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

Academy of Engineering
(name of the main educational unit (POU) - developer of the EP HE)

COURSE SYLLABUS

Fundamentals of information security and cyber resilience
(name of discipline/module)

Recommended by the Didactic Council for the Education Field of:

27.03.04 CONTROL IN TECHNICAL SYSTEMS
(code and name of the area of training/specialty)

The course instruction is implemented within the professional education programme of higher education:

DATA ENGINEERING AND SPACE SYSTEMS CONTROL
(name (profile/specialization) EP HE)

2024

1. GOAL OF DISCIPLINE MASTERING

The discipline “Fundamentals of information security and cyber resilience” is included in the bachelor’s program “Data Engineering and Space Systems Control” in the direction of 27.03.04 “Control in Technical Systems” and is studied in the 3rd semester of the 2nd year. The discipline is implemented by the Department of Mechanics and Control Processes. The discipline 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, abilities, skills and experience in the field of information security and information protection

2. REQUIREMENTS FOR 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 formed in students when mastering the discipline (results of mastering the discipline)

Cipher	**Competence**	**Indicators of Competency Achievement** (within this discipline)
GC-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 received 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	GC-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 received from various sources in order to effectively use the received information to solve problems; GC-12.2 Evaluates information, its reliability, builds logical conclusions based on incoming information and data;
PC-5	Able to develop, debug, test functionality, and modify software; apply software design methods and tools, develop and coordinate software documentation	PC-5.1 Knows existing system and application software, methods for designing and developing software, structures and databases, program interfaces. Knows the regulatory and technical documentation for the development of software documentation; PC-5.2 Can apply methods and tools for designing software, data structures, databases, and software interfaces. Able to analyze regulatory and technical documentation to develop program documentation for software; PC-5.3 Possesses basic skills in technologies for development, debugging, performance testing and modification of system application software, modernization of technical solutions for software development;

3. PLACE OF DISCIPLINE IN THE STRUCTURE OF HE EP

Discipline "Fundamentals of information security and cyber resilience" refers to the part formed by the participants in educational relations of block 1 “Disciplines (modules)” of the educational program of higher education.

As part of the educational program of higher education, students also master other disciplines and/or practices that contribute to achieving the planned results of mastering the discipline “Fundamentals of Information Security and Cyber Resilience.”

Table 3.1. List of components of EP HE that contribute to achieving the planned results of mastering the discipline

Cipher	**Name of competency**	**Previous disciplines/modules, practices***	**Subsequent disciplines/modules, practices***

GC-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 received 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		Automatic Control Theory;
			Optimal Control Methods;
			Analysis of Geoinformation Data;
			Research work / Scientific research work;
			Technological Training;
			Undergraduate practice / Pre-graduate practice;

PC-5	Able to develop, debug, test functionality, and modify software; apply software design methods and tools, develop and coordinate software documentation		Research work / Scientific research work;
			Technological Training;
			Undergraduate practice / Pre-graduate practice;
			*Virtual and Augmented Reality Technology***;
			*Virtual and augmented reality technologies***;
			Analysis of Geoinformation Data;

* - to be filled out in accordance with the competency matrix and SUP EP VO

** - elective disciplines/practices

4. SCOPE OF DISCIPLINE AND TYPES OF STUDY WORK

The total labor intensity 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 study.

Type of educational work	**TOTAL,**ac.ch.		**Semester(s)**
			3
Contact work, ac.ch.	*36*		*36*
Lectures (LC)	18		18
Laboratory work (LR)	18		18
Practical/seminar sessions (SZ)	0		0
Independent work of students, ac.ch.	*36*		*36*
Control (exam/test with assessment), academic degree.	*0*		*0*
Total labor intensity of the discipline	**ac.ch.**	*72*	*72*
	credit units	***2***	*2*

5. CONTENT OF DISCIPLINE

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

Section number	**Name of the discipline section**	**Contents of the section (topic)**		**Type of educational work***
Section 1	The essence, tasks 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.	LK, LR
		1.2	Definition of information. Documented information. Electronic message. Assets. Resources. ¶Various definitions of information security, information protection, cybersecurity, cyber resilience¶	LK, LR
		1.3	Modern formulation of the information security problem. ¶Purpose and structure of the discipline. Recommended basic and additional reading. Internet sources. Information security specialists. Licensing of information security activities.¶	LK, LR
Section 2	The concept of national security, types of security. Information security of the Russian Federation	2.1	Bodies ensuring the national security of the Russian Federation, goals, objectives.	LK, LR
		2.2	National interests of the Russian Federation in the information sphere. Priority areas in the field of information security in the Russian Federation.	LK, LR
		2.3	Trends in the development of information policy of states and departments. State secret.	LK, LR
Section 3	International, national and departmental regulatory legal 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 relating to the protection of intellectual property. Provisions of the Civil Code of the Russian Federation on information protection.	LK, LR
		3.2	The international cooperation. Code of Administrative Offences. Criminal code and information protection. Basic 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.	LK, LR
Section 4	Information security threats. Management of risks.	4.1	The concept of threat. Types of threats. The nature of the origin of threats: intentional factors, natural factors. Sources of threats. ¶Threat model and information security violator model. ¶	LK, LR
		4.2	General characteristics of risk analysis, assessment and management. Scales. Assessment based on identifying the weak link. Risk assessment based on consideration of the stages of an invasion. Software tools used for risk analysis.	LK, LR
Section 5	Information and automated systems	5.1	Definitions of information (IS) and automated information processing systems (AS). GOST standards for speakers. Typical types of AC structure. Types of influence on information in IS and AS. NPP safety threats and their classification.	LK, LR
		5.2	Measures to counter threats to nuclear power plant safety. AS vulnerabilities. Principles of constructing a nuclear power plant protection system. Automated process control systems (APCS).	LK, LR
Section 6	Technical channels of information leakage	6.1	Technical channels of information leakage (TCIL) and methods of blocking them. Passive and active	LK, LR

Section number	**Name of the discipline section**	**Contents of the section (topic)**		**Type of educational work***
			protection against information leakage through technical channels. Definition, classification and general characteristics of TKUI.	
		6.2	Visual and acoustic channels. Protection of information in telephone channels. Protection against spurious electromagnetic radiation and interference (PEMIN). Technical bookmarks.	LK, LR
		6.3	Methods for detecting TKUI. Ways and methods of covering TKUI. Requirements for the selection and equipment of premises for automated data processing according to the conditions of protection from TKUI. The concept of controlled territory and methods for determining its size. Features of protecting personal computer equipment from information leakage through technical channels.	LK, LR
Section 7	Technical means to ensure the safety of the facility.	7.1	Definition and main goals of protecting modern facilities. Technical means of ensuring the protection of an object: definition, system classification, general analysis. Technical means and systems for protecting territory, buildings and premises.	LK, LR
		7.2	Technical means of monitoring and controlling the movement of people and objects. Technical means and systems for identifying people. Technical means and access control systems to the territory, buildings and premises, to information processing and storage facilities. Methods for selecting technical equipment, general information about the market for technical security equipment.	LK, LR
Section 8	Methods for controlling access to information	8.1	Methods for identifying and authenticating users. Password method. Biometric authentication. Methods of access control, methods and means of their implementation.	LK, LR
		8.2	Brief description of modern access control tools. Mathematical models of information access control. Subject-object access model.	LK, LR
		8.3	Security policy and access model. Electronic keys. ID cards, key rings. Types of cards. Unified biometric system of Russia.	LK, LR
Section 9	Malware	9.1	Malicious bookmarks (BW): definition, types. Destructive effects of bookmarks. Systems for access control and protection against airborne threats. Prevention and minimization of the consequences of exposure to air pollution.	LK, LR
		9.2	Brief description of protection measures: legal, administrative and organizational, hardware and software. Computer viruses. Classification	LK, LR
		9.3	The main channels for the spread of viruses and other malware. Anti-virus tools: a brief description of popular anti-virus programs.¶Copy protection tools. Examples of tools and technologies¶	LK, LR
Section 10	Network Security Fundamentals	10.1	Introduction to the Internet and Intranet. Methods of attacking networks and protecting against internetwork access. Features for different levels of the ISO/OSI model.	LK, LR

Section number	Name of the discipline section	Contents of the section (topic)		Type of educational work*
		10.2	Firewall technologies. ME functions. Formation of internetworking policy. Criteria for evaluating firewalls	LK, LR
		10.3	Construction of secure virtual VPN networks. VPN Security Tools. ¶Protection at the channel and session levels. Protocols PPTP, L2TP, SSL/TLS, SOCKS. ¶Protection at the network level. IPSEC protocol¶	LK, LR
		10.4	Security of remote access to the local network. Centralized control. Access control based on single sign-on with authorization.¶Attack detection technologies. Classification of attack detection and prevention systems (IDS/IPS). Threats and vulnerabilities of wireless networks.¶	LK, LR
Section 11	Organizational and legal support for information protection	11.1	The essence and role of organizational and legal aspects of information security. Regulatory legal framework for information security. Law of the Russian Federation “On information, information technologies and information protection”. ¶Types and categories of restricted access information: state and other types of secrets. Law of the Russian Federation “On State Secrets”, “On Commercial Secrets”, “On Personal Data”, “On the National Payment System”, “On the Security of 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 comply 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.” Law of the Russian Federation “On Electronic Digital Signature”. Criminal legal regulation of information protection.¶	LK, LR
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 the general IT security criteria. Functional safety requirements. Security assurance requirements. Standards ISO/IEC 17799: 2002 (BS 7799:2000).	LK, LR
		12.2	Information security management 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).¶	LK, LR
Section 13	Certification and certification in the field of information security	13.1	Purpose and general characteristics. Voluntary certification. Mandatory confirmation of compliance. Declaration of conformity. Mandatory certification.	LK, LR
		13.2	Conducting certification tests: principles of testing, documents of certification tests. Certification of products imported from abroad of the Russian	LK, LR

Section number	Name of the discipline section	Contents of the section (topic)		Type of educational work*
			Federation. Certification at regional and international levels.	

* - to be filled out only for full-time education: LC – lectures; LR – laboratory work; SZ – practical/seminar classes.

6. MATERIAL AND TECHNICAL SUPPORT OF DISCIPLINE

Table 6.1. Material and technical support of the discipline

Audience type	Auditorium equipment	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; board (screen) and technical means of multimedia presentations.	
Computer class	A computer class for conducting classes, group and individual consultations, ongoing monitoring and intermediate certification, equipped with personal computers ([Parameter] pcs.), a whiteboard (screen) and technical means for multimedia presentations.	
For independent work	An auditorium for independent work by students (can be used for seminars and consultations), equipped with a set of specialized furniture and computers with access to EIOS.	

* - the audience for independent work of students is MANDATORY!

7. EDUCATIONAL, METHODOLOGICAL AND INFORMATIONAL SUPPORT OF DISCIPLINE

Main literature:

1. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Introduction to information protection in automated systems - M.: Hotline-telecom, 2001, -148 p.

2. Belov E.B., Los V.P., Meshcheryakov R.V., Shelupanov A.A. Fundamentals of information security.Textbook for universities, M.: Hotline - Telecom, 2006. - 544 p.

3. Tikhonov V.A., Raikh V.V. Information security: conceptual, legal, organizational and technical aspects: textbook. allowance. – M.: Gelios ARV, 2006.-528 pp.

4. Shangin V.F. Information security of computer systems and networks: textbook.Manual .- M.: Publishing house "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 business information security, Ed. Kurilo A.P., Alpina Publishers, 2011, - 392 p.

7. Bondarev V.V. Introduction to Information Security of Automated Systems (2nd edition). – M.: MSTU im.N.E. Bauman. 2018. – 252s

8. Organizational and legal support of information security. edited by A.A. Alexandrova, M.P. Sychev - M.: MSTU im.N.E. Bauman. 2018. – 292 p.

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

Additional literature:

1. Thorokin A.A. Fundamentals of engineering and technical information protection. – 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 Communications, 2000. -192 p.

3. Pyarin V.A., Kuzmin A.S., Smirnov S.N. Electronic business security. – 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.: Gelios ARV, 2004.-144 p.

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

7. Shumsky A.A., Shelupanov A.A. System analysis in information security: Textbook. allowance. – 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 informatization objects: Proc. allowance. – 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. EBS of RUDN University and third-party EBS, to which university students have access based on concluded agreements

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

2. Databases and search engines

- electronic fund of legal and regulatory technical documentationhttp://docs.cntd.ru/
- Yandex search enginehttps://www.yandex.ru/
- search systemGoogle https://www.google.ru/
- abstract databaseSCOPUS http://www.elsevierscience.ru/products/scopus/

Educational and methodological materials for students' independent work when mastering a discipline/module:*

1. A course of lectures on the discipline "Fundamentals of information security and cyber resilience."

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

8. ASSESSMENT MATERIALS AND POINT-RATING SYSTEM FOR ASSESSING THE LEVEL OF COMPETENCIES FOR A DISCIPLINE

Evaluation materials and point-rating system* for assessing the level of development of competencies (parts of competencies) based on the results of mastering the discipline“Fundamentals of information security and cyber resilience” are presented in the Appendix to this Work Program of the discipline.

* - OM and BRS are formed on the basis of the requirements of the relevant local regulatory act of RUDN University.

DEVELOPER:

Assistant professor		Varfolomeev Alexander Alekseevich
Position, PBU	*Signature*	*Last name I.O.*

HEAD OF DEPARTMENT:

Head of the department		Razumny Yuri Nikolaevich
Position PBU	*Signature*	*Last name I.O.*

HEAD OF EP HE:

Professor		Razumny Yuri Nikolaevich
Position, PBU	*Signature*	*Last name I.O.*