**SYLLABUS**

**Fall semester 2022-2023 academic years**

**on the educational program “Radio engineering, electronics and telecommunications”**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Discipline’s code** | **Discipline’s title** | **Independent work of students (IWS)** | **Number of credits** | **Number of credits** | **Independent work of student with teacher (IWST)** |
| **Lectures (L)** | **Practical training (PT)** | **Laboratory (Lab)** |
| 8B722 | Information security in telecommunications | 98 | 15 | - | 30 | 5 | 7 |
| **Academic course information** |
| **Form of education** | **Type of course**  | **Types of lectures** | **Types of practical training**  | **Form of final control**Writing |
| The lecture is offline.Practical lesson - offline | Theoretical | Problematic, analytical | Problrm solving, writing codes |
| Lecturer  | Turlykozhayeva Dana Abdikumarovna | Writing |
| e-mail | Abdikumarovna.d@gmail.com |
| Telephone number | 87472666916 |

|  |  |  |
| --- | --- | --- |
| **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) |
| Learn the basic principles of network security and monitoring | 1. List the main concepts and definitions related to information security, the main concepts of public key infrastructure; principles of creating a secure IT infrastructure, basic tunneling technologies of application and network levels, classification of firewalls, classification of intrusion detection and prevention systems; | 1.1 Classification of threats to telecommunication systems, services and security mechanisms;1.2 knowledge of information exchange protocols at the network level; 1.3 To know the legislative and regulatory framework of the Republic of Kazakhstan in the field of information security. |
| 2. Using basic symmetric and asymmetric encryption algorithms, cryptographic hash functions, and message authentication methods; | 2.1 Use tabular methods to encode secret text information;2.2 Be able to solve some problems of number theory used in cryptography;2.3 Use of classic cryptographic methods of encoding secret information: symmetric and asymmetric encryption. |
| 3. Distinguish between firewall policies and intrusion detection systems; | 3.1 Knowledge of digital security certificates and the possibilities of their application;3.2 Reading the penetration detection system (IDS) tools. |
| 4. Prioritize network security solutions that address multiple threats across networks. | 4.1 Knowledge of cryptanalysis methods and the need for cryptanalysis; Knowledge of cryptographic hash functions;4.2 Application of cryptanalysis methods of classical and modern algorithms of information protection. |
| 5. Ability to analyze basic encryption types | 5.1 To know the basic the main goals and objectives of ensuring security in telecommunication systems5.2 To know the features of the use of cryptographic methods5.3 To understand the construction of simple antennas |
| **Prerequisites** | IKT2104 Information and Communication Technologies,M1202 Mathematics, ORT2212 Fundamentals of Radio Engineering and Telecommunications, TCS3218 Digital Communication Technology |
| **Post requisites** | Graduate work |
| **Information resources**  | **Literature:**1. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов.- М.: Академия, 2005.- 254, [2] с.
2. Молдовян, А. А. и др. Криптография: Учеб..- СПб.: Лань, 2001.- 218, [6] с.
3. Нечаев, В.И. Элементы криптографии: (Основы теории защиты информации).- М.: Высш. шк., 1999.- 108, [1] с
4. Беляев А.В. Курс лекций по «Методы и средства защиты информации». <http://citforum.ru/internet/infsecure/index.shtml>
5. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000..
6. Домарев, В.В. Защита информации и безопасность компьютерных систем /.- Науч.-попул. изд.- Киев: СОФТ, 1999.- 453, [26] с
7. Галочкин, А.И. Введение в теорию чисел: Учеб. пособие - 2-е изд.- М.: МГУ, 1995.- 158, [2] c

**Онлайн қолжетімді:** Үй тапсырмасы мен СӨЖ бойынша қосымша оқу материалы univer.kaznu.kz сайтындағы UMKD бөлімінде парақшаңызда қолжетімді болады.**Интернет-ресурстар**<https://refdb.ru/look/1214614.html> - «Ақпараттық қауіпсіздік негіздері» тақырыбындағы дәрістер<http://www.4stud.info/networking/network-security.html> Желі қауіпсіздігінің негіздері. Желі қорғау объектісі ретінде<https://www.fortinet.com/ru/solutions/enterprise-midsize-business/network-security> - Желінің қауіпсіздігін анықтау және түсіндіру<https://www.owasp.org/index.php/Main_Page> - осалдықтардың деректер базасы.<https://intuit.ru/studies/courses/102/102/lecture/2971> - INTUIT желілік қауіпсіздік бойынша дәрістер |
|  |  |

|  |  |
| --- | --- |
| **Academic policy of the course in the context of university moral and ethical values** | **Academic Behavior Rules:** All students are required to register for the MOOC. The deadlines for completing the modules of the online course must be strictly observed in accordance with the schedule for studying the discipline. Leave in case of current MOOC or SPOC courses. f points! The deadline for each task is indicated in the calendar (schedule) for the implementation of the **ATTENTION!** Failure to meet deadlines results in loss o content of the training course, as well as in the MOOC. Leave in case of current MOOC or SPOC courses.**Academic values:**- 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 Abdikumarovna.d@gmail.com |
| **Evaluation and attestation policy** | **Criteria-based evaluation:** assessment of learning outcomes in relation to descriptors (verification of the formation of competencies in midterm control and exams).**Summative evaluation:** assessment of work activity in an audience (at a webinar); assessment of the completed task.Below are the minimum grades by percentage:95% - 100%: А 90% - 94%: А-85% - 89%: В+ 80% - 84%: В 75% - 79%: В-70% - 74%: С+ 65% - 69%: С 60% - 64%: С-55% - 59%: D+ 50% - 54%: D- 0% -49%: F  |

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

|  |  |  |  |
| --- | --- | --- | --- |
| week | Topic name | Number of hours | Max.score |
| **Module 1**  |
| 1 | **Lec 1.** A general understanding of information security, a brief history of its development. The main components of information security. | 1 |  |
| 1 | **Sem 1.** Modern standards of information security | 1 | 15 |
| 1 | **Lab 1.** Implementation of the Caesar Cipher in Python | 2 | 5 |
| 2 | **Lec 2.** Security threats. Classification of hazards. | 1 |  |
| 2 | **Sem 2.** Encryption tables. Displacement ciphers. Double replacement. | 1 | 15 |
| 2 | **Lab 2.** Implementation of the Vigener cipher in Python | 2 | 5 |
| 2 | **IWST 1.** SIW consultation Caesar Cipher |  |  |
| 3 | **Lec 3.** Services and security mechanisms. Network-level information exchange protocols. | 1 |  |
| 3 | **Sem 3.** Trisemus encryption tables. Vigenere encryption system | 1 | 10 |
| 3 | **Lab 3.** Implementation of the substitution cipher in Python | 2 | 5 |
| 3 | **SIW 1.** Topic "basic principles of building a reliable and secure IT infrastructure"(form: oral: answer questions) |  | 20 |
| 4 | **Lec 4.** Classification of network attacks. Categories of attacks and their definitions, conditions for their implementation. Attack mechanism. | 1 |  |
| 4 | **Sem 4.** Double Wheatstone square. Playfair bigram cipher. | 1 | 20 |
| 4 | **Lab 4.** Implementation of Homophonic cipher in Python | 2 | 5 |
|  | **IWST 2.** Legislative measures of protection in the Republic of Kazakhstan.\* Law of the Republic of Kazakhstan on information\*Law of the Republic of Kazakhstan on State Secrets\* Law of the Republic of Kazakhstan on Communication. (Form: writing an abstract) |  |  |
| 5 | **Lec 5.** Cryptographic security mechanisms. The main tasks and concepts of cryptography. Principles of cryptographic information protection. | 1 |  |
| 5 | **Sem 5.** Elements of number theory. GCD and comparison (case study method). Fermat and Euler's theorems for solving cryptographic problems. | 1 | 20 |
| 5 | **Lab 5.** Implementation of the RSA cipher in Python | 2 | 5` |
| **Module 2**  |
| 6 | **Lec 6.** Symmetric and asymmetric encryption in information security problems. | 1 |  |
| 6 | **Sem 6.** A cryptosystem without key transfer. Solving problems in a cryptosystem without key transfer | 1 | 15 |
| 6 | **Lab 6.** Implementation of Substitution Cipher and tabular gamming in Python | 2 | 5 |
| 7 | **Lec 7.** The principle of creation of public key encryption systems | 1 |  |
| 7 | **Sem 7.** RSA Public-key information security algorithm | 1 | 20 |
| 7 | **Lab 7.** Hacking Caesar Cipher with a Key | 2 | 5 |
| 7 | **IWST 3.** Security certificates. Types of security certificates. |  |  |
|  |  **LEVEL CONTROL 1** |  | **100** |
| 8 | **Lec 8.** Hash functions | 1 |  |
| 8 | **Sem 8.** Digital signature algorithms. | 1 | 10 |
| 8 | **Lab 8.** Creating a key from a password in Python | 2 | 5 |
| 8 | **IWS 2.** Reflection coefficients S11 and VSWR core wave |  |  |
| 9 | **Lec 9.** Segmentation of networks at the channel level. Using VLAN technology to create subnets. A typical network topology that uses a VLAN network. | 1 |  |
| 9 | **Sem 9.** Digital signature algorithms. | 1 | 15 |
| 9 | **Lab 9.** Encrypting and decrypting files using Python | 2 | 5 |
| 10 | **Lec 10.** Port-based VLAN networks | 1 |  |
| 10 | **Sem 10.** IEEE 802.1 standard | 1 | 20 |
| 10 | **Lab 10.** Pair cipher in Python | 2 | 5 |
| 10 | **IWST 4.** Digital signature algorithms. |  | 5 |
|  | **Module 3**  |  |  |
| 11 | **Lec 11** Brandmauer technologies. Basic concepts of network technologies (protocol stack, TCP connection States).Brandmauer classification | 1 |  |
| 11 | **Sem 11.** Brandmauer management basics. | 1 | 18 |
| 11 | **Lab 11.** Symmetric encryption in Python | 2 | 5 |
| 12 | **Lec 12.** Tunnel technologies. Communication level protocols. IPSec protocol family. | 1 |  |
| 12 | **Sem 12.** GRE Protocol | 1 | 17 |
| 12 | **Lab 12.** Asymmetric encryption in Python | 2 | 5 |
| 12 | **IWST 5.** Asymmetric encryption in Python |  |  |
| 13 | **Lec 13.**  SSL/TLS protocol. | 1 |  |
| 13 | **Sem 13.** SIEM: IBM QRadar, McAfee ESM, Cisco MARS systems analysis | 1 | 15 |
| 13 | **Lab 13.** Matrix encryption in Python | 2 | 5 |
| 13 | **IWS 3.** Matrix encryption in Python |  |  |
| 14 | **Lec 14** Intrusion detection and prevention systems (IDPS). The main purpose of the IDPS. IDPS classification methods | 1 |  |
| 14 | **Sem 14.** Intrusion detection and prevention systems (IDPS).Anti-virus scanning. | 1 | 10 |
| 14 | **Lab 14.** Encryption levels in Python | 2 | 5 |
|  | **IWST 6.** Encryption levels in Python |  |  |
| 15 | **Lec 15.** Priority of movement and creation of alternative routes. Creating alternative internet access routes | 1 |  |
| 15 | **Sem 15.** Generating traffic using IDP | 1 | 10 |
| 15 | **Lab 15.** Transpose cipher in Python | 2 | 5 |
| 15 | **IWST 7.** Transpose cipher in Python |  |  |
|  |  LEVEL CONTROL 2 |  | **100** |

Dean \_ Beisen N. A.\_\_

Head of Department \_Ibraimov M. K.\_\_

Lecturer \_Turlykozhayeva D. A.\_\_

.