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

FUNDAMENTALS OF INFORMATION SECURITY AND CYBER RESILIENCE

(name of discipline/module)

Recommended for the field of study/specialty:

27.03.04 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):

DATA SCIENCE AND SPACE SYSTEMS

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

2026

1. THE GOAL OF MASTERING THE DISCIPLINE

The course "Fundamentals of Information Security and Cyber Resilience" is part of the bachelor's program "Data Science and Space Systems" in the 27.03.04 "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 13 sections and 32 topics and focuses on the main types of potential technological threats and methods for ensuring information security.

The purpose of mastering the discipline is to acquire knowledge, skills, abilities and experience in the field of information security and information protection.

2. REQUIREMENTS FOR THE RESULTS OF MASTERING THE DISCIPLINE

Mastering the course "Fundamentals of Information Security and Cyber Resilience" 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)
UC-12	Able to search for relevant sources of information and data, perceive, analyze, memorize, and transmit information using digital tools, as well as algorithms when working with data obtained from various sources in order to effectively use the information obtained to solve problems; evaluate information, its reliability, and draw logical conclusions based on incoming information and data	UC-12.1 Searches for the necessary sources of information and data, perceives, analyzes, remembers and transmits information using digital means, as well as with the help of algorithms when working with data obtained from various sources in order to effectively use the information received to solve problems; UC-12.2 Conducts an assessment of information, its reliability, builds logical conclusions based on incoming information and data;
PC-5	Able to develop, debug, test performance, and modify software; apply software design methods and tools, develop and coordinate software documentation	PC-5.1 Knowledge of existing system and application software, software design and development methods, database structures and structures, and software interfaces. Knowledge of regulatory and technical documentation for the development of software documentation; PC-5.2: Able to apply methods and tools for designing software, data structures, databases, and programming interfaces. Able to analyze regulatory and technical documentation for the development of software documentation; PC-5.3 Possesses basic skills in technologies for development, debugging, performance testing and modification of system application software, and modernization of technical solutions for software development;

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

Course "Fundamentals of Information Security and Cyber Resilience" refers to the part formed by the participants of educational relations 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 "Fundamentals of Information Security and Cyber Resilience."

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***
UC-12	Able to search for relevant sources of information and data, perceive, analyze, memorize, and transmit information using digital tools, as well as algorithms when working with data obtained from various sources in order to effectively use the information obtained to solve problems; evaluate information, its reliability, and draw logical conclusions based on incoming information and data		Research work / Scientific research work; Technological Training; Undergraduate Training; Research Work; Automatic Control Theory; Optimal Control Methods; Analysis of Geoinformation Data;
PC-5	Able to develop, debug, test performance, and modify software; apply software design methods and tools, develop and coordinate software documentation		*Virtual and Augmented Reality Technology***; *Virtual and augmented reality technologies***; Analysis of Geoinformation Data; Research work / Scientific research work; Technological Training; Undergraduate Training; Research Work;

* - 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 “Fundamentals of Information Security and Cyber Resilience” is 2 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	*36*		*36*
Lectures (LC)	18		18
Laboratory work (LW)	18		18
Practical/seminar classes (SC)	0		0
Independent work of students, academic hours	*36*		*36*
Control (exam/test with assessment), academic hours	*0*		*0*
Total complexity of the discipline	**academic hours**	*72*	*72*
	credit	***2***	*2*

The total workload of the course “Fundamentals of Information Security and Cyber Resilience” is 2 credits.

Table 4.2. 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	*36*		*36*
Lectures (LC)	18		18
Laboratory work (LW)	18		18
Practical/seminar classes (SC)	0		0
Independent work of students, academic hours	*36*		*36*
Control (exam/test with assessment), academic hours	*0*		*0*
Total complexity of the discipline	**academic hours**	*72*	*72*
	credit	***2***	*2*

The total workload of the course “Fundamentals of Information Security and Cyber Resilience” is 2 credits.

Table 4.3. 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	*36*		*36*
Lectures (LC)	18		18
Laboratory work (LW)	18		18
Practical/seminar classes (SC)	0		0
Independent work of students, academic hours	*36*		*36*
Control (exam/test with assessment), academic hours	*0*		*0*
Total complexity of the discipline	**academic hours**	*72*	*72*
	credit	***2***	*2*

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	The nature, objectives and problems of information security	1.1	Introduction	The role of information in modern society as a key resource. The development of the information industry and digital economy. The objective need to ensure information security and protect information from internal and external threats.	OK
		1.2	Definition of information. Documented information. Electronic message. Assets. Resources. ¶Various definitions of information security, information protection, cybersecurity, cyber resilience¶	Definition of information as data, regardless of its presentation form. Documented information as data recorded on a tangible medium. Electronic communication as data transmitted via electronic means of communication. Assets and resources as objects of protection. Applied definitions of information security, information protection, and cybersecurity.	OK
		1.3	Modern formulation of the problem of information security	The modern definition of information security is as ensuring availability, integrity, and confidentiality. Information security specialists: areas of work and requirements.	OK
Section 2	The concept of national security and types of security. Information security in the Russian Federation.	2.1	Bodies ensuring national security of the Russian Federation, goals, objectives.	The role and place of information security in the national security system.	OK
		2.2	Russia's National Interests in the Information Sphere. Priority Areas of Information Security in the Russian Federation.	Priority areas in the field of information security in the Russian Federation: ensuring citizens' rights, developing domestic technologies, and protecting against information and psychological influences.	OK
		2.3	Trends in the development of information policy of states and agencies. State secrets.	State secrets are information protected by the state in the field of military, foreign policy, economic and other activities.	OK
Section 3	International, national and departmental regulatory framework in the field of information security	3.1	General Provisions. Conceptual Documents on Information Security. Key Federal Regulatory Legal Acts. Laws Regarding Intellectual Property Protection. Provisions of the Civil Code of the Russian Federation on Information Security.	General provisions of legal regulation in the field of information security. Conceptual documents: the Information Security Doctrine of the Russian Federation, the National Security Strategy. Key federal regulatory legal acts. Laws concerning the protection of intellectual property.	OK
		3.2	International cooperation. Code of Administrative Offenses. Criminal Code and information protection. Key bylaws in the field of information security. Decrees of the President of the Russian Federation, resolutions of the Government of the Russian Federation, de-	International cooperation in information security. Code of Administrative Offenses: liability for violations in the information sphere. Criminal Code and information protection: elements of crimes. Key bylaws in the field of information security.	OK

Section number	Name of the discipline section	Topic Title		Topic Contents	Type of academic work*
			partmental regulatory framework.		
Section 4	Information security threats. Risk management.	4.1	The concept of threat	The concept of an information security threat. Types of threats: destruction, modification, blocking, and theft of information. The nature of threats: intentional and natural factors. Sources of threats: external and internal. Threat model and model of an information security violator.	LC, LW
		4.2	General characteristics of risk analysis, assessment and management	Risk assessment scales. Weakness-based assessment. Risk assessment based on intrusion stages. Software tools for risk analysis and management.	LC, LW
Section 5	Information and automated systems	5.1	Definitions of information (IS) and automated information processing system (AS)	Typical types of automated system structures. Types of impact on information in information systems and automated systems. Security threats to automated systems.	LC, LW
		5.2	Measures to counter threats to nuclear power plant security.	AS vulnerabilities. Principles of designing an AS protection system. Automated process control systems (APCS).	LC, LW
Section 6	Technical channels of information leakage	6.1	Definition, classification and general characteristics of TKUI.	Technical information leakage channels (TILCs) and methods for blocking them. Passive and active protection against information leakage through technical channels.	LC, LW
		6.2	Visual and acoustic channels.	Protecting information in telephone channels. Protection against stray electromagnetic radiation and interference. Technical bugs as a means of unauthorized data collection.	LC, LW
		6.3	Methods for detecting TKUI.	Methods and techniques for blocking technical channels of information leakage. Requirements for the selection and equipment of premises for automated data processing systems to protect against technical channels of information leakage. The concept of a controlled area.	LC, LW
Section 7	Technical means of ensuring the safety of the facility.	7.1	Definition and main objectives of protection of modern objects.	Technical means of ensuring facility security: definition, system classification, general analysis. Technical means and security systems.	LC, LW
		7.2	Technical means of monitoring and controlling the movement of people and objects.	People identification equipment and systems. Equipment and systems for access control to areas, buildings, and premises, as well as information processing and storage systems. Methods for selecting equipment and general information on the security equipment market.	LC, LW
Section 8	Methods of access control to information	8.1	Methods of user identification and authentication.	Password authentication: advantages and disadvantages. Biometric authentication using fingerprints, irises, and voice. Access control methods, implementation techniques, and tools.	LC, LW

Section number	Name of the discipline section	Topic Title		Topic Contents	Type of academic work*
		8.2	Brief description of modern means of access control.	Mathematical models of information access control. Subject-object access model.	LC, LW
		8.3	Security policy and access model.	Electronic keys, identification cards, key fobs. Card types: magnetic, smart cards, RFID.	LC, LW
Section 9	Malicious programs	9.1	Malicious bookmarks (MB): definition, types.	Destructive effects of backdoors. Access control systems and protection against malicious backdoors. Prevention and mitigation of the effects of malicious backdoors.	LC, LW
		9.2	Brief description of protective measures	Brief description of protective measures: legal, administrative, organizational, hardware, and software. Computer viruses: classification by habitat, method of infection, and destructive capabilities.	LC, LW
		9.3	The main channels for the distribution of viruses and other malicious programs.	Antivirus tools: a brief description of popular antivirus programs. Copy protection tools. Examples of malware.	LC, LW
Section 10	Fundamentals of Network Security	10.1	Introduction to the Internet and Intranet.	Network attack methods: traffic interception, data spoofing, denial of service. Protection against firewalls. Specifics for different layers of the ISO/OSI model.	LC, LW
		10.2	Firewall technologies.	Firewall functions: packet filtering, proxying, address translation. Forming a firewall policy. Firewall evaluation criteria.	LC, LW
		10.3	Building secure virtual VPN networks.	VPN security tools. Protection at the data link and session layers. PPTP, L2TP, SSL/TLS, and SOCKS protocols. Network-layer protection. IPSEC protocol.	LC, LW
		10.4	Security of remote access to a local network.	Centralized control. Access control using single sign-on with authorization. Intrusion detection technologies. Classification of intrusion detection and prevention systems (IDS/IPS). Threats and vulnerabilities of wireless networks.	LC, LW
Section 11	Organizational and legal support for information protection	11.1	The essence and role of organizational and legal aspects of information security.	The regulatory framework for information security. The Law of the Russian Federation "On Information, Information Technologies, and Information Protection." Types and categories of restricted information: state and other secrets. The Laws of the Russian Federation "On State Secrets," "On Commercial Secrets," "On Personal Data," "On the National Payment System," and "On the Security of the Critical Information Infrastructure of the Russian Federation." State licensing and certification system for information security activities. Decree of the President of the Russian Federation "On Measures to Ensure Compliance with the Law in the Development, Production, Sale, and Operation of Encryption	LC, LW

Section number	Name of the discipline section	Topic Title		Topic Contents	Type of academic work*
				Tools, as well as the Provision of Information Encryption Services." The Law of the Russian Federation "On Electronic Digital Signature." Criminal-legal regulation of information security.	
Section 12	Information security standards	12.1	Historical overview of the development of foreign information security standards.	GOST R ISO/IEC 15408-2002, as an authentic version of the common criteria for IT security. Functional security requirements. Security assurance requirements. ISO/IEC 17799:2002 (BS 7799:2000) standards.	OK
		12.2	Information security management standards ISO/IEC 27001-27040.	German BSI standards. SysTrust, SCORE, and GIAC standards. Wireless network standards. Russian information security standards. Information security standards for Russian banking organizations. GOST R 57580.1-2017 and GOST R 57580.2-2018. Internet information security standards (IETF, RFC).	OK
Section 13	Certification and certification in the field of information security	13.1	Purpose and general characteristics.	Voluntary certification. Mandatory confirmation of conformity. Declaration of conformity. Mandatory certification.	OK
		13.2	Conducting certification tests	Testing principles and certification test documents. Certification of products imported from outside the Russian Federation. Certification for compliance with information security requirements. Certification of information technology facilities.	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 (14 in total), 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. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Introduction to information security in automated systems – M.: Goryachaya Liniya-Telecom, 2001, 148 p.

2. Belov E.B., Los V.P., Meshcheryakov R.V., Shelupanov A.A. Fundamentals of Information Security. Textbook for Universities, Moscow: Hot Line – Telecom, 2006. - 544 p.

3. Tikhonov V.A., Reich V.V. Information security: conceptual, legal, organizational and technical aspects: textbook. - M .: Helios ARV, 2006.- 528 p.

4. Shan'gin V.F. Information security of computer systems and networks: textbook. Manual. - M.: ID "FORUM": INFRA-M, 2008.-416 p.

5. Moore T., Pym D., Ioannidis C., Economics of Information Security and Privacy, Springer, 2010, - 320 pp.

6. Ensuring information security for business, Edited by A.P. Kurilo, Alpina Publishers, 2011, 392 p.

7. Bondarev V.V. Introduction to Information Security of Automated Systems (2nd edition). – Moscow: Bauman Moscow State Technical University. 2018. – 252 p.

8. Organizational and legal support of information security. edited by A.A. Alexandrov, M.P. Sychev – M.: Bauman Moscow State Technical University. 2018. – 292 p.

9. Malyuk A.A. Fundamentals of security policy for critical information infrastructure systems. – M.: Goryachaya Liniya-Telecom, 2018. – 314 p.

Further reading:

1. Torokin A.A. Fundamentals of engineering and technical information protection. – M.: Os-89, 1998.-336 p.

2. Devyanin P.N., Mikhal'skiy O.O., Pravikov D.I., Shcherbakov A.Yu., Theoretical

foundations of computer security, – M: Radio and communication, 2000. -192 p.

3. Pyarin V.A., Kuzmin A.S., Smirnov S.N. Security of electronic business. – M.: Helios ARB, 2002. – 432 p.

4. Snytnikov A.A. Licensing and certification in the field of information security. – M.: Helios ARV, 2003.- 192 p.

5. Sobolev A.N., Kirillov V.M. Physical foundations of technical means of ensuring information security: Textbook. – M.: Helios ARV, 2004.- 144 p.

6. Streltsov A.A. Legal support of information security of Russia: theoretical and methodological foundations. – Minsk.: BELLITFOND, 2005.-304 p.

7. Shumsky A.A., Shelupanov A.A. Systems analysis in information security: Textbook. – M.: Helios ARV, 2005.- 224 p.

8. Semkin S.N., Belyakov E.V., Grebenev S.V., Kozachok V.I. Fundamentals of organizational support for information security of information technology objects: Textbook. manual. - M .: Helios ARV, 2005.- 192 p.

9. Astakhov A. The art of information risk management. – M.: DMK Press, 2010. – 312 p.

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

- Electronic library system of RUDN - ELS RUDN http://lib.rudn.ru/MegaPro/Web
- Electronic Library System "University Library Online" http://www.biblioclub.ru
- EBS Yurayt http://www.biblio-online.ru
- Electronic Library System "Student Consultant" www.studentlibrary.ru
- Electronic Library System "Troitsky Bridge"

2. Databases and search engines

- electronic fund of legal and regulatory documentation http://docs.cntd.ru/
- Yandex search engine https://www.yandex.ru/
- Google search engine https://www.google.ru/
- SCOPUS abstract database http://www.elsevierscience.ru/products/scopus/

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

1. Lecture course on the subject "Fundamentals of Information Security and Cyber Resilience".

* - 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		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:

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