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 training area/specialty)

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

AIML and Space Sciences / Artificial Intelligence, Machine Learning and Space Sciences

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

2025

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 direction 27.04.04 "Control in Technical Systems" and is studied in the 3rd semester of the 2nd year. The course is implemented by the Department of Mechanics and Control Processes. The course consists of 4 sections and 9 topics and is aimed at studying the fundamental principles of information security threat models for computer systems and assessing their impact on information security risks; analysis of the main methods for solving typical problems and familiarization with the area of their application in professional activities.

The purpose of mastering the discipline is to form fundamental knowledge and skills in applying methods for solving problems necessary for professional activities, and to increase the general level of digital literacy of students.

2. REQUIREMENTS TO THE RESULTS OF MASTERING THE DISCIPLINE

Mastering the discipline "Technology Threats and Cybersecurity Systems" is 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 Competence Achievement** (within the framework of 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 main 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 knowledge 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 EDUCATION

Discipline "Technology 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 "Technology 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, practices*	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 / Research work (acquiring primary skills in 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 / Research work (acquiring primary skills in research work);	Undergraduate practice / Pre-graduation practice;

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

** - elective disciplines/practices

4. SCOPE OF THE DISCIPLINE AND TYPES OF STUDY WORK

The total workload of the discipline "Technology 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,**ac.h.		**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*
General complexity of the discipline	**ac.h.**	***108***	*108*
	credit.ed.	***3***	*3*

5. CONTENT OF THE DISCIPLINE

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

Section number	Name of the discipline section	Section Contents (Topics)		Type of academic work*
Section 1	Standards and regulations governing the concepts and classification of threats and vulnerabilities of the CS	1.1	Standards and regulations	LC, LW
		1.2	Vulnerabilities of information systems. Classification of vulnerabilities of information systems.	LC, LW
Section 2	Mechanisms of violation of the IB KS	2.1	Unauthorized access to information	LC, LW
		2.2	Information leaks through technical channels	LC, LW
Section 3	Assessment of threats of violation of the information security of the CS	3.1	Assessing the possibility of implementation (emergence) of information security threats and determining their relevance	LC, LW
		3.2	Assessing the relevance of information security threats	LC, LW
		3.3	Assessment of the level of danger of vulnerabilities of information components of information and communication systems	LC, LW
Section 4	Methods of protecting the CS from information security threats	4.1	Information security management system. Information security risk assessment.	LC, LW
		4.2	Hardware and software tools for information security in the CS.	LC, LW

* - filled in 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 of the discipline

Audience type	Equipping the auditorium	Specialized educational/laboratory equipment, software and materials for mastering the discipline (if necessary)
Lecture	An auditorium for conducting lecture-type classes, equipped with a set of specialized furniture; 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 (15 units), a board (screen) and technical means for multimedia presentations.	
For independent work	A classroom for independent work of students (can be used for conducting seminars and consultations), equipped with a set of specialized furniture and computers with access to the Electronic Information System.	

* - the audience 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 EBS and third-party EBSs to which university students have access on the basis of concluded agreements
   - Electronic library system of RUDN - ELS RUDN https://mega.rudn.ru/MegaPro/Web
   - Electronic library system "University library online"http://www.biblioclub.ru
   - EBS "Yurait"http://www.biblio-online.ru
   - Electronic Library System "Student Consultant" www.studentlibrary.ru
   - EBS "Znanium"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 "Technology Threats and Cybersecurity Systems".

* - all educational 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		Varfolomeev Alexander Alekseevich
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:

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