INFORMATION SECURITY AND DATA PROTECTION

1. **Total number of hours:** 126 hours, **credits –** 3.5
2. **Distribution of hours:** 54 hours of class study (27 hours of lectures, 27 hours of labs), 72 hours of self study works
3. **Department:** Department of Computer Engineering, Faculty of Computer Science, Irkutsk State Technical University
4. **Type:** compulsory
5. **Prerequisites:**
   - Higher mathematics
   - Fundamentals of information science and programming
   - Digital electronics
6. **Instructors**

   Person in charge: **Dr. Vladimir Glukhikh,** Associate Professor (gluxix_v@mail.ru)

   Others: (-)
7. **Hours per week:** Lectures – 2 hours per week, labs – 2 hour per week
8. **General objectives**

   Information or data that circulate in data-computing networks can be garbled, destroyed or misused. Data distortion can be either irregular, or purposeful in order to damage their owner, or protective with the aim to impede their misuse. The objective of the given course is to study main principles, methods and means of control of data reversible distortion:

   · Data generation (encoding of discrete and continuous information)

   · Reversible distortion of data (compression, noise combating encoding, encryption)

   · Data diffusion (transfer, storage)

   · Data integrity and authenticity check

   · Recovery of reversible distorted data (decoding, decryption)

   · Data use and modification

· Irrelevant data deletion

9. Specific objectives

Knowledge

1. Threat sources of data integrity
2. Threat sources of data misuse
3. Types of data distortion
4. Basic principles of information protection
5. Methods of noise combating encoding of data
6. Cryptographic methods of data protection
7. Fundamentals of data protection organization
8. Legal rules of information protection
9. Hardware-based methods of data protection

Abilities

1. To use the methods of noise combating encoding of data
2. To provide the integrity of stored and transmitted data
3. To estimate the integrity of stored and transmitted data
4. To protect stored and transmitted data from misuse

Competences

1. To organize safe functioning of information networks
2. To minimize losses due to malicious attacks on information networks
3. To generate protected data for transmission and storage in open communication channels and unguarded information networks

10. Course content

Lecture content (27 hours)

Lecture 1. INTRODUCTION (2 hours)

* Tasks and principles of information protection
* Discrete and continuous information
* Information coding

Lecture 2. Noiseproof coding (2 hours)

* Redundant codes

* Correcting Hemming codes

Lecture 3. Cyclic codes (2 hours)

* Polynomial representation of cyclic codes

* Construction of generating and check matrices of cyclic codes

* Coding and decoding devices

Lecture 4. Data acknowledgement and hashing (2 hours)

* Algorithm of CRC checksumming

* Algorithm of hash function calculation

Lecture 5. Information security (2 hours)

* Basic concepts of data security and confidentiality

* Analysis of security threats

* Standards of security

Lecture 6. Symmetric encryption methods (2 hours)

* Algorithm of block encryption DES

Lecture 7. Operation modes of symmetric encryption algorithms (2 hours)

Lecture 8. Asymmetric encryption methods (2 hours)

* Algorithm of enciphering RSA

* Algorithm of enciphering ECES

Lecture 9. Electronic digital signature (2 hours)

Lecture 10. Administration of encryption keys (2 hours)

Lecture 11. User authentication (2 hours)

Lecture 12. Anti-virus technologies (2 hours)

Lecture 13. Systems of e-payments (3 hours)

* Bank plastic cards

* E-money

Labs content (27 hours)

The labs are focused on the development and study of hardware data protection. Laboratory work is performed on specialized the laboratory benches, using the

technology in-circuit programming of programmable logical integrated circuits (PLD).

Lab 1. Hamming encoder (4 hours)

Lab 2. Pseudorandom number generator (2 hours)

Lab 3. Controller DES (4 hours)

Lab 4. CRC controller (4 hours)

Lab 5. Generator of asymmetric keys (4 hours)

Lab 6. Controller of hash functions (4 hours)

Lab 7. RSA Controller (4 hours)

Self study activities

- Studying of methods of self-correcting coding
- Studying of cryptographic methods of data protection
- Preparing to labs
- Preparing presentations and reports.
- Course paper in network area.

11. Evaluation methodology

Final grade: 0.4 * T1+ 0.4 * T2 +0.2 * T3

- T1: average grade of lab works
- T2: grade for independent researches
- T3: grade for final oral exam

12. Basic bibliography

1. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. — М.: Радио и связь, 2000. — 168 с. // Soft hardware for information security provision. Protection of programs and data: textbook for HEI / P. Yu. Belkin, O.O. Mikhalskiy, A.S. Pershakov and others. – Moscow: Radio and communication, 2000 – 168 p. (in Russian)

2. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учебное пособие для ву-

зов / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич — М.: Радио и связь, 2000. — 168 с. // Soft hardware for information security provision. Protection in operating systems: Textbook for HEI / V.G. Proskurin, S.V. Krutov, I.V. Matskevich - Moscow: Radio and communication, 2000 – 168 p. (in Russian)

3. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защиты информации в компьютерных системах. — М.: Радио и связь, 2001. — 378 с. // Romanets Yu.V., Timofeev P.A., Shangin V.F. Information protection in computer systems. – Moscow: Radio and communication, 2001 – 378 p. (in Russian)

4. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. — М.: Радио и связь, 2000. — 192 с. // Theoretical fundamentals of computer security: Textbook for HEI / Devyanin P.N., Mikhalskiy O.O., Pravikov D.I. and others. - Moscow: Radio and communication, 2000 – 192 p. (in Russian)

5. Чижухин Г. Н. Основы защиты информации в вычислительных системах и сетях ЭВМ: Учебное пособие. — Пенза: Изд-во Пенз. гос. ун-та, 2001. — 164 с. // Chizhukhin G.N. Fundamentals of information protection in computing systems and networks: Textbook. – Pensa: Publishing House of Pensa State University, 2001. – 164 p. (in Russian)

6. Хоффман Л. Дж. Современные методы защиты информации / Пер. с англ. – М.: Советское радио, 1980. — 268 с. // Hoffman L.J. Up-to-date methods of information protection. Translation from English. – Moscow: Soviet radio, 1980. – 268 p. (in Russian)

13. Complementary bibliography

1. Мещеряков Р. В., Шелупанов А. А., Белов Е. Б., Лось В. П. Основы информационной безопасности. — М.: Горячая линия-Телеком, 2006.— 540 с. // Mesheryakov R.V., Shelupanov A.A., Belov E.B., Los’ V.P. Fundamentals of information security. – Moscow: Hotline-Telecom, 2006. – 540 p. (in Russian)

2. Партыка Т. Л., Попов И. И. Информационная безопасность. — М.:: ФОРУМ: ИНФРА-М, 2002 — 368 с. // Partyka T.L., Popov I.I. Information security. – Moscow: FORUM: INFRA-M, 2002 – 368 p. (in Russian)

3. Самосук М. Компьютерное пиратство / Защита программного обеспечения. Под ред. Гроубера. - М.: Мир, 1992 // Samosuk M. Computer piracy / Software protection. Under edition of Grouber. – Moscow: Mir, 1992. (in Russian)

4. Семкин С. Н., Семкин А. Н. Основы информационной безопасности объектов обработки информации. Научно-практическое пособие. — Орел: Труд, 2000. — 300 с. // Semkin S.N., Semkin A.N. Fundamentals of information security of objects of information handling. Scientific and practical manual. – Orel: Trud, 2000. – 300 p. (in Russian)

5. Shneider B. Applied cryptography, 2nd Edition, John & Sons, 1996/ (Шнайдер Б. Прикладная криптография. – М.: Мир, 1999) (in Russian)

6. Trusted Computer System Evaluation Criteria. US Department of Defense 5200.28-STD, 1993. (in English)

14. Web links

- Portal with resources in the area of cryptography
  http://www.cryptography.ru

- Purdue University web-site
  http://ftp.cerias.purdue.edu/pub

- Web-site of National Institute of Standardization and Technologies, Department of information security. Collection of standards and publications of NIST in the area of information security.
  http://csrc.nist.gov

- Standards and publications of BSI community
  http://www.bsi.de/english/index.htm

- Information letter JetInfo. Publications and standards in the area of information security
  http://www.jetinfo.ru

- Mailing list on conferences on information security
  http://www.securityfocus.com

- Up-to-date papers on information security
  http://www.bugtrack.ru

- Strategic security and smart tools
  http://www.all.net

- Russian version of the web-site of “Aladdin” company, the producer of hardware for protection of software and commercial information (electronic keys HASP, identifier e-Token and others).
  http://www.aladdin.ru

- Web-site of the company “Informzashita” (Information security)
  http://www.infosec.ru