Improving the safety and quality of the software of computer systems in the context of innovative development of industry

Full Doctor (Doctor of Engineering Sciences),
Senior Researcher, Associate Professor,
Head of Computer Engineering
& System Programming Department,
Khmelnitsky National University
Tetiana Hovorushchenko

Actuality

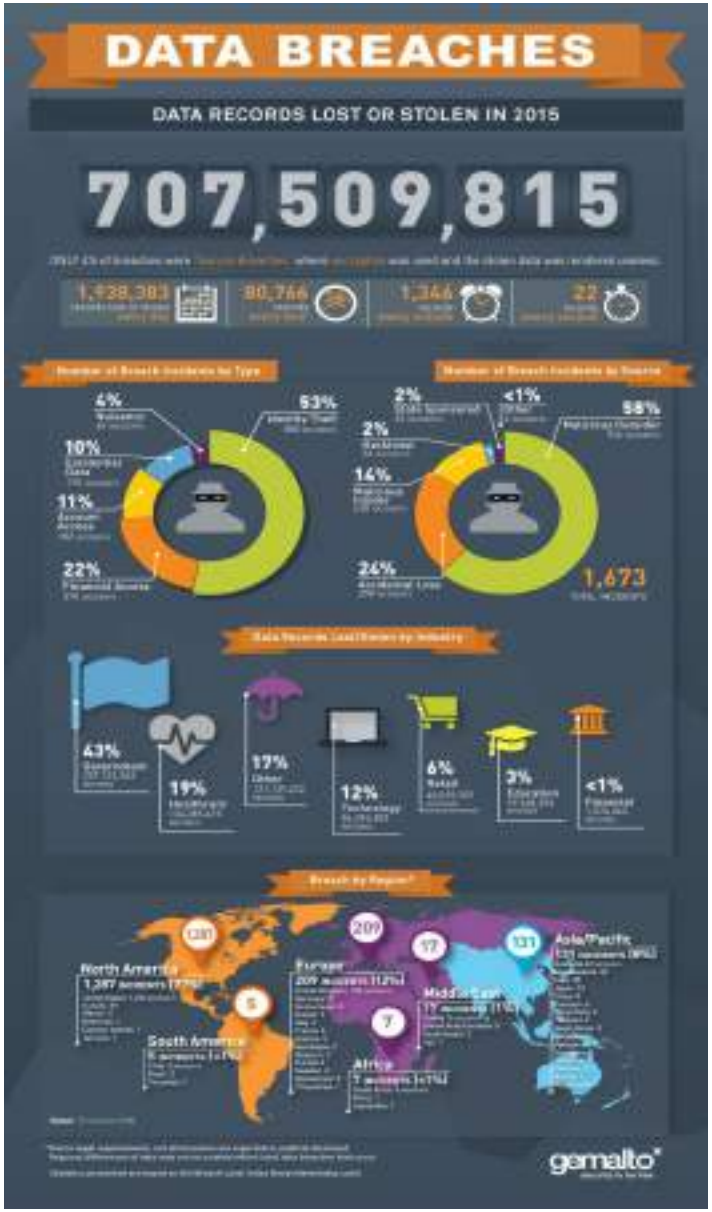
- At the present stage of economic development of Ukraine, the information's management becomes a critically important function to business, and volumes of information are constantly growing, so the issue of information security is all the more acute
- Cyber attacks on systems of critical infrastructure cause real threats to the safety of the general community, and software bugs and failures are threatened by catastrophes that lead to human casualties, environmental disasters, significant financial losses

Problems

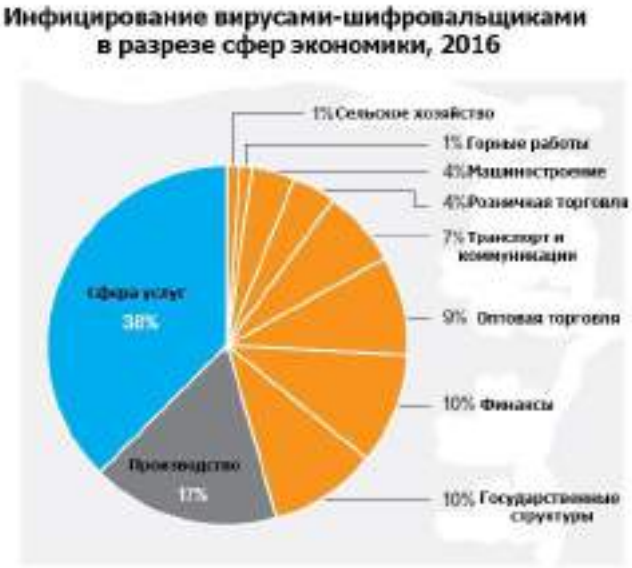
Currently, all spheres of human activity are related to computer systems (CS), the basis of which is software

- Actual problem №1 during using CS – reliable protection of information from cyber-threats and malware (viruses)
- Actual problem №2 during developing software for CS – improving the quality of software due to the automated evaluation of the completeness of displaying business requirements in the software requirements specifications (SRS), on the basis of which further development of software is followed

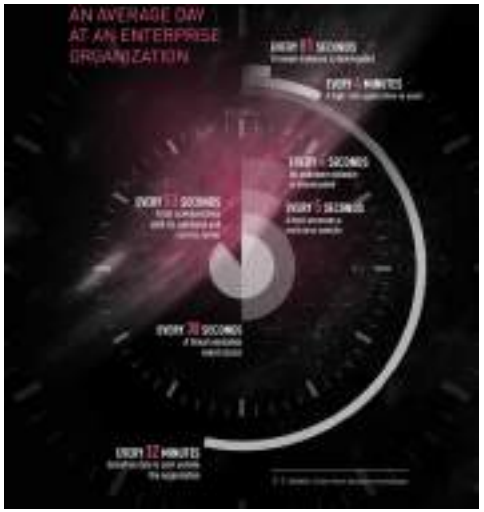
Problem №1



Criticality Index of Data Loss



Infection of CS by viruses in the context of economic spheres

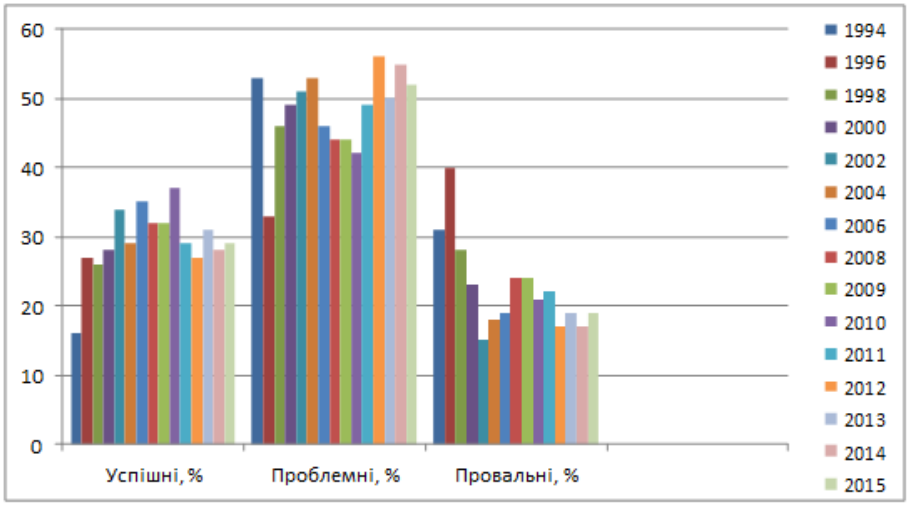


An average day at an enterprise organization

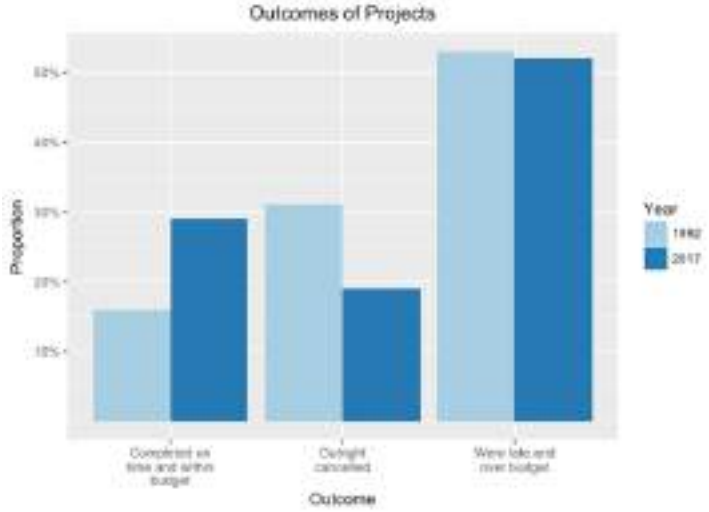
Problem №1

- Every month, Ukraine is exposed to cyber attacks by 3000-3500 times
- The most "famous" results of cyber attacks were the hacking of the Ukrzaliznytsia system, the Ministries and the Pension Fund
- During the cyber attack BugDrop, which took place in Ukraine in February 2017, malicious software was sent to users and more than 600 gigabytes of information was stolen
- "Petya" virus in Ukraine in June 2017 infected with 12.5 thousand computers, resulting in a country suffered a million losses
- Cyber-war between Ukraine and Russia, during which Ukraine turned into a testing ground for Russian hackers
- Only 46% of malware is detected by antivirus products
- In the last 12 months, every second industrial company in the world has experienced from one to five cyber incidents

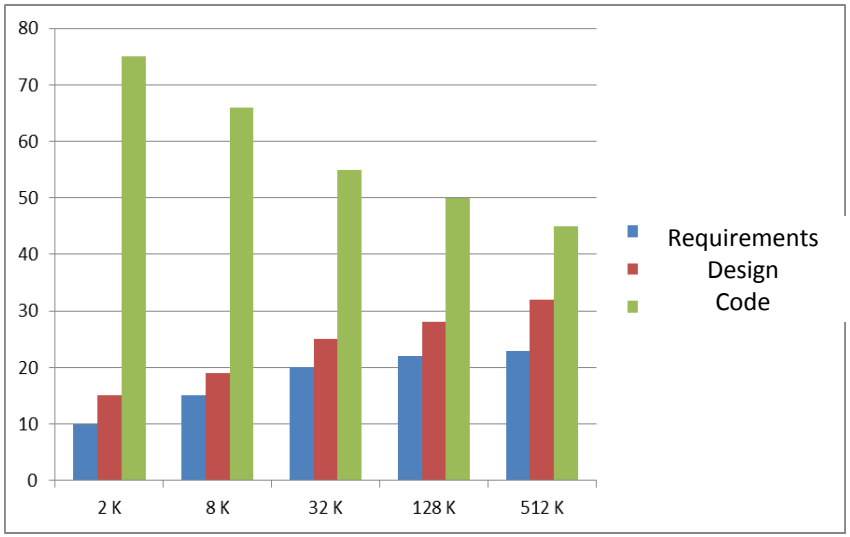
Problem №2



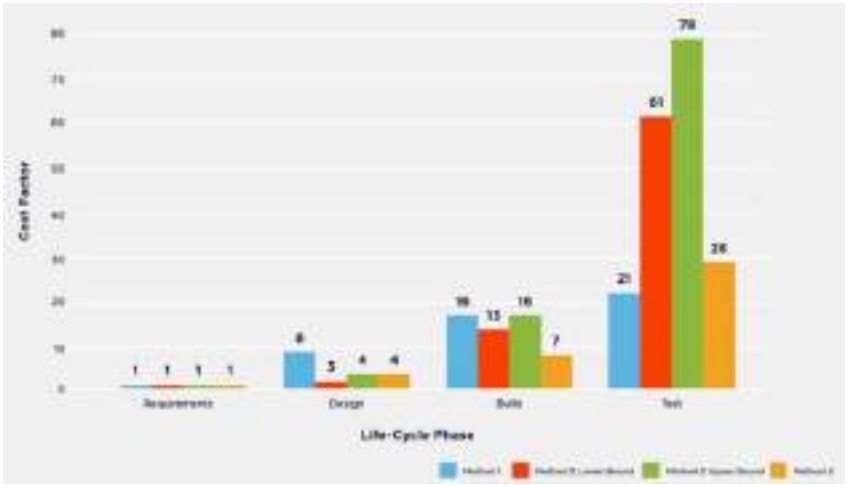
Statistics on the success of software projects in 1994-2015



Comparative statistics of the success of software projects in 1992 and 2017



Distribution of software bugs, which emerged at different stages of the life cycle



The cost to fix software defects rose exponentially with each successive stage of the project life cycle

Problem №2

Examples of accidents due to inaccuracy and incompleteness of the requirements in SRS:

Event	Cause	Consequences
Explosion of rocket Ariane 5 in 1996	Mismatch of requirements to ensure reliability and maximum allow-able load	The cost of equipment and development - 7.5 $ billion, "lost profits" - 2 $ billion
Accidents of Mars Climate Orbiter and Mars Polar Lander in 1999	Defects in the project through the use of different measurement units	327.6 $ million – apparatus, 91.7 $ million - launch
Violation of flight of launch vehicle of Titan IV in 1999	Error in software of management system of motor	The loss of the satellite Milstar
The crash of plane «Superjet 100»	Incompatibility and inconsistency of software	The death of 48 people

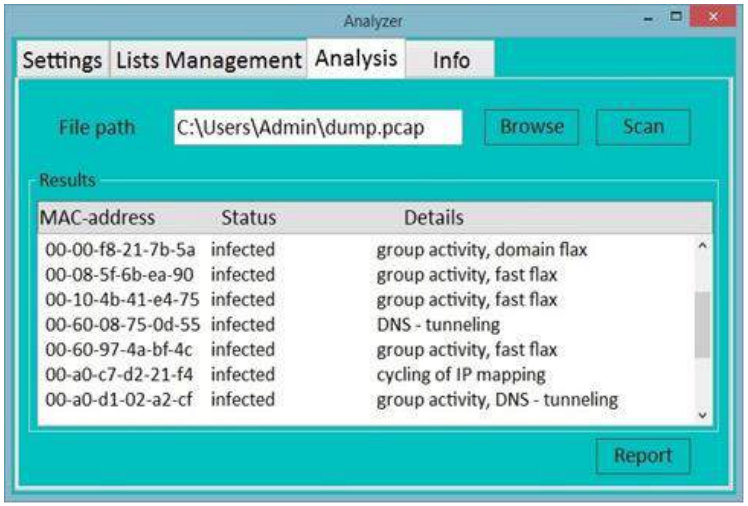
Event	Cause	Consequences
"Death" sessions of radiation therapy with Therac-25 in 1985-1987 [27]	Incompleteness of SRS; defects in the development and formulation of the project; incorrect assessment and prediction of risks	6 patients received a lethal radiation dose
Failure in mobile system of missile defense "Patriot" in 1991 [27, 28]	Rounding error that was not critical at the level of a single component, but intensified during its integration into the system	28 American soldiers were killed and about 100 people were injured
Falling into the Pacific Ocean of three satellites in 2010 [27, 29]	Error in software system integration	The impossibility of completing the GLONASS

Analysis of the results obtained by other scientists

- Known approaches and systems for detecting cyber-threats and malicious software are not capable of ensuring reliable and effective protection of the CS from cyber-threats and malware, and are not capable to counteract and neutralize them due to the imperfection of the methods and the increase in the number of new cyber-threats and malware
- The current state of the field of software engineering implies that a person forms the software requirements specification (SRS) based on business requirements, which often leads to losses of essential information and to the occurrence of errors in the early stages of the software lifecycle. The consequences of insufficiency of information in the SRS are to reduce its quality, reliability, functional safety and security, survivability and dependability, and the unsuccessfulness of software projects

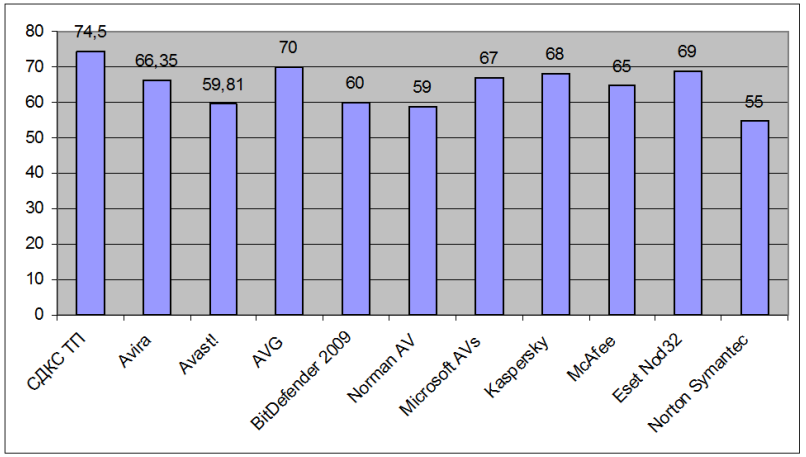
The intelligent system for detection of cyber-threats and malware

Subsystem for diagnostics of the CS for the presence of Trojans in the scanner mode



Subsystem for detection of botnets on the basis of analysis of DNS-traffic

Subsystem for detection of metamorphic viruses

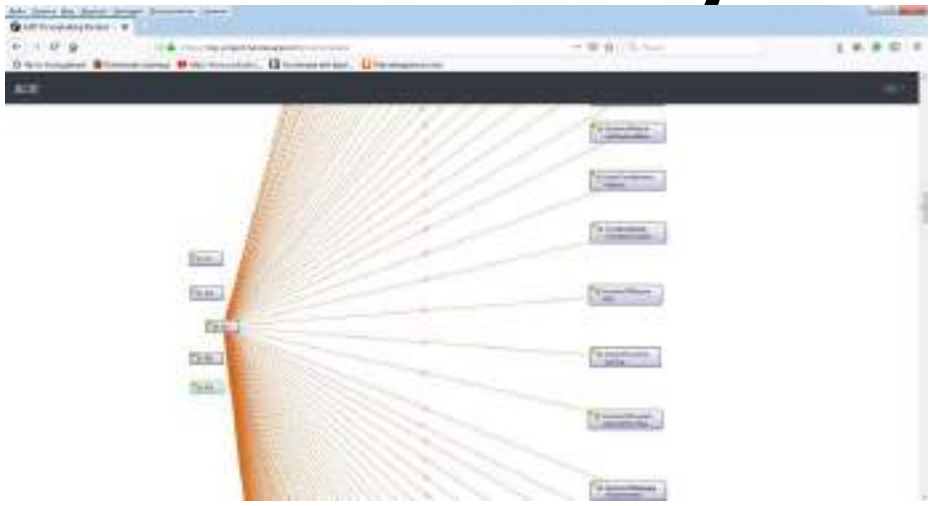


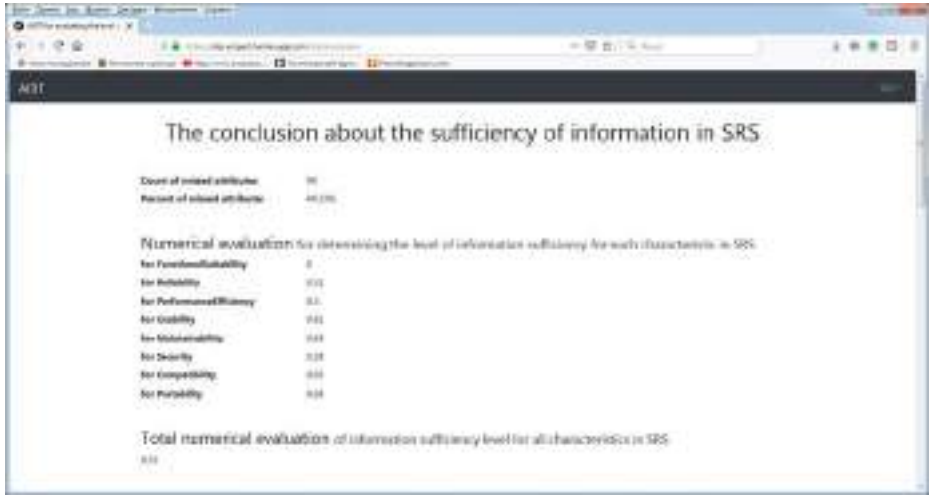
The validity of diagnostics of the CS for the detection of cyber-threats and malware

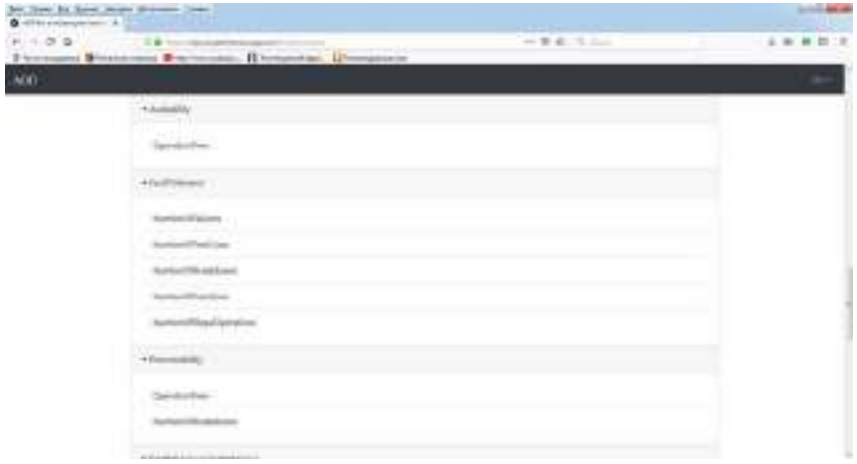
The intelligent system for detection of cyber-threats and malware:

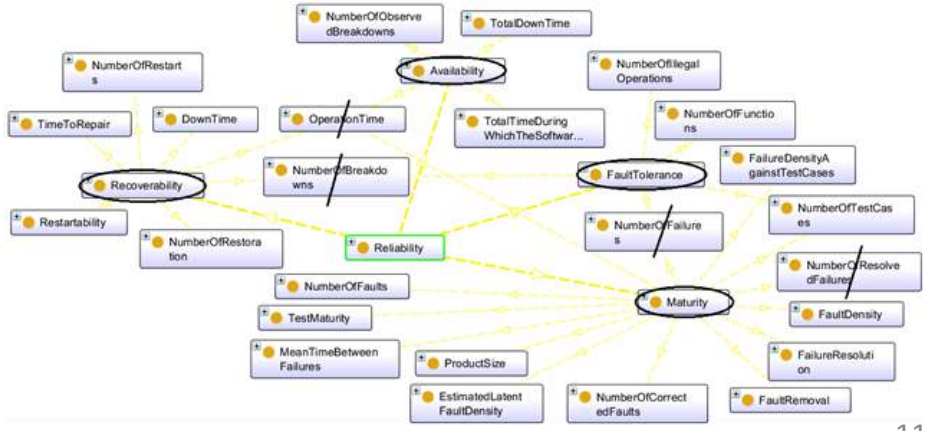
- improves the validity and effectiveness of detecting the cyber-threats and malware, reducing the level of false positives and the computational complexity of the detection process
- raises the efficiency of diagnosing computer systems for the availability of new Trojan programs
- increases the validity of detection of bots of known and unknown botnets by 8-22% compared to known tools of detecting the botnets
- raises the validity of detecting the metamorphic viruses by 7-14%

Intelligent system for automatically analyzing the software requirements specifications on the subject of the sufficiency of their information









Intelligent system for automatically analyzing the software requirements specifications on the subject of the sufficiency of their information:

- assesses and increases the level of information sufficiency (as required and at the customer's request - up to 100%) in the SRS, reducing the size of the knowledge gap and the sector with unknown information about software, which arises as a result of information losses due to incompleteness and difference in understanding of needs and context of SRS information
- improves the quality of software which will be develop by the SRS
- automates routine parsing the SRS
- provides quick training for system engineers and project managers

Results of our research team

- 2 successfully completed International Scientific projects (TEMPUS SAFEGUARD, TEMPUS SEREIN), dedicated to the issues of providing the cybersecurity in the CS and improving the quality of software
- 1 doctoral dissertation and 4 candidate's dissertation were defended, 1 more candidate's dissertation is being prepared for defence
- a number of papers have been published in periodicals included in the rating international scientometric databases; a number of reports have been submitted at the rating international conferences in Ukraine and in Europe

The possibility of using the obtained solutions for the industry

- the developed systems can be used in state institutions, military formations and law-enforcement bodies (in particular, in cyber police), because they are aimed at ensuring the national security of Ukraine in terms of increasing its cybersecurity
- in commercial organizations the developed systems can protect the company's CS from cyber-threats and malware, and also enable the enterprise (as the software customer) to evaluate the level of development of the initial stages of the lifecycle by developers (in particular, evaluate and, if necessary, force developers to improve the quality of the SRS, as well as select the most qualitative specification in the presence of several alternative SRS)

THANKS FOR YOUR ATTENTION!

Tetiana Hovorushchenko,

Full Doctor (Doctor of Engineering Sciences),
Senior Researcher, Associate Professor,
Head of Computer Engineering
& System Programming Department,
Khmelnitsky National University (Ukraine)

tat_yana@ukr.net ,
govorushchenko@gmail.com