Federal State Autonomous Educational Institution of Higher Education
Peoples' Friendship University of Russia named after Patrice Lumumba

Academy of Engineering

(name of the main educational unit (MEU) that developed the educational program of higher education)

WORKING PROGRAM OF THE DISCIPLINE

TECHNOLOGY THREATS AND CYBERSECURITY SYSTEMS

(name of discipline/module)

Recommended for the field of study/specialty:

27.04.04 CONTROL IN TECHNICAL SYSTEMS

(code and name of the field of study/specialty)

The discipline is mastered within the framework of the implementation of the main professional educational program of higher education (EP HE):

Artificial Intelligence, Machine Learning, and Space Science

(name (profile/specialization) of the educational institution of higher education)

2026

1. THE GOAL OF MASTERING THE DISCIPLINE

The course "Technology Threats and Cybersecurity Systems" is part of the Master's program "Artificial Intelligence, Machine Learning, and Space Sciences" in the 27.04.04 "Control in Technical Systems" program and is studied in the third semester of the second year. The course is offered by the Department of Mechanics and Control Processes. It consists of four sections and nine topics and focuses on the fundamental principles of information security threat models for computer systems and assessing their impact on information security risks. It also examines key methods for solving typical problems and introduces their application in professional activities.

The purpose of mastering this course is to develop fundamental knowledge and skills in applying problem-solving methods necessary for professional activity, and to improve the overall level of digital literacy among students.

2. REQUIREMENTS FOR THE RESULTS OF MASTERING THE DISCIPLINE

Mastering the course "Technological Threats and Cybersecurity Systems" aimed at developing the following competencies (parts of competencies) in students:

Table 2.1. List of competencies developed in students while mastering the discipline (results of mastering the discipline)

Cipher	Competence	Indicators of Competency Achievement (within this discipline)
GPC-10	Capable of managing the development of methodological and regulatory documents, technical documentation in the field of automation of technological processes and production, including on the life cycle of products and their quality	GPC-10.1 Familiar with the basic approaches to the development of methodological and regulatory documents, technical documentation in the field of automation of technological processes and production; GPC-10.2 Has a command of approaches to managing the development of technical documentation and regulatory documents in the field of automation of technological processes and production, including the life cycle of products and their quality;
GPC-6	Capable of collecting and analyzing scientific and technical information, generalizing domestic and foreign experience in the field of automation and control equipment	GPC-6.1 Knows the basic methods of collecting and analyzing scientific and technical information; GPC-6.2 Able to analyze and generalize domestic and foreign experience in the field of automation and control equipment; GPC-6.3 Has knowledge of methods for collecting and analyzing scientific and technical information, and can also generalize domestic and foreign experience in the professional field;

3. PLACE OF THE DISCIPLINE IN THE STRUCTURE OF THE EDUCATIONAL EDUCATIONAL INSTITUTION

Course "Technological Threats and Cybersecurity Systems" refers to the mandatory part of block 1 “Disciplines (modules)” of the educational program of higher education.

As part of the higher education program, students also master other disciplines and/or practices that contribute to the achievement of the planned results of mastering the discipline "Technological Threats and Cybersecurity Systems."

Table 3.1. List of components of the educational program of higher education that contribute to the achievement of the planned results of mastering the discipline

Cipher	Name of competence	Previous courses/modules, practical training*	Subsequent disciplines/modules, practices*
GPC-6	Capable of collecting and analyzing scientific and technical information, generalizing domestic and foreign experience in the field of automation and control equipment	Research work / Scientific research work (acquiring primary skills in scientific research work); Relational Database Management System; Python for Data Science; Inferential Statistics;	Undergraduate practice / Pre-graduation practice;
GPC-10	Capable of managing the development of methodological and regulatory documents, technical documentation in the field of automation of technological processes and production, including on the life cycle of products and their quality	Research work / Scientific research work (acquiring primary skills in scientific research work);	Undergraduate practice / Pre-graduation practice;

* - filled in accordance with the competency matrix and the SUP EP HE

** - elective courses/practices

4. SCOPE OF THE DISCIPLINE AND TYPES OF EDUCATIONAL WORK

The total workload of the course "Technological Threats and Cybersecurity Systems" is 3 credits.

Table 4.1. Types of educational work by periods of mastering the educational program of higher education for full-time education.

Type of academic work	**TOTAL,**academic hours		**Semester(s)**
			3
Contact work, academic hours	*34*		*34*
Lectures (LC)	17		17
Laboratory work (LW)	17		17
Practical/seminar classes (SC)	0		0
Independent work of students, academic hours	*38*		*38*
Control (exam/test with assessment), academic hours	*36*		*36*
Total complexity of the discipline	**academic hours**	***108***	*108*
	credit	***3***	*3*

5. CONTENT OF THE DISCIPLINE

Table 5.1. Content of the discipline (module) by types of academic work

Section number	Name of the discipline section	Topic Title		Topic Contents	Type of academic work*
Section 1	Standards and regulatory documents governing the concepts and classification of threats and vulnerabilities of the CS	1.1	Standards and regulatory documents	An overview of international and national information security standards. Regulatory documents governing information security requirements. Technical regulations and guidelines.	LC, LW
		1.2	Information system vulnerabilities. Classification of information system vulnerabilities.	Definition of vulnerability as a flaw or weakness in an information system. Classification of vulnerabilities by their origin: software, hardware, organizational, and human. Classification by impact level and exploitation method.	LC, LW
Section 2	Mechanisms of violation of the IB KS	2.1	Unauthorized access to information	Unauthorized access is defined as gaining access to information in violation of established access control rules. Methods of unauthorized access include direct connection, exploitation of software vulnerabilities, password guessing, session hijacking, and social engineering.	LC, LW
		2.2	Information leaks through technical channels	Definition of a technical information leakage channel as a physical medium through which protected information can be transmitted. Types of technical channels: acoustic, vibration, electromagnetic, and optical. Spurious electromagnetic emissions and interference. Eavesdropping devices and information retrieval using technical intelligence.	LC, LW
Section 3	Assessment of threats of information security breach of the CS	3.1	Assessing the possibility of the implementation (emergence) of information security threats and determining their relevance	Methods for assessing the likelihood of a threat occurring, taking into account existing vulnerabilities and potential threat sources. Factors influencing the likelihood of a threat occurring include the presence of a vulnerability, the qualifications of the attacker, and the availability of attack tools. Determining the relevance of the threat to a specific information system.	LC, LW
		3.2	Assessing the relevance of information security threats	Criteria for classifying threats as relevant. Analysis of the attacker model. Consideration of the category of information being processed and its level of confidentiality. Ranking threats by relevance for making decisions on protective measures.	LC, LW
		3.3	Assessment of the risk level of vulnerabilities of information components of information and communication systems	Methods for assessing the severity of identified vulnerabilities. Using metrics and scales to quantify the severity. Prioritizing vulnerability remediation based on their severity and potential damage.	LC, LW
Section 4	Methods for protecting the	4.1	Information security management system.	The concept of an information security management system as a	LC, LW

Section number	Name of the discipline section	Topic Title		Topic Contents	Type of academic work*
	CS from information security threats		Information security risk assessment.	set of organizational structures, policies, procedures, and resources for security management. The risk assessment process includes asset identification, identification of threats and vulnerabilities, and assessment of the likelihood and potential damage. Selection of risk treatment methods includes acceptance, mitigation, transfer, and avoidance.	
		4.2	Hardware and software tools for information security in the CS.	Classification of hardware and software security tools. User identification and authentication tools. Access control systems. Firewalls and traffic filtering tools. Antivirus protection tools. Intrusion detection and prevention systems. Cryptographic data protection tools. Information leak prevention tools. Backup and recovery tools.	LC, LW

* - to be completed only for FULL-TIME education: LC – lectures; LW – laboratory work; SC – practical/seminar classes.

6. LOGISTIC AND TECHNICAL SUPPORT OF DISCIPLINE

Table 6.1. Material and technical support for the discipline

Audience type	Equipment of the auditorium	Specialized educational/laboratory equipment, software and materials for mastering the discipline (if necessary)
Lecture	A lecture hall equipped with specialized furniture, a whiteboard (screen), and multimedia presentation equipment.	
Computer class	A computer room for conducting classes, group and individual consultations, ongoing monitoring and midterm assessment, equipped with personal computers (in the amount of ____ units), a board (screen) and technical means for multimedia presentations.	
Computer class	A computer room for conducting classes, group and individual consultations, ongoing monitoring and midterm assessment, equipped with personal computers (in the amount of ____ units), a board (screen) and technical means for multimedia presentations.	
For independent work	A classroom for independent student work (can be used for seminars and consultations), equipped with a set of specialized furniture and computers with access to the Electronic Information System.	

* - the classroom for independent work of students MUST be indicated!

7. EDUCATIONAL, METHODOLOGICAL AND INFORMATIONAL SUPPORT OF THE DISCIPLINE

Main literature:

1. Maglaras L., Kantzavelou I. (ed.). Cybersecurity issues in emerging technologies. – CRC press, 2021.

2. Sarfraz M. (ed.). Cybersecurity Threats with New Perspectives. – BoD–Books on Demand, 2021.

Further reading:

1. Toch E. et al. The privacy implications of cyber security systems: A technological survey //ACM Computing Surveys (CSUR). – 2018. –T. 51. – No. 2. – P. 1-27.

2. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity // Journal of computer and system sciences. – 2014. –T. 80. – No. 5. – pp. 973-993.

Resources of the information and telecommunications network "Internet":

1. RUDN University Electronic Library System and third-party electronic library systems to which university students have access based on concluded agreements

- RUDN University Electronic Library System – RUDN University Electronic Library System https://mega.rudn.ru/MegaPro/Web

- Electronic Library System "University Library Online" http://www.biblioclub.ru
- EBS "Urayt" http://www.biblio-online.ru
- Electronic Library System "Student Consultant" www.studentlibrary.ru
- EBS “Knowledge” https://znanium.ru/

2. Databases and search engines
   - Sage https://journals.sagepub.com/
   - Springer Nature Link https://link.springer.com/
   - Wiley Journal Database https://onlinelibrary.wiley.com/
   - Scientometric database Lens.org https://www.lens.org

Educational and methodological materials for independent work of students in mastering a discipline/module:*

1. Lecture course on the subject "Technological threats and cybersecurity systems".

* - all teaching and methodological materials for independent work of students are posted in accordance with the current procedure on the discipline page in TUIS!

DEVELOPER:

Associate Professor		Saltykova Olga Alexandrovna
Position, DEPARTMENT	*Signature*	*Surname I.O.*

HEAD OF THE DEPARTMENT:

Head of Department		Razumny Yuri Nikolaevich
Position of the DEPARTMENT	*Signature*	*Surname I.O.*

HEAD OF THE EP HE:

Professor		Razumny Yuri Nikolaevich
Position, DEPARTMENT	*Signature*	*Surname I.O.*