**SYLLABUS**

**Fall semester 2021-2022 academic years**

**on the educational program “Information Security Systems (6B06301)”**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Discipline’s code** | **Discipline’s title** | **Independentwork of students (IWS)** | **No. of hours per week** | | | | | **Number of credits** | **Independent work of student with teacher (IWST)** |
| **Lectures (L)** | **Practicaltraining (PT)** | | **Laboratory (Lab)** | |
| TSB3223  TSB3306 | Technical Security | 98 | 15 | 0 | | 30 | | 5 | 6 |
| **Academic course information** | | | | | | | | | |
| **Form of education** | **Type of course** | **Types of lectures** | | | **Types of practical training** | | **Number of IWS** | | **Form of final control** |
| Online/offline | theoretical, practical | subject-oriented, analytical | | | situational tasks | | 3 | | Oral |
| Lecturer | Mukhitova Aigul Aripovna | | | | | | Scheduled | | |
| e-mail | mukhitova.aigul@gmail.com | | | | | |
| Telephone number | +77012280248 | | | | | |

|  |
| --- |
| **Academic presentation of the course** |

|  |  |  |
| --- | --- | --- |
| **Aim of course** | **Expected Learning Outcomes (LO)**  As a result of studying the discipline the undergraduate will be able to: | **Indicators of LO achievement (ID)**  (for each LO at least 2 indicators) |
| Analysis of threat models of unauthorized use of information resources requiring software and hardware to protect information.  Acquaintance with the methods and tools of information protection (IP) in detection mechanisms (OS), database management systems (DBMS) and CS, their practical application.  Overview of integrated solutions that implement modern IS technologies in IS based on specialized software products and certified technical means of information protection (TMIP). | LО 1 The ability to improve and develop one's intellectual and general cultural level | ID 1.1 Knowledge of the conditions for the creation and operation of software and hardware for ensuring information security of information systems.  ID 1.2 Knowledge of the main trends in the development of the market for hardware and software for information security of information systems.  ID 1.3 The ability to analyze the IPS available on the market, using cryptographic technologies, in order to determine the TSIS complex for a given IS, taking into account the threat model and IS requirements.  ID 1.4 Ability to apply software and hardware to ensure information security in various projects. work with software and technical documentation on TMIP. |
| LO 2 Possession of methods and means of obtaining, storing, processing and broadcasting information through modern computer technologies, including global computer networks | ID 1.1 Knowledge of the conditions for the creation and operation of software and hardware for ensuring information security of IS.  ID 1.2 Understanding the main trends in the development of the market for software and hardware to ensure information security of information systems.  ID 1.3 Ability to analyze hardware and software for information security. |
| LO 3 The ability to understand the essence and significance of information in the development of modern society, to be aware of the dangers and threats that arise in this process, to comply with the basic requirements of information security, including the protection of state secrets | ID 1.1 Knowledge of the basics of information and bibliographic culture; basic information security requirements.  ID 1.2 Ability to work with information in global computer networks, taking into account the basic requirements of information security, to work with traditional media. |
| LO 4 The ability to take into account modern trends in the development of electronics, measuring and computer technology, information technology in their professional activities | ID 1.1 Skills for searching, storing, processing and analyzing information from various sources and databases.  ID 1.2 Knowledge of the basics of building computer networks and the protocols used; basic concepts of information systems and databases; basic data representation models, composition and main functions of database management systems. |
| LO 5 Ability to use computer skills, knowledge of information technology methods, to comply with the basic requirements of information security. | ID 1.1 Skills for using the achievements of modern information technologies, measuring and computing equipment for solving professional problems.  ID 1.2 Knowledge of current trends in the development of electronics, measuring and computer technology, information technology.  ID 1.3 Skills to analyze current trends in the development of electronics, measuring and computing equipment, information technology |
| **Prerequisites** | Data protection | |
| **Post requisites** | Security of intelligent systems | |
| **Information resources** | 1. Proskurin VG Hardware and software for information security. Protection in operating systems: textbook. manual for universities / V. G. Proskurin, S. V. Krutov, I. V. Matskevich. - M.: Radio and communication, 2000. - 168 p. : ill.  2. Zaitsev, A.P. Technical means and methods of information protection: Textbook for universities / A.P. Zaitsev, R.V. Meshcheryakov, A.A. Shelupanov. - M.: RiS, 2014. - 442 p.  Meshcheryakov, R.V. Technical means and methods of information protection: Textbook for universities / A.P. Zaitsev, A.A. Shelupanov, R.V. Meshcheryakov; Ed. A.P. Zaitsev. - M.: Gor. line-Telecom, 2012. - 442 p.  3. Fefilov, A.D. Methods and means of protecting information in networks / A.D. Fefilov. -M. : Book laboratory, 2011. - 105 p. : ill., tab. - ISBN 978-5-504-00608-6; [Electronic resource]. - URL: http://biblioclub.ru/index.php?page=book&id=140796  4. Software and hardware protection of computer information. Practical course: textbook / E. I. Dukhan, N. I. Sinadsky, D. A. Khorkov; Yekaterinburg: Ural State University, 2008.  URL: http://elar.urfu.ru/bitstream/10995/1403/5/1331981\_schoolbook.pdf  **Software:**  1. Acronis Backup & Recovery 11.5  2. Secret Net 6.5  3. DeviceLock 7.  4. ViPNet Custom 3.1.  5. XSpider 7.8.  **Internet resources:**  1.https://www.anti-malware.ru/security/ids-ips  2. https://www.techopedia.com/definition/31429/technical-security-techsec  2. http://www.securitylab.ru/  3. http://comp-bez.ru/ | |

|  |  |
| --- | --- |
| **Academic policy of the course in the context of university moral and ethical values** | **AcademicBehaviorRules:**  All students have to register at the MOOC. The deadlines for completing the modules of the online course must be strictly observed in accordance with the discipline study schedule.  ATTENTION! Non-compliance with deadlines leads to loss of points! The deadline of each task is indicated in the calendar (schedule) of implementation of the content of the curriculum, as well as in the MOOC.  **Academicvalues:**  - Practical trainings/laboratories, IWS should be independent, creative.  - Plagiarism, forgery, cheating at all stages of control are unacceptable.  - Students with disabilities can receive counseling at e-mail mukhitova.aigul@gmail.com. |
| **Evaluation and attestation policy** | **Criteria-basedevaluation:**  assessment of learning outcomes in relation to descriptors (verification of the formation of competencies in midterm control and exams).  **Summativeevaluation:** assessment of work activity in an audience (at a webinar); assessment of the completed task. |

**CALENDAR (SCHEDULE) THE IMPLEMENTATION OF THE COURSE CONTENT:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| weeks | | Topic name | | LO | | ID | Amount of hours | Maximum score | | Form of Knowledge Assessment | | | The  Form of the lesson  / platform |
| Module **1** | | | | | | | | | | | | | | |
| 1 | **L.1** Basic concepts terms and definitions in the field of technical protection of information (TPI). The place of TPI in the system of measures to ensure information security in the Republic of Kazakhstan. Goals and objectives of the TPI. | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | Video lecture  in MS Teams | | |
| 1 | **Lab 1** Computer system and information protection. Types of technical intelligence. | | LО 1 | | ID 1.1. | | 2 | | 10 | | discussion /consolida  tion | Webinar  in MS Teams | | |
| 2 | **L.2** Protected information and information resources. Information security objects. Informatization objects, their classification and characteristics. | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | Video lecture  in MS Teams | | |
| 2 | **Lab 2** Protection mechanisms implemented in software and hardware information security facilities from NSD: access control; registration and control of critical events; data integrity control; cryptographic protection; examples of means of protecting information from unauthorized access. | | LО 1 | | ID 1.1. | | 2 | | 10 | | Analysis | Webinar  in MS Teams | | |
| 3 | **L.3** Threats to the security of restricted access information. Programmatic and mathematical influence. Malicious programs and their classification | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 3 | **Lab 3** Determination of unmasking signs of objects. | | LО 1 | | ID 1.1. | | 2 | | 10 | | discussion /consolida  tion | offline | | |
| 3 | **IWST 1** Consultation on the implementation of IWS1.  **IWS 1.** Protected information and information resources | | LО 1  LО 2 | | ID 1.1. | |  | | 20 | | CW | offline | | |
| 4 | **L 4** Technical channels of information leakage | | LО 2 | | ID 1.2. | | 1 | | 0 | | QS | offline | | |
| 4 | **Lab 4** Identification of technical channels of leakage information for premises and technical  funds | | LО 2 | | ID 1.3. | | 2 | | 10 | | discussion /consolida  tion | offline | | |
| 5 | **L 5** Information security threat model. Methods for identifying and analyzing information security threats and software vulnerabilities | | LО 2 | | ID 1.3. | | 1 | | 0 | | QS | offline | | |
| 5 | **Lab 5** Classification of devices for unauthorized retrieval of information | | LО 2 | | ID 1.3. | | 2 | | 10 | | discussion /consolida  tion | offline | | |
| 5 | **IWST 2. IWS 1** acception | | LО 2 | | ID 1.3. | |  | | 30 | | report/presentatiom |  | | |
|  | **MT 1** | |  | |  | |  | | 100 | |  |  | | |
| **Module П** | | | | | | | | | | | | | | |
| 6 | **L 6** Data bank information security threats, data access software vulnerabilities. International Approach to Vulnerability Identification and Analysis: CVE and CVS | | LО 3 | | ID 3.1. | | 1 | | 0 | | QS | offline | | |
| 6 | **Lab 6** Overview of embed detection tools  devices | | LО 1 | | ID 1.1. | | 2 | | 10 | | discussion /consolida  tion | offline | | |
| 7 | **L.7** Legal basis for information protection | | LО 4 | | ID 4.1. | | 1 | | 0 | | QS | offline | | |
| 7 | **Lab 7** Overview of embed detection tools  devices | | LО 1 | | ID 1.1. | | 2 | | 10 | |  | offline | | |
| 7 | **IWST 3** Consultation on the implementation of **IWS2.**  **IWS2.** Legal basis for information protection | | LО 1  LО 4 | | ID 1.1.  ID 4.1. | |  | | 20 | | CW | offline | | |
| 8 | **L 8** Licensing of activities in the field of information protection. Responsibility for offenses in the field of information protection | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 8 | **Lab 8** The practice of conducting search  events | | LО 1 | | ID 1.1. | | 2 | | 10 | | TK | offline | | |
| 9 | **L 9**  TMP work planning  Requirements for the protection of information and the creation of an information protection system | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 9 | **Lab 9** The choice of methodology for conducting an event for information protection | | LО 1 | | ID 1.1. | | 2 | | 10 | | Analysis | offline | | |
| 10 | **L 10** A set of works to create an information security system | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 10 | **Lab 10** Sound absorption methods, soundproofing, shielding, filtering and limiting, jamming and noise | | LО 5 | | ID 5.1. | | 2 | | 10 | | discussion /consolida  tion | offline | | |
| 10 | **IWST 4** IWS2 acception | | LО 1 | | ID 1.1. | |  | | 30 | | report/presentatiom | offline | | |
|  | **МТ (MidtermExam)** | |  | |  | |  | | 100 | |  |  | | |
| 11 | **L 11** Organizational bases for the implementation of TSP activities | | LО 3 | | ID 3.1. | | 1 | | 0 | | QS | offline | | |
| 11 | **Lab 11** Passive and active protection methods  information | | LО 1 | | ID 1.1. | | 2 | | 10 | | TK | offline | | |
| 12 | **L 12** Measures and means of technical protection of confidential information from leakage through technical channels of information leakage | | LО 3 | | ID 3.2. | | 1 | | 0 | | QS | offline | | |
| 12 | **Lab 12** Used for soundproofing  soundproofing and shielding materials,  filters and limiters | | LО 1 | | ID 1.1. | | 2 | | 10 | | TK | offline | | |
| 12 | **IWST 5** Consultation on the implementation of IWS3. **IWS 3** Make organizational bases for the implementation of TSP activities | | LО 5 | | ID 5.1. | |  | | 20 | | TK | offline | | |
| 13 | **L 13** Means of active protection of premises against speech information leaks | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 13 | **Lab 13** Acoustic and vibration generators  noise, voice recorder suppressors | | LО 4 | | ID 4.1. | | 2 | | 10 | | TK | offline | | |
| 14 | **L 14** Means of active protection of premises against. Leaks of information through electromagnetic channels | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 14 | **Lab 14** Linear and spatial generators  noise, suppressors and directors  interference | | LО 4 | | ID 4.2. | | 2 | | 10 | | TK | offline | | |
| 15 | **L 15** Information security certification | | LО 1 | | ID 1.1. | | 1 | | 0 | | QS | offline | | |
| 15 | **Lab 15** Access control and management systems,  application of engineering solutions | | LО 1 | | ID 1.1. | | 2 | | 10 | | TK | offline | | |
| 15 | **IWST 6** IWS3 acception | | LО 5 | | ID 5.2. | |  | | 30 | | report/presentatiom | offline | | |
|  | **MT 2** | |  | |  | |  | | 100 | |  |  | | |

[Abbreviations: QS - questions for self-examination; TK - typical tasks; IT - individual tasks; CW - control work; MT - midterm.

Chairman of the Methodological Council Gusmanova F.R.

Head of the Department Musiralieva Sh. Zh.

Lecturer Mukhitova A.A.