|  |
| --- |
| Discipline „Information Protection and Security”, code: 44-b |
| Annotation: The main objective of the course is to provide students with knowledge and skills to assess the security risk of a computer network. The types of attacks and malicious code that cause inaccessibility or degradation of the quality of network services are considered. Students are acquainted with the current standards for security of the data transmitted through the Internet. Modern networking solutions and information security solutions to achieve optimal modularity, robustness, flexibility, security and ease of management are analyzed. The typical potential vulnerabilities of the network protocols, infrastructures, models and services are presented. |
| Main issues of the syllabus content:* International standards concerning computer network security. Standards BSS, ISO / IEC. Stages and activities to build a network security management system.
* Security of classified information networks - basic principles and requirements. Major vulnerabilities. Risk - nature, detection, risk assessment, risk minimization mechanisms. Information and network security policies. Requirements for security policies.
* Security of the OS. Linux security model. Windows server security model. Protecting files and directories. Controlling access to objects.
* Security of the OS. Malware - viruses, worms, Trojans. Detection and protection. Buffer overflow attack.
* TCP / IP protocol suite vulnerabilities. IP spoofing and Denial of Service attacks (DoS).
* DNS attacks. Vulnerabilities of zone transfer and dynamic updates. DNS Cache Poisoning Attack.
* Port scanning - Nmap. Vulnerability scanning - Nessus. Passive packet monitoring.
* Corporate information security solutions. Firewalls – purpose, functionality, classification.
* Authentication vulnerabilities. Dictionary attacks. Breaking passwords with Rainbow Tables. Password-by-pass schemes.
* Bots and Botnets. Distributed DoS attacks.
* Security issues in Peer-to-Peer networks (P2P).
* Security on wireless networks.
* Web security. SQL injection attack. Web spoofing (fishing). Clickjacking.
* Security in virtualization and
 |