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

Engineering Academy
(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 training area/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)

2025

1. THE GOAL OF MASTERING THE DISCIPLINE

The course "Fundamentals of Information Security and Cyber Resilience" is part of the bachelor's degree program "Data Science and Space Systems" in the direction 27.03.04 "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 13 sections and 32 topics and is aimed at studying the main types of possible technological threats and ways to ensure information security

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

2. REQUIREMENTS TO THE RESULTS OF MASTERING THE DISCIPLINE

Mastering the discipline "Fundamentals of Information Security and Cyber Resilience" 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)
UC-12	Able to search for the necessary sources of information and data, perceive, analyze, remember and transmit information using digital means, as well as using algorithms when working with data obtained from various sources in order to effectively use the information received to solve problems; evaluate information, its reliability, build 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 using algorithms when working with data obtained from various sources in order to effectively use the information obtained 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, modify software; apply software design methods and tools, develop and coordinate software documentation	PC-5.1 Knows existing system and application software, methods of designing and developing software, structures and databases, software interfaces. Knows regulatory and technical documentation for developing software documentation; PC-5.2 Can apply methods and tools for designing software, data structures, databases, and software interfaces. Can analyze regulatory and technical documentation for developing software documentation; PC-5.3 Possesses basic skills in technologies for development, debugging, testing the functionality and modification of system application software, and upgrading technical solutions for software development;

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

Discipline "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, practices*	Subsequent disciplines/modules, practices*
UC-12	Able to search for the necessary sources of information and data, perceive, analyze, remember and transmit information using digital means, as well as using algorithms when working with data obtained from various sources in order to effectively use the information received to solve problems; evaluate information, its reliability, build 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, 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 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 “Fundamentals of Information Security and Cyber Resilience” is “2” credit units.

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	*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*
General complexity of the discipline	**ac.h.**	***72***	*72*
	credit.ed.	***2***	*2*

5. CONTENT OF THE DISCIPLINE

*Table 5.1. Contents of the discipline (modus)*la) by types of educational work

Section number	Name of the discipline section	Section Contents (Topics)		Type of academic work*
Section 1	The nature, objectives and problems of information security	1.1	Introduction. The role of information in the life of modern society. Development of the information industry. The objective need for information security and information protection.	LC, LW
		1.2	Definition of information. Documented information. Electronic message. Assets. Resources. ¶Different definitions of information security, information protection, cybersecurity, cyber resilience¶	LC, LW
		1.3	Modern statement of the problem of information security. ¶Purpose and structure of the discipline. Recommended primary and additional literature. Internet sources. Information security specialists. Licensing of information security activities.¶	LC, LW
Section 2	The concept of national security, types of security. Information security of the Russian Federation	2.1	Bodies ensuring national security of the Russian Federation, goals, objectives.	LC, LW
		2.2	National interests of the Russian Federation in the information sphere. Priority areas in the field of information protection in the Russian Federation.	LC, LW
		2.3	Trends in the development of information policy of states and departments. State secrets.	LC, LW
Section 3	International, national and departmental regulatory framework in the field of information security	3.1	General Provisions. Conceptual Documents in the Field of Information Security. The Most Important Federal Regulatory Legal Acts. Laws Concerning the Protection of Intellectual Property. Provisions of the Civil Code of the Russian Federation on Information Protection.	LC, LW
		3.2	International cooperation. Code of Administrative Offences. Criminal Code and information protection. Main by-laws in the field of information security. Decrees of the President of the Russian Federation, resolutions of the Government of the Russian Federation, departmental regulatory framework.	LC, LW
Section 4	Information security threats. Risk control.	4.1	The concept of threat. Types of threats. Nature of origin of threats: intentional factors, natural factors. Sources of threats. ¶Threat model and model of information security violator. ¶	LC, LW
		4.2	General characteristics of risk analysis, assessment and control. Scales. Assessment based on identifying a weak link. Risk assessment based on considering the stages of an intrusion. Software tools used for risk analysis.	LC, LW
Section 5	Information and automated systems	5.1	Definitions of information (IS) and automated system (AS) of information processing. GOSTs for AS. Typical types of AS structure. Types of impact on information in IS and AS. AS security threats and their classification.	LC, LW
		5.2	Measures to counteract threats to AS security. AS vulnerabilities. AS protection system design principles. Automated process control systems (APCS).	LC, LW
Section 6	Technical channels of information leakage	6.1	Technical information leakage channels (TILC) and methods of blocking them. Passive and active protection against information leakage via	LC, LW

Section number	Name of the discipline section	Section Contents (Topics)		Type of academic work*
			technical channels. Definition, classification and general characteristics of TILC.	
		6.2	Visual and acoustic channels. Information protection in telephone channels. Protection from side electromagnetic radiation and interference (SEMI). Technical bookmarks.	LC, LW
		6.3	Methods of detecting TKUI. Methods and techniques for blocking TKUI. Requirements for the selection and equipment of premises for AS data processing according to the conditions of protection from TKUI. The concept of a controlled territory and methods for determining its size. Features of protecting personal computing equipment from information leakage through technical channels.	LC, LW
Section 7	Technical means of ensuring facility security.	7.1	Definition and main objectives of protection of modern objects. Technical means of ensuring protection of the object: definition, system classification, general analysis. Technical means and systems of protection of the territory, buildings and premises.	LC, LW
		7.2	Technical means of monitoring and controlling the movement of people and objects. Technical means and systems for identifying people. Technical means and systems for controlling access to the territory, buildings and premises, to information processing and storage facilities. Methods for selecting technical means, general information about the market of technical means for ensuring security.	LC, LW
Section 8	Methods of access control to information	8.1	Methods of user identification and authentication. Password method. Biometric authentication. Methods of access control, methods and means of their implementation.	LC, LW
		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. Unified biometric system of Russia.	LC, LW
Section 9	Malicious programs	9.1	Malicious bookmarks (MB): definition, types. Destructive actions of bookmarks. Systems of access control and protection from MB. Prevention and minimization of the effects of MB.	LC, LW
		9.2	Brief description of protection measures: legal, administrative and organizational, hardware and software. Computer viruses. Classification	LC, LW
		9.3	Main channels of distribution of viruses and other malicious programs. Anti-virus tools: brief description of popular anti-virus programs.¶Copy protection tools. Examples of tools and technologies¶	LC, LW
Section 10	Fundamentals of Network Security	10.1	Introduction to Internet and Intranet. Methods of attacking networks and protecting against firewalls. Features for different layers of the ISO/OSI model.	LC, LW
		10.2	Firewall technologies. Firewall functions. Formation of firewall policy. Firewall evaluation criteria	LC, LW

Section number	Name of the discipline section	Section Contents (Topics)		Type of academic work*
		10.3	Building secure virtual VPN networks. VPN security tools. ¶Protection at the channel and session levels. PPTP, L2TP, SSL/TLS, SOCKS protocols. ¶Protection at the network level. IPSEC protocol.¶	LC, LW
		10.4	Remote access security to the local network. Centralized control. Access control by 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 nature 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 types of secrets. The Law of the Russian Federation "On State Secrets", "On Commercial Secrets", "On Personal Data", "On the National Payment System", "On the Security of the Critical Information Infrastructure of the Russian Federation". State system of licensing and certification of activities in the field of information security. Decree of the President of the Russian Federation "On measures to ensure compliance with the law in the field of development, production, sale and operation of encryption tools, as well as the provision of services in the field of information encryption". The Law of the Russian Federation "On Electronic Digital Signature". Criminal-legal regulation of information protection.¶	LC, LW
Section 12	Information security standards	12.1	Historical outline of the development of foreign information security standards. GOST R ISO/IEC 15408-2002 as an authentic version of general criteria for IT security. Functional security requirements. Security assurance requirements. ISO/IEC 17799: 2002 (BS 7799:2000) standards.	LC, LW
		12.2	Information security control standards ISO/IEC 27001-27040 . German BSI standards. SysTrust, SCORE, GIAC standards.¶Standards for wireless networks. Domestic information security standards. Standards for ensuring information security of organizations of the banking system of the Russian Federation. GOST R 57580.1-2017 and GOST R 57580.2 – 2018.¶Internet information security standards (IETF, RFC).¶	LC, LW
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.	LC, LW
		13.2	Conducting certification tests: principles of testing, certification test documents. Certification of products imported from outside the Russian Federation. Certification at the regional and international levels.	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. MalyUC 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: Hotline – Telecom, 2006. - 544 p.

3. Tikhonov V.A., Reich V.V. Information security: conceptual, legal, organizational and technical aspects: textbook. manual. - 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 of business, Edited by Kurilo A.P., Alpina Publishers, 2011, - 392 p.

7. Bondarev V.V. Introduction to information security of automated systems (2nd edition). - M.: Bauman Moscow State Technical University.N.E. Bauman. 2018. – 252s

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

9. MalyUC A.A. Fundamentals of security policy for critical information infrastructure systems. - M.: Hotline - Telecom, 2018. - 314 p.

Further reading:

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

2. Devyanin P.N., Mikhalsky 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 pp.

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

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 pp.

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 pp.

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

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 RUDNhttp://lib.rudn.ru/MegaPro/Web
- Electronic library system "University library online"http://www.biblioclub.ru
- EBS Yuraithttp://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 normative-technical documentationhttp://docs.cntd.ru/
- Yandex search enginehttps://www.yandex.ru/
- search engineGoogle https://www.google.ru/
- abstract databaseSCOPUS 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 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		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:

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