in practice.
- The data protection reform is a key enabler of the **Digital Single Market** which the **Commission** has prioritized. The reform will allow European citizens and businesses to fully benefit from the **digital economy**.

Personal Data Protection

Everyone has the right to the protection of **personal data.**

- Under **EU law**, personal data can only be gathered legally under strict conditions, for a legitimate purpose.
- People or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.
- In the EU, from May 25, 2018, the Regulation (EC) N 2016/679 of the European Parliament and the Council of the EU on the protection of individuals in the processing of personal data and on the free circulation of such data, as well as the repeal of Directive 95/46 / EC (**GDPR**), is applied. . The regulation concerns the protection of personal data of residents of the European Union. Therefore, it is important to know about the GDPR:

  - **belarusian** organizations, their representative offices in the EU that cooperate with individuals in the EU or target their sales of goods and services on them, including by monitoring demand, etc .;

Terminology

- Personal data: Information relating to an identified or identifiable of natural person (data subject).
- Processing: Any operations performed on personal data, whether or not by automatic means.
- Controller: Natural or legal person, public authority, agency or other body which … determines the purposes and means of processing of personal data.
- Processor: Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- Recipient: Natural or legal person, public authority, agency or other body to whom data are disclosed (unless in the course of a particular inquiry).
- Consent: Any freely given, specific and informed indication of wishes by which the subject signifies agreement to processing.

The Law (Akt) on Protection of Personal Data in **Belarus**

In **Belarus**, Ukraine, Russia and other countries the new EU **GDPR** regulations will have to be implemented primarily by companies working with personal data of persons in the EU:

- rights of individuals whose personal data are or may be processed in data files of data protection authorities,
- processing of personal data of natural people,
- competences of the Inspector General for the *Protection of Personal Data*,
- rules for securing personal data,
- rules of registration of personal data files,
- rules for the transfer of personal data to a third country.

Main Rules

- Personal Data may only be processed if:
  - the data subject has given his/her consent.
- It is necessary to process:
  - for the performance of a contract, the subject of which is a person;
  - or to protect the interests of the data subject,
  - or to perform a task in the public interest.

- The data is processed according to good practice data processing.
- Data to be processed is adequate, relevant and not excessive in relation to the purposes for which it is collected.
- Data processing will be organised in a manner that ensures required updating of data.
- The data collected can not be stored in a form that allows the data subject to be identified for longer than is necessary for the purposes for which the data is processed.

Notification

- **Processing of personal data in general requires pre-notification to the *Data Protection Agency***, including:

1. Name and address of controller, his representatives + processor.
2. Category and purpose of processing.
3. General description of processing.
4. Description of categories of data subjects and data about them.
5. Recipients to whom data may be disclosed.
6. Proposed transfers of data to third countries.
7. General description of security measures.
8. Dates for commencement of processing an erasure of data.

- Exceptions when:

– data are not confidential; or
– purpose is to keep a legally required register intended to provide information to the public.

Security of Processing

• Those who work for controller or processor may only process data on instructions from the controller.

• Controller and processor must implement appropriate technical and organisational security measures to protect data against:

-accidental destruction or loss,
-unauthorised disclosure or other processing.

• Controller has a duty to ensure that processors can implement necessary security measures.

• There must be a written contract between controller and processor, stipulating the security measures and (if necessary) the country in which the law is to be applied.

Protection of Intellectual Property

- *Three legislative frameworks* are applicable to programs and data:
  - *copyright law*,
  - *patent law*,
  - *trade secrets law*.

- Copyright law was conceived to protect works of art, music, literature.
  - ➢ Provides incentive to produce works of art.

- Patent law was conceived to protect inventions and innovation in science, technology and engineering.
  - ➢ Provides an incentive to inventors to disclose their inventions.

- Trade secrets identify information that must be kept secret.

Organizational and Technical Measures and Methods

To build a IS policy, the following areas of protection are taken into account:

-protection of objects,

-protection of processes,

-procedures and information processing programs,

-protection of communication channels,

-suppression of secondary electromagnetic emissions,

-management of the security system.

The first line of defense is to secure physical access to resources.

What can be done with physical access to a well-secured computer?

- to steal it in its entirety
- to remove the data drive
- to reset the BIOS
- to connect additional hardware, such as spyware
- to clasp the network cables

In rooms of administrators and server rooms there are often located unsecured terminals. Notes, documents, prints, work prints, backups can be found there.

According to some rules, such things must be:

- classified
  (proprietary, confidential),

- secured from the electronic side
  (encryption of backups, databases, …),

- appropriately protected physically
  (armored cabinets, keys in safes, combination locks,
  biometric protection, …).

Organizational and Technical Protection

Organizational and technical protection provides:

-organization of protection,

-systematic work with staff,

-documents, instructions, internal regulations,

-the use of technical security measures (for example the simplest door locks, magnetic cards or other means of identifying individuals, etc.),

-information and analytical activities to identify internal and external threats,

-systematic staff exercises.

Methods Based on Hardware and Software Tools

Combine security services, built into network operating systems.

Include:

- identification and authentication,
- access control,
- logging,
- audit,
- cryptography,
- steganography,
- screening,
- UPSs.

Access Control

Goal: Protect confidentiality and integrity of information.

- Control what a subject can do to prevent damage to the system.
- Regulate the operations that can be executed by a subject on data and resources.
- Typically provided as part of operating systems and of database management systems.

Concepts:

- The basic idea of access control is that there is an active subject requiring access to a passive object to perform some specific access operation.
- A reference monitor grants or denies access.

Subjects:

- Active entity performing operations in the system.
- Subjects can be classified into:
  - *users*: single individuals connecting to the system,
  - *groups*: sets of users,
  - *roles*: a function or a position within a organization,
  - *processes*: executing programs on behalf of users.
- Relations may exist among the various types of subject.

Objects:

- Any system resource.
  - *file, printer, host, room, building* etc.
- Protection objects: objects controlled by access control system.

Note: *not all resources managed by a system need to be protected.*

Access Rights

- Operations that a subject can execute on protection objects.
- Each type of operation corresponds to an access right:
  - access control must be able to control the specific type of operation.
- The most simple example of access rights is:
  - *read*: look at the contents of an object,
  - *write*: change the contents of an object.
- Other types of rights depending on the resources to be protected:
  - *execute*, *select*, *insert*, *update*, *delete*, etc.
- Advanced Rights: *ownership*, *delegate*, *remove.*

Example: Unix subjects, Objects, Rights

- Subjects: *users*, *groups*, *others*.
- Objects: *files*, *directories*.
- Access rights: *read*, *write*, *execute*.

- For files:
  - *read*: reading from a file,
  - *write*: writing to a file,
  - *execute*: executing a (program) file.

- For directories:
  - *read*: list the files within the directory,
  - *write*: create, rename, or delete files within the directory,
  - *execute*: enter the directory.

Access Control vs. Authentication

Completely different things.

- **Access Control:**
  -Establishing if a user has the right of doing a certain operation.

- **Authentication:**
  -Establishing who you are whether a user possesses a certain attribute or not.

- Authentication is necessary for access control.

Access Control Models

- Access control models (policies): define who can access to resource.

- Discretionary (DAC) or Identity Based AC (IBAC)
- Mandatory (MAC)
- Role-Based (RBAC)
- Attribute-Based (ABAC)

- Administrative policies: define who can specify access control policies (models).

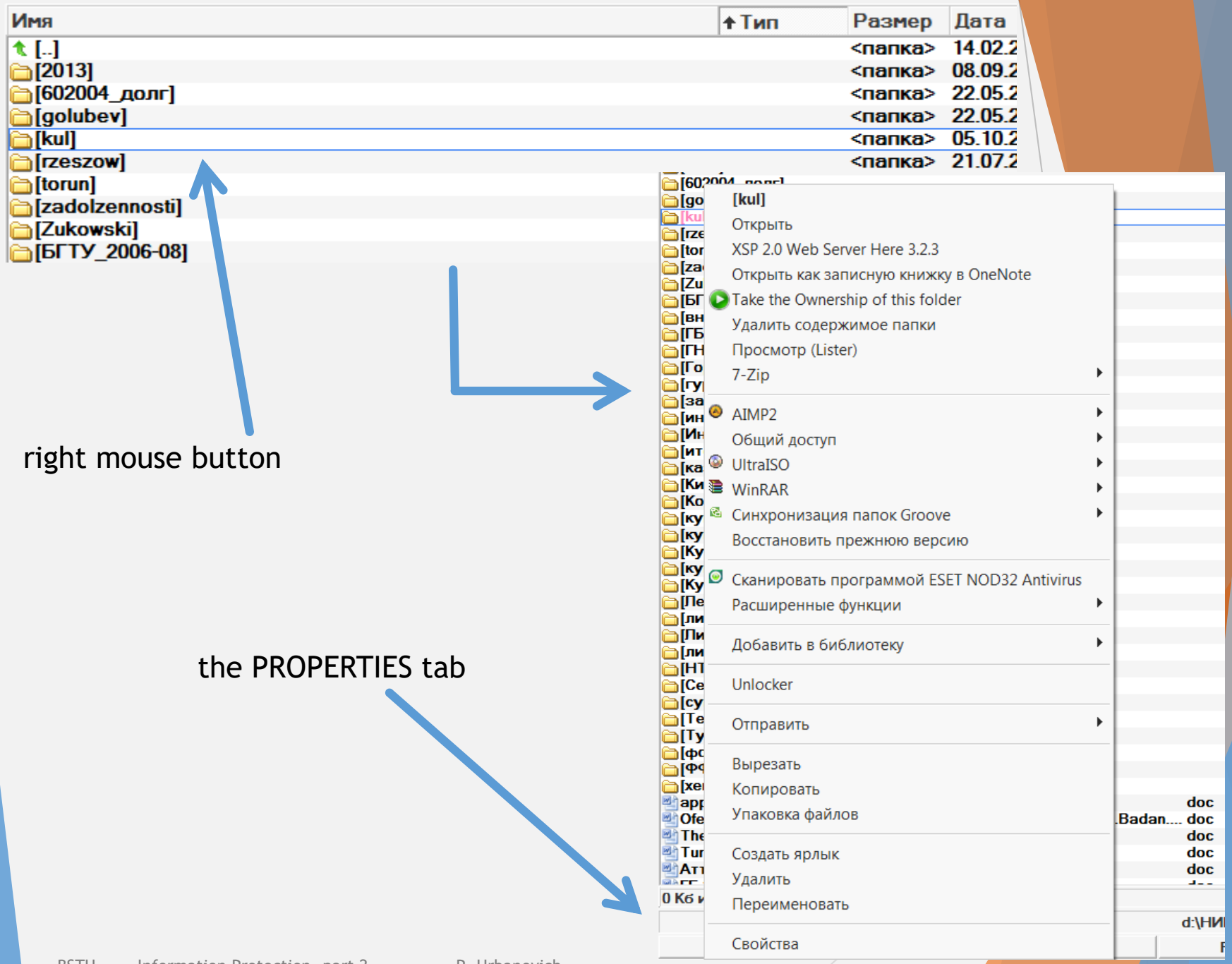
The Concept of DAC

DAC (**D**iscretionary **A**ccess **C**ontrol) - applied security policy taking into account the identity of the objects and their rights;

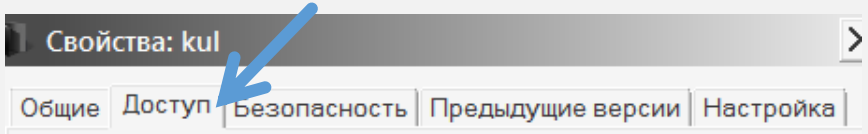
- the user (subject) passes his/her privileges to the running (activated) processes (object),
- for **each pair** (subject-object), an enumeration of the allowed access types (read, write, etc.), that is, those types of access that are authorized for a given subject (individual or group of individuals) to the given resource (object),
- there are several approaches to constructing discretionary access control,

- each object of the system has a subject connected to it, called the **owner**,
- the **owner** determines the access rights to the object,
- the system has one dedicated subject –the **superuser** (administrator), who has the right to establish ownership rights for all other subjects of the system,
- a subject with a certain right of access may transfer this right to any other entity.

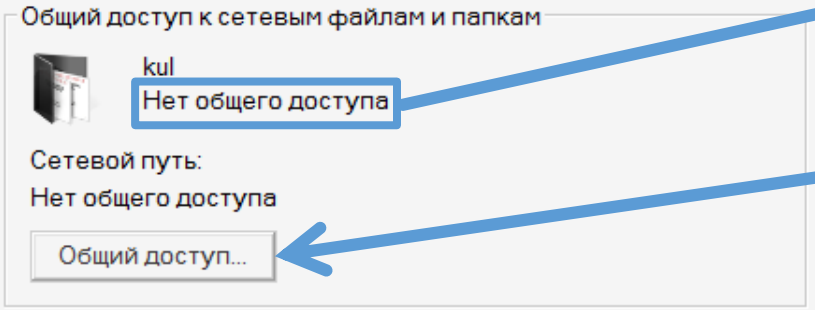
- The traditional Unix system of users, groups, and read-write-execute permissions is an example of DAC.


Имя
Тип
Размер
Дата
[..]
[2013]
[602004_долг]
[golubev]
[kul]
[rzeszow]
[torun]
[zadolzennosti]
[Zukowski]
[БГТУ_2006-08]
<папка>
[kul]
Открыть
XSP 2.0 Web Server Here 3.2.3
Открыть как записную книжку в OneNote
Take the Ownership of this folder
Удалить содержимое папки
Просмотр (Lister)
7-Zip
AIMP2
Общий доступ
UltraISO
WinRAR
Синхронизация папок Groove
Восстановить прежнюю версию
Сканировать программой ESET NOD32 Antivirus
Расширенные функции
Добавить в библиотеку
Unlocker
Отправить
Вырезать
Копировать
Упаковка файлов
Создать ярлык
Удалить
Переименовать
Свойства
right mouse button
the PROPERTIES tab

the ACCESS tab

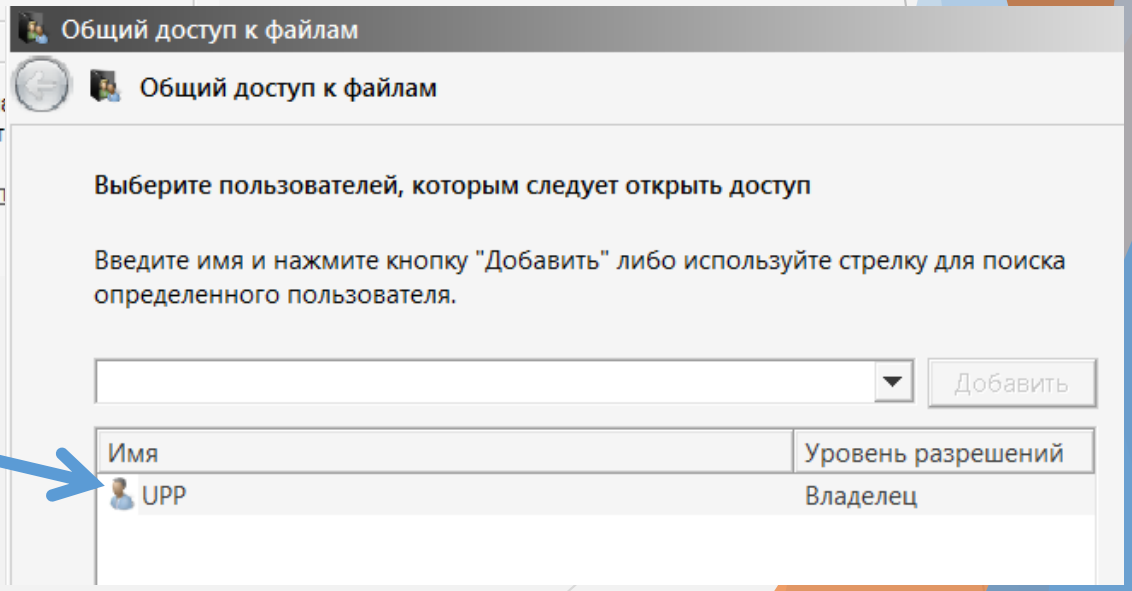


there is no GENERAL ACCESS



GENERAL ACCESS

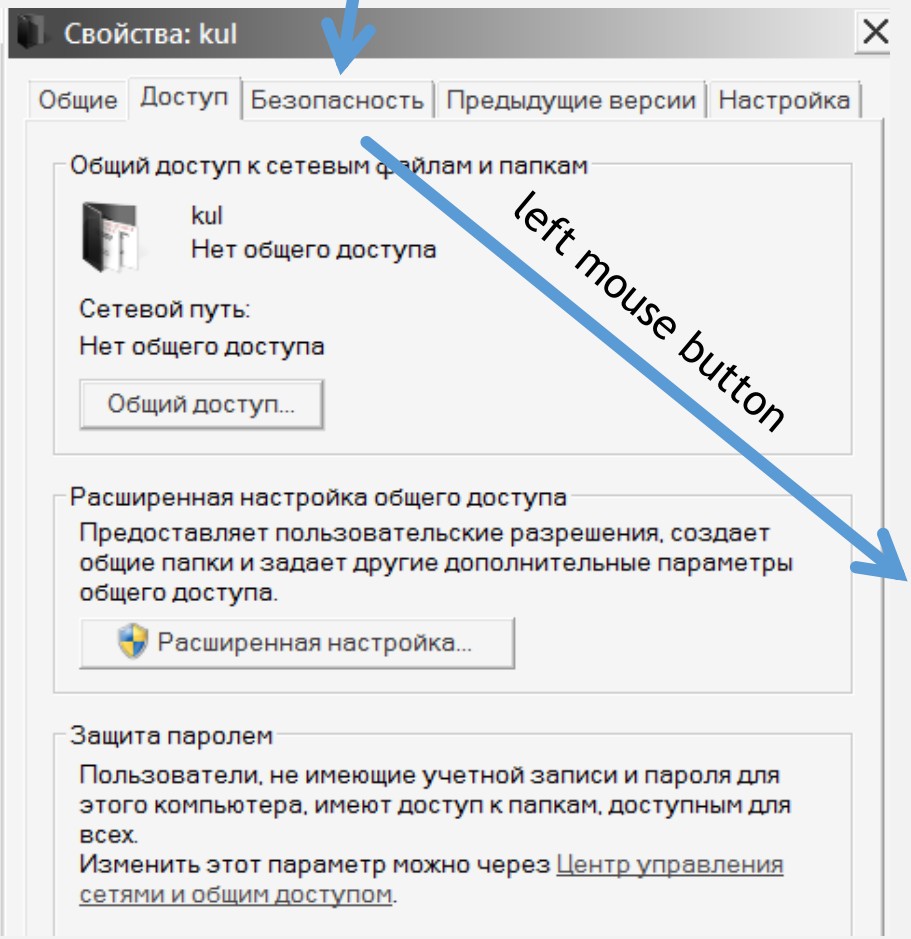
left mouse button



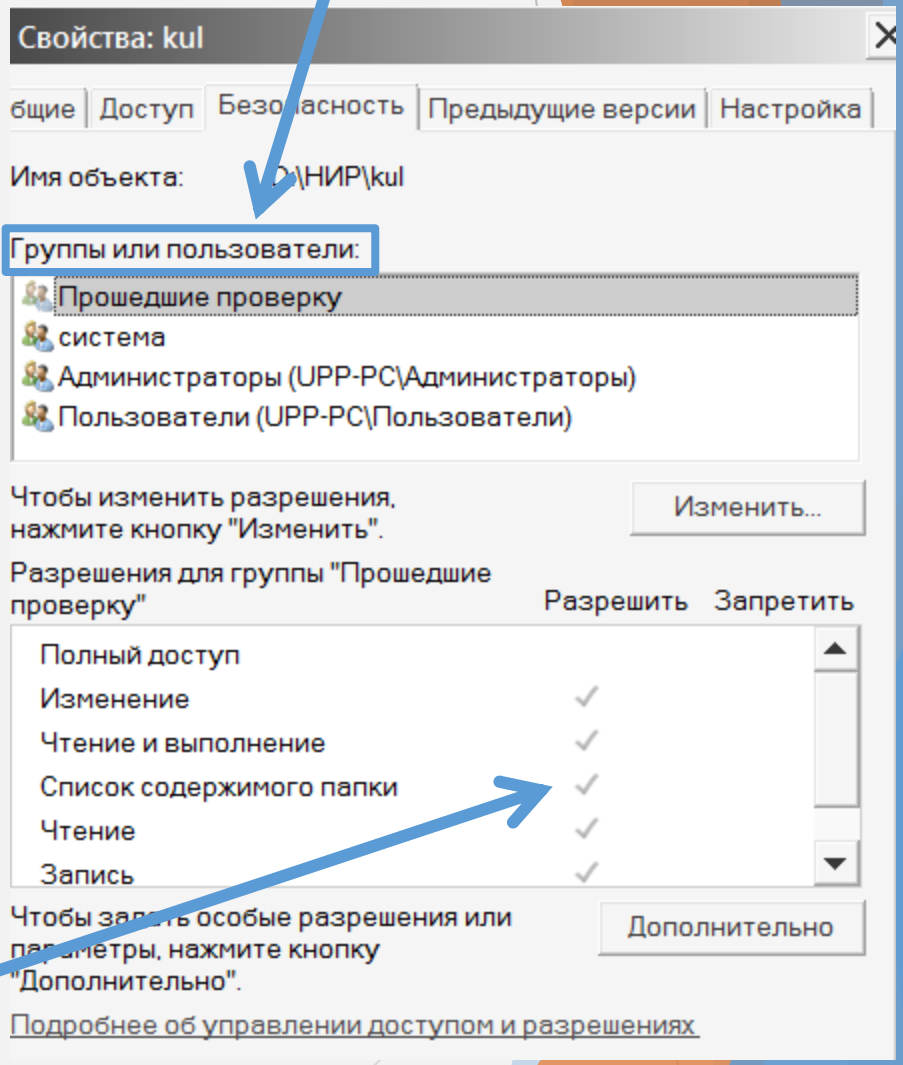
resource owner

SECURITY tab

GROUPS or USERS



left mouse button



granting the right of access

The Concept of MAC

Mandatory **a**ccess **c**ontrol(**MAC**) - the system constrains the ability of a *subject* or *initiator* access to an *object* based on **multiple levels of security.**

Subjects and objects each have a set of **security attributes**.

Multilevel security or **multiple levels of security**(**MLS**) is the application of a computer system to process information with incompatible classifications (i.e., at **different security levels**), permit access by **users with different security clearances** and prevent users from obtaining access to information for which they lack authorization.

Linux and many other Unix distributions have **MAC for CPU (multi-ring), disk,** and **memory.**

Microsoft Starting with Windows Vista and Server 2008 Windows incorporates **Mandatory Integrity Control**, which adds ***Integrity Levels***(**IL**) to **processes running** in a **login session.**

Elements of a Security Management Policy

1: Inventory of Authorized and Unauthorized Devices.

2: Inventory of Authorized and Unauthorized Software.

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.

4: Continuous Vulnerability Assessment and Remediation.

5: Malware Defenses.

6: Application Software Security.

7: Wireless Access Control.

8: Data Recovery Capability.

9: Security Skills Assessment and Appropriate Training to Fill Gaps.

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.

11: Limitation and Control of Network Ports, Protocols, and Services.

12: Controlled Use of Administrative Privileges.

13: Boundary Defense (net's).

14: Maintenance, Monitoring, and Analysis of Audit Logs.

15: Controlled Access Based on the Need to Know.

16: Account Monitoring and Control.

17: Data Protection.

18: Incident Response and Management.

19: Secure Network Engineering.

20: Penetration Tests and Red Team Exercises.

References:

1.Urbanowicz, P. Bezpieczenstwo w cyberprzestrzeni a prawo karne / P. Urbanowicz, M. Smarzewski // Ksiega pomiatkowa pomiatkowa ku czci Księdza Profesora Andrzeja Szostka MIC, Lublin: KUL. – 2016. – P. 479-488 (URL: https://elib.belstu.by/handle/123456789/28916)

2. Урбанович, П. П. Информационная безопасность и надежность систем : учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. - Минск : БГТУ, 2007. - 87 с. (URL: http://elib.belstu.by/handle/123456789/2937)

3. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студ.. - Минск : БГТУ, 2016. - 220 с.
(URL: http://elib.belstu.by/handle/123456789/23763)

4. Урбанович, П. П. Защита информации и надежность информационных систем : пос. для студ. вузов спец. 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)» / П. П. Урбанович, Д. В. Шиман.- Минск : БГТУ, 2014. - 91 с. (URL: https://elib.belstu.by/handle/123456789/23761)

4. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. - Lublin : Wydawnictwo KUL, 2004. - 150 p. (URL: https://elib.belstu.by/handle/123456789/27516)

5. Osborn S., Sandhu R., Nunawer Q. Configuring Role-Based Access Control To Enforce Mandatory And Discretionary Access Control Policies, ACM Trans. Info. Syst.

6. Steve Demurjian. Implementation of Mandatory Access Control in Role-based Security System, 2001

7. [Electronic Resource], URL: https://oficynamm.pl/oferta_elementy/do_pobrania/ szkola/ odows_artykul.pdf

8. [Electronic Resource], URL: http://kft.umcs.lublin.pl/mgozdz/bezpieczenstwo-wyklad.pdf

9. [Electronic Resource], URL: www.securitum.pl/baza-wiedzy/publikacje/przykladowa-polityka-bezpieczenstwa

10. [Electronic Resource], URL:http://www.giodo.gov.pl/