FUNDAMENTALS OF INFORMATION SECURITY

Lecturer: Sagymbekova A. O.

Learning outcomes

Students successfully completing the course will be able to:

- describe the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures;
- identify the tactics, techniques and procedures used by cyber criminals;
- apply technologies, products, and procedures are used to protect confidentiality, to ensure integrity, to provide high availability;
- analyze network intrusion data to verify potential exploits;
- use network monitoring tools to identify attacks against network protocols and services;
- choose various methods to prevent malicious access to computer networks, hosts, and data

List of laboratory works

1	Traditional ciphers
2	Modern Symmetric Key Encryption
3	Asymmetric Encryption Algorithms
4	Encrypting and Decrypting Data using a Hacker Tool
5	Using Wireshark to Examine Ethernet Frames, to Observe the TCP 3-Way Handshak Exploring Nmap
6	Linux administration: Locating Log Files, Linux Servers, Navigating the Linux Filesystem an Permission Settings
7	Attacking a MySQL Database
8	Extract an Executable from a PCAP
9	Interpret HTTP and DNS Data to Isolate Threat Actor
10	Isolated Compromised Host Using 5-Tuple

Basic literature

- Computer Security. Principles and Practise / William Stallings, Lawrie Brown.- Second edition.- USA: Pearson Education Inc., 2012.
- Understanding Cryptography. Paar, C.- New York, 2010
- Management of Information Security / M.E. Whitman, H.J. Mattord.- Fourth Edition.- USA: Cengage Learning, 2014

Supplementary literature

- Applied cryptography: Protocols, Algorithms, and Source Code / Bruce Schneier.- United States of America: John Wiley & Sons, Inc, 1996
- Securiti Enqineerinq / R. Anderson.- Second edition.- Canada: Wiley, 2008.
- Beautiful Security [Текст]: Leading Securuty Experts Explain How They Think / A. Oram, J. Viega.- USA, Sebastopol: O'Reilly, 2009.
- Open Source Security Tools / Raven Alder, Josh Burke.- USA: Syngress Publishing, Inc, 2007.
- Implementing Cisco Security Mnitoring, Analysis and Response System.- USA: The power of knowing, 2009.
- Security+ Study Guide / Ido Dudrawsky.- USA: Linacre house, 2010.
- Introduction to Hardware Security and Trust / M Tehranipoor; Editors: Wang Cliff.- USA: Springer, 2012.
- Cryptography Engineering : Design Principles and Practical Applications / N Ferguson, B Schneier, T Kohno.- United States of America: Wiley Publishing, Inc., 2010.
- Principles of Database Security / S. Balamurugan, S. Charanyaa.- Germany: Scholars Press, 2014.
- Cybersecurity Essentials. On-line e-book at www.netacad.com
- CCNA Cybersecurity Operations. On-line e-book at www.netacad.com
- Cybersecurity Essentials. Student Lab Source Files.
- CCNA Cybersecurity Operations. Student Lab Source Files.

Student performance evaluation system for the course

Period	Assignments	Grade (%)		Total
1st attestation	Labs (1-6) Practice (5-6) Quize (1-2) MidTerm	10 each 5 each 5 each 20	60 10 10 20	100 % (30 points)
2nd attestation	Labs (7-10) Practice (7-9) Quize (3-4) EndTerm	11*2+15*2 6 each 5 each 20	52 18 10 20	100 % (30 points)
Final exam	Written Exam	100	100	100 % (40 points)
Total	0,3*1stAtt+0,3*2ndAtt+0,4*Final			100

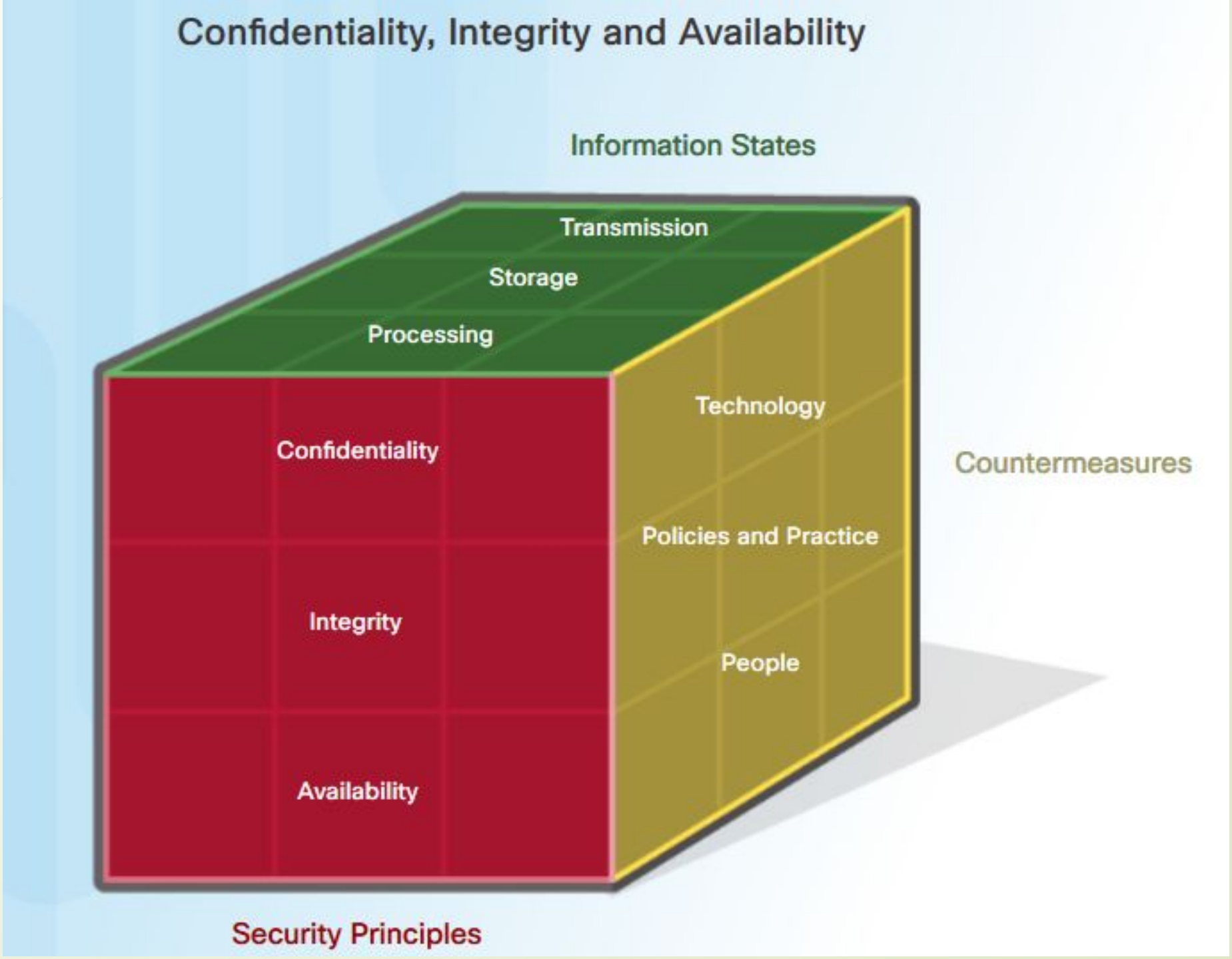
Cybersecurity principles

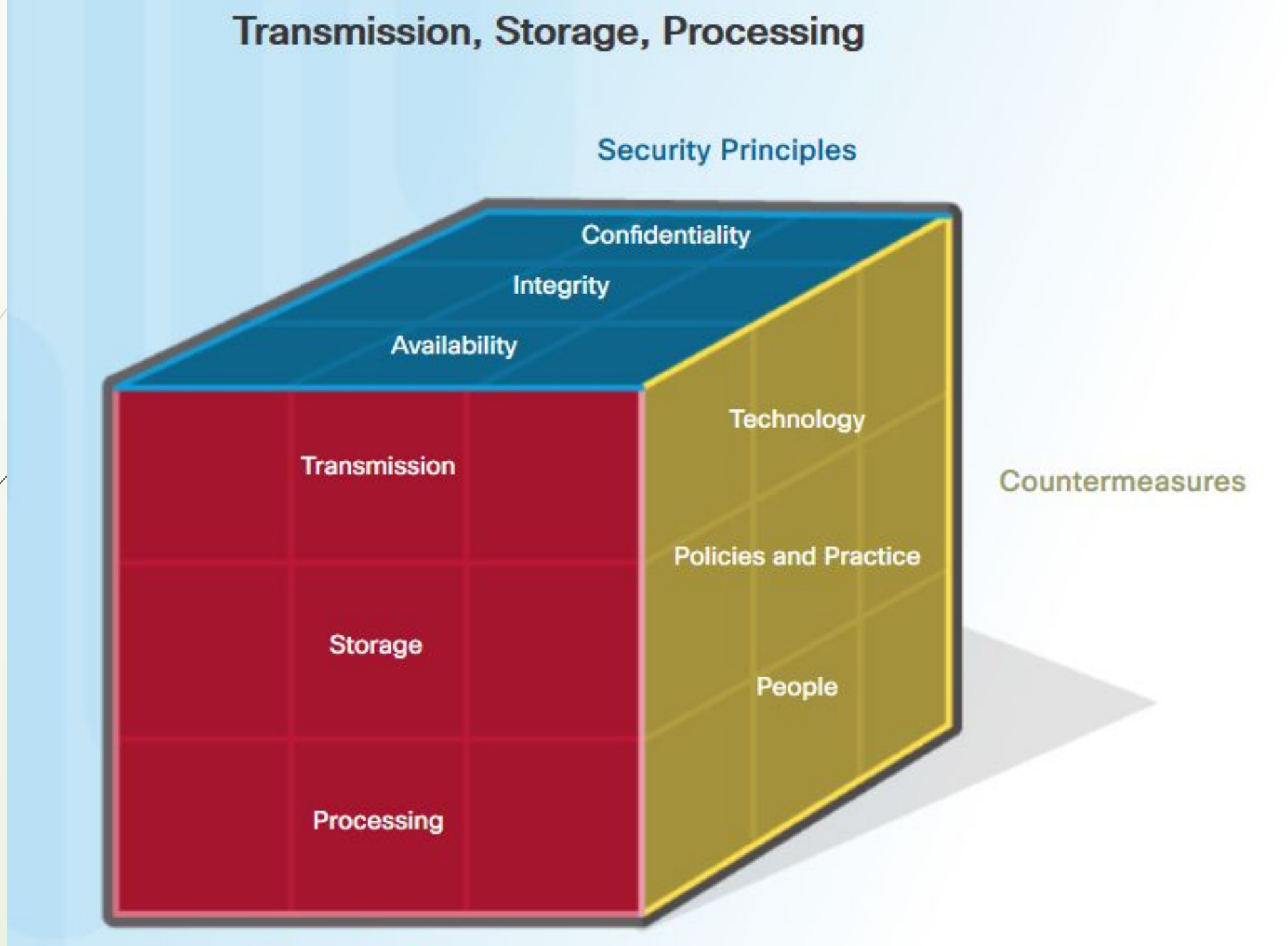
Computer Security

- protection of automated information system for preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

CIA triad

- Cybersecurity experts have developed a commonly used architecture called the "cybersecurity cube". It is often used as a tool for protecting network infrastructure, domains and the Internet. The cube of cybersecurity looks like a Rubik's cube.


Confidentiality, Integrity and Availability
Information States
Transmission
Storage
Processing
Confidentiality
Integrity
Availability
Technology
Policies and Practice
People
Countermeasures
Security Principles


Transmission, Storage, Processing
Security Principles
Confidentiality
Integrity
Availability
Transmission
Storage
Processing
Technology
Policies and Practice
People
Countermeasures

Cybersecurity Countermeasures