**Final exam program for the course «Technical Security»**

**for the 2021-2022 academic year**

**Faculty** *Information Technology*

**Department** *Information Systems*

**Code and name of the educational program***: 6B06301-Information Security Systems*

**Discipline name:** *Technical Security*

***Course*** \_\_\_\_3\_\_\_\_

**Lecturer: \_***Mukhitova Aigul Aripovna***\_ \_\_\_\_\_\_\_\_**

**The form of the final control** on a subject: in writing: traditional - question, answer. The exam form is synchronous, offline

The exam will take place in the classroom specified in the prepared exam schedule.

Duration - 2 hours.

EXAM PROCEDURE

- The student must arrive 20 minutes before the time indicated in the exam schedule.

- Students who are late for the exam are not allowed to take the exam.

- Take your passport, pen and pencil with you.

- have a mask in accordance with sanitary standards.

- Do not use smartphones, calculators, dictionaries and other additional materials during the exam and do not talk with other students. In case of violation of these warnings, an act is drawn up and the student is suspended from the exam. And the examination sheet for the subject has a mark "F" (unsatisfactory).

Student actions during the exam

- 15 minutes before the start of the exam, the teachers on duty land the students indicated in the sheet, sign the sheet confirming that they are familiar with the place

- after answering the questions of the exam ticket (within 2 hours), the student hands over his work to the teacher on duty. Entries will not be accepted after 2 hours.

**Topics for which the exam questions were drawn up (program)**

1. Protected information and information resources

2. Objects of information protection

3. Determination of threats to the security of restricted information

4. Programmatic and mathematical influence. Malicious programs and their classification

5. Technical channels of information leakage

6. Model of information security threats. Methods for identifying and analyzing information security threats and software vulnerabilities

7. Data bank of information security threats, including a database of software vulnerabilities. International Approach to Vulnerability Identification and Analysis: CVE and CVSS

8. Legal basis for information protection

9. Licensing of activities in the field of information protection. Responsibility for offenses in the field of information protection

10. Security and fire alarm

11. Means and systems of communication

12. TV security systems

13. Technical support of other types of security

14 Integrated security systems

15. Requirements for the protection of information and the creation of an information protection system

16. A set of works to create an information security system

17. Organizational bases for the implementation of activities for TCDI

18. Measures and means of technical protection of confidential information from leakage through technical channels of information leakage

19. Protection of information from unauthorized access

20. Programs and methods of certification tests.

21. Protection of information when working with database management systems.

22. Features of the implementation of information protection requirements in the interaction of subscribers with public information networks.

23. Basic measures to protect information from leakage through technical channels. Organizational protection measures: temporary restrictions, territorial restrictions.

24. Ways and means of protecting informatization objects from information leakage through technical channels when it is processed using technical means.

25. Features of the implementation of measures to protect personal data.

26. General procedure for certification of information security tools.

27. Methods and means of controlling the security of information processed by technical means.

28. Methods and means of monitoring the protection of acoustic speech information from leakage through technical channels

29. Methods and means of controlling the security of information from unauthorized access.

30. General characteristics and classification of measures and means of protecting information from unauthorized access

**LIST OF RECOMMENDED LITERATURE**

1. Information technology security. Criteria for assessing the security of information technology: RD: approved. State Technical Commission of Russia. - M., 2002.

2. Automated systems. Protection from unauthorized access to information. Classification of automated systems and information security requirements: RD: approved. State Technical Commission of Russia. - M .: Publishing house of standards, 1992.

3. Computer equipment. Protection from unauthorized access to information. Indicators of security from unauthorized access to information: RD: approved. State Technical Commission of Russia. - M .: Publishing house of standards, 1992.

4. Protection against unauthorized access to information. Terms and definitions: RD: approved. State Technical Commission of Russia. - M .: Publishing house of standards, 1992.

8. GOST R 15408–02. Criteria for evaluating information technology security. - Input. 2004-01-01 - M .: Publishing house of standards, 2002.

5. ISO/IEC 17799:2000. Information Technology. Code of Practice for Information Security Management. International Standard / ISO/IEC, 2000.

6. Zegzhda D. P. How to build a secure information system. Technology for creating safe systems / D. P. Zegzhda, A. M. Ivashko; under scientific ed. P. D. Zegzhdy, V. V. Platonova. - St. Petersburg: Mir and Family-95, Interline, 1998. - 256 p. : ill. ; 20 cm - 500 copies.

7. Devyanin P. N. Theoretical foundations of computer security: textbook. manual for universities / P. N. Devyanin, O. O. Mikhalsky, D. I. Pravikov, A. Yu. Shcherbakov. - M.: Radio and communication, 2000. - 192 p. : ill. ; 21 cm

8. Microsoft Windows NT Workstation 4.0 resources: [trans. from English] / Microsoft Corporation. - St. Petersburg. : BHV - St. Petersburg, 1998. - 800 p. : ill. ; 28 cm. + 1 electron. opt. disk. – Translated edition: Microsoft Windows NT Workstation 4.0 Resource Kit / Microsoft Corporation, 1996.

9. 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.

Assessment criteria (Assessment scale):

|  |  |  |  |
| --- | --- | --- | --- |
| «Excellent» - | А | 4,0 | 95-100 |
| А- | 3,67 | 90-94 |
| «Good» -  | В+ | 3,33 | 85-89 |
| В | 3,0 | 80-84 |
| В- | 2,67 | 75-79 |
| С+ | 2,33 | 70-74 |
| «Satisfactory» -  | С | 2,0 | 65-69 |
| С- | 1,67 | 60-64 |
| D+ | 1,33 | 55-59 |
| D- | 1,0 | 50-54 |
| «Failure» -  | FX | 0,5 | 25-49 |
| F | 0 | 0-24 |