

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Порохня Андрей Викторович

Должность: И.о. директора института передовой инженерии

Дата подписания: 22.10.2026 13:25:38

Уникальный программный ключ:

990bea3aecc48c23bd8699e48288f8d1960c600

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION

Federal State Autonomous Educational Institution of Higher Education

"NORTH CAUCASUS FEDERAL UNIVERSITY"

APPROVED BY

Acting Director of the Institute

Advanced Engineering

A.A. Porokhnya

WORK PROGRAM OF THE DISCIPLINE
Network intrusion detection systems based on AI

Field of study	11.03.02 Infocommunication Technologies and Communication Systems
Profile	Intelligent Data Processing in Infocommunication Systems and Networks
Year of start of training	2026
Form of study	Full-time
Implemented in a semester	6

Developed by:

Associate Professor of the Department of Computational Mathematics and Cybernetics, Faculty of Mathematics and Computer Science named after Professor N.I. Chervyakov

Peleshenko V. S.

Stavropol, 2026

1. The purpose and objectives of mastering the discipline:

The purpose of mastering the discipline "Network Intrusion Detection Systems Based on Artificial Intelligence" is the formation of the future bachelor's degree in the direction of training 11.03.02 is the theoretical and practical preparedness of the student to organize and conduct measures for the integrated provision of information security.

The task of the course in accordance with this program is to provide students with a system of knowledge about integrated information security, about the main problems of information protection, such as:

- the procedure for carrying out an inventory and categorization of information resources;
- the procedure for attestation of informatization objects for compliance with information security requirements;
- the procedure for identifying threats of unauthorized access to information and special effects on it in information and telecommunication systems;
- study of methods and means of protection based on AI.

2. Place of the discipline in the structure of the educational program

The discipline "Network Intrusion Detection Systems Based on Artificial Intelligence" belongs to the mandatory part for 11.03.02. Its development takes place in the 6th semester.

3. List of planned learning outcomes in the discipline correlated with the planned results of mastering the educational program of higher education

Code, formulation of competence	Indicator code, wording	Planned results characterizing the stages of the formation of competencies, indicators
UK-3 Able to carry out social interaction and fulfill his role in the team	ID-1 UK-3 participates in interpersonal and group interaction, using an inclusive approach, effective communication	Performs the assigned tasks of practice as part of a group, observing the rules of social interaction.
	ID-2 UK-3 ensures the work of the team to obtain optimal results of joint work, taking into account the individual capabilities of its members, the use of methodology for achieving success, methods, information technologies and foresight technologies	Applies effective methods of teamwork to obtain optimal work results and their analysis. Applies information technologies and foresight technologies.
	ID-3 UK-3 ensures the fulfillment of tasks based on monitoring teamwork and timely response to significant deviations	Performs the assigned tasks of the practice, as well as ensures their implementation based on the monitoring of teamwork.
UK-4 Is able to carry out business communication in oral and written forms in the state language of the Russian Federation and a foreign language(s)	ID-1 UK-4 chooses an acceptable style of business communication in the state and foreign languages, verbal and non-verbal means of interaction with partners in oral and written forms;	Fulfills the tasks of practice, choosing an acceptable style of business communication in the state and foreign languages, verbal and non-verbal means of interaction with partners in oral and written forms

	ID-2 ^{UK-4} uses information and communication technologies to increase the efficiency of professional interaction, search for the necessary information in the process of solving standard communicative tasks in the state and foreign languages;	Searches for the necessary information in the process of solving standard communicative tasks in the state and foreign languages, and also uses information and communication technologies to improve the efficiency of professional interaction
	ID-3 ^{UK-4} evaluates the effectiveness of the applied communication technologies in professional interaction in the state and foreign languages, and selects the optimal ones.	In the performance of the assigned tasks, the practice evaluates the effectiveness of the applied communication technologies in professional interaction in the state and foreign languages, and makes a choice of optimal
UK-5 Able to perceive the intercultural diversity of society in socio-historical, ethical and philosophical contexts	ID-1 ^{UK-5} identifies, compares and analyzes information about the cultural characteristics and traditions of various social groups, in order to choose a strategy for interaction with their carriers;	Searches for the information necessary to solve the tasks, identifying and analyzing information about the cultural characteristics and traditions of various social groups, to choose a strategy for interacting with their carriers
	ID-2 ^{UK-5} demonstrates a respectful attitude to the historical heritage and socio-cultural traditions of various social groups, based on knowledge of the stages of historical development of Russia (including the main events, the main historical figures) in the context of world history and a number of cultural traditions of the world (depending on the environment and the objectives of education), including world religions, philosophical and ethical teachings;	Fulfilling the tasks of the practice, he demonstrates a respectful attitude to the historical heritage and socio-cultural traditions of various social groups
	ID-3 ^{UK-5} chooses ways of constructive interaction with people, taking into account their socio-cultural characteristics, in order to successfully perform professional tasks and strengthen social integration;	Fulfilling the tasks of the practice, chooses ways of constructive interaction with people, taking into account their socio-cultural characteristics in order to successfully perform professional tasks and strengthen social integration
	ID-4 ^{UK-5} analyzes various socio-cultural trends, facts and phenomena on the basis of a holistic view of the foundations of the universe and the prospects for its development,	Analyzes various socio-cultural trends, facts and phenomena on the basis of a holistic view of the foundations of the universe

	understands the relationship between the diversity of worldviews and the course of development of history, science, human ideas about nature, society, cognition and oneself.	and the prospects for its development
PC-7. Capable of administering remote access security tools (operating systems and specialized protocols)	ID-1PC-7 understands and uses the basic principles, protocols and software cryptographic tools for ensuring the information security of network devices.	Knows the basic principles, protocols and software cryptographic tools for ensuring the information security of network devices.
	ID-2PC-7 understands the general principles of operation and architecture of hardware, software, software and hardware of the administered network; protocols of the channel, network, transport and application layers of the open systems interaction model.	Is able to use the general principles of operation and architecture of hardware, software and software and hardware of the administered network; protocols of the channel, network, transport and application layers of the open systems interaction model
	ID-3PK-7 uses software, hardware and software and hardware to protect network devices from unauthorized access; configures the parameters of modern software and hardware firewalls.	Applies software, hardware and software and hardware to protect network devices from unauthorized access; Configures the parameters of modern software and hardware firewalls
	ID-4PC-7 connects and configures modern remote access security tools (operating systems and specialized protocols); works with control and measurement hardware and software.	Capable of connecting and configuring modern remote access security tools (operating systems and specialized protocols); Works with control and measurement hardware and software.
	ID-5PC-7 installs additional software products to ensure remote access security and parameterization.	Installs additional software products to ensure the security of remote access and parameterizes them.

4. Scope of the academic discipline (module) and forms of control *

Scope of classes: total: <u>3 CP 108 academic hours</u>	OFO, in acad. hours
Contact work:	
Lectures/from them practical training	
Laboratory work/from them practical training	-
Practical training/of which practical training	32
Independent work	76
Forms of control	
Exam	-
Credit	Yes

Credit with a grade	-
Course work	no

* The discipline (module) provides for the use of e-learning, distance educational technologies

5. The content of the discipline, structured by topics (sections) with an indication of the number of academic hours and types of classes allotted for them

№	Section (topic) of the discipline and summary	Emerging competencies, indicators	Full-time				Current Forms control Academic Performance
			Contact work of students with the teacher / of them in the form of practical training, hours			Independent work, hours	
			Lectures	Practical exercises	Laboratory work		
1.	Architecture and principles of building intelligent IDS: 1. Comparative analysis of signature and anomalous intrusion detection methods. 2. The building blocks of intelligent IDS are sensors, analyzers, and decision modules. 3. Topological schemes for the placement of intelligent detection systems in the corporate network.			2		8	Interview
2.	Preparation and analysis of datasets for AI training: 1. An overview of the network security reference datasets: NSL-KDD, CIC-IDS2017, and UNSW-NB15. 2. Network data preprocessing methods include cleansing, normalization, and feature coding. 3. The problem of class imbalance in network traffic and ways to solve it.			2		8	Interview

3.	Feature Engineering from network traffic: 1. Differences between batch analysis and Flow-based analysis. 2. Traffic statistics for DDoS detection and port scanning. 3. Feature Selection methods and data redundancy control.			4		8	Interview
4.	Comparative analysis of classical machine learning algorithms for IDS: 1. Use ensemble methods (Random Forest) to improve the stability of attack detection. 2. Using the Support Vector Method (SVM) to find the boundaries between norm and invasion. 3. Evaluation of the performance of classical classification algorithms in high-speed networks.			4		8	Interview
5.	Metrics for assessing the quality of intelligent IDS: 1. Confusion Matrix and analysis of errors of the first and second types in cybersecurity. 2. Interpret Precision, Recall, and F1-score metrics when working with malicious traffic. 3. Analysis of ROC and PR curves as tools for assessing the effectiveness of intelligent protection.			4		8	Interview
6.	Deep Learning for Network Application and Database Protection: 1. Multilayer neural network architectures for deep analysis of HTTP requests. 2. Use of recurrent networks (RNN/LSTM) to detect anomalies in SQL transaction sequences. 3. Methods of tokenization and vector representation of text requests to web servers.			4		8	Interview

7.	Intelligent traffic analysis at different layers of the OSI model: 1. Features of the analysis of anomalies in packet headers and protocol flags at the network and transport layers. 2. Intelligent detection of hidden channels (tunneling) at the application layer of the OSI model. 3. Construction of defense-in-depth based on a cascade of neural network models.			4		8	Interview
8.	Organization of additional training of models and adaptation to new threats: 1. The problem of degradation of AI accuracy (Model Drift) and changes in the profile of network behavior (Concept Drift). 2. Active Learning methodology with expert participation in the IDS adaptation loop. 3. MLOps principles for automating the life cycle of neural network security models.			4		8	Interview
9.	Stress testing of intelligent IDS using adversarial AI methods: 1. The concept of Adversarial Examples to bypass neural network detectors. 2. Classification of adversarial influences: Evasion attacks and Poisoning attacks. 3. Adversarial Training methods to increase the robustness of protection systems.			4		12	Interview
	TOTAL for the 6th semester			32		76	
	TOTAL			32		76	

6. Fund of assessment tools for current monitoring of progress and intermediate certification of students in the discipline

The Assessment Tools Fund (ACF) for the current monitoring of progress and intermediate certification of students is based on the list of competencies to be mastered with an indication of the stages of their formation in the process of mastering the discipline (module). The CSF provides objective control over the achievement of the planned learning outcomes. The CSF includes:

- description of indicators and criteria for assessing competencies at various stages of their formation, description of assessment scales;
- methodological materials that determine the procedures for assessing knowledge, skills, and (or) experience of activity, characterizing the stages of competence formation;

- standard control tasks and other materials necessary to assess knowledge, skills and the level of mastery of the formed competencies in the process of mastering the discipline (module).

The FAT is an appendix to this program of the discipline (module).

7. Methodical instructions for students on mastering the discipline

Starting work, each student should take into account the following provisions.

The discipline is built on a thematic principle, each topic is a logically complete section.

The lecture material is devoted to the consideration of the key, basic provisions of the courses and the explanation of educational tasks submitted for independent work of students.

Practical classes are conducted in order to consolidate the learned information, to acquire skills for its application in solving practical problems in the relevant subject area.

Independent work of students is aimed at independent study of additional material, preparation for practical classes, as well as the performance of all types of independent work.

For the successful development of the discipline, it is necessary to perform all types of independent work, using the recommended sources of information.

8. Educational, methodological and information support of the discipline

8.1. List of basic and additional literature necessary for mastering the discipline

8.1.1. List of basic literature:

1. Averchenkov V. I., Rytov M. Yu., Kuvyklin A. V., Gainulin T. R. *Metody i sredstva inzhenerno-tehnicheskogo zashchity informatsii* [Methods and Means of Engineering and Technical Information Protection]. 2nd ed., ster. Moscow, Flinta Publ., 2011. 187 p. http://old.biblioclub.ru/93275_Metody_i_sredstva_inzhenerno_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html

2. Chipiga, A. F. (SevKavGTU). *Multichannel measuring systems for monitoring the safety of objects: textbook*. textbook / A. F. Chipiga, V. V. Fedorenko, I. V. Fedorenko; FBGOU Sev.-Kav. Gos. Techn. University. - Stavropol : SevKavSTU Publishing House, 2011. - 126 p. : ill. - References: p. 123-128 (58 titles)

3. Chipiga, A. F. *Informatsionnaya bezopasnost' avtomatizirovannykh sistem* [Information security of automated systems]. Textbook. Moscow, Gelios ARV Publ., 2010. 336 p. (in Russian).

4. Melnikov V. P., Kleymenov S. A., Petrakov A. M. *Informatsionnaya bezopasnost' i zashchita informatsii* [Information security and information protection]. Melnikov V. P., Kleymenov S. A., Petrakov A. M. ; ed. by S. A. Kleymenov. – 3rd ed., ster. – Moscow : Academy, 2008. – 331 p.

8.1.2. List of educational and methodological support for students' independent work in the discipline:

1. Chipiga, A. F. (SevKavGTU). *Information Security: Textbook. Manual (Practicum)* / A. F. Chipiga, M. A. Lapina, V. V. Belous ; M-vo obrazovaniya i nauki Ros. Federatsii, GOU VPO Sev.-Kav. Gos. Techn. University. – Stavropol : SevKavGTU, 2009. – 282 p.

2. Sergeeva Y. S. *Information Protection. Lecture Notes. Textbook*. - Moscow: A-Prior, 2011. - 128 p. http://old.biblioclub.ru/72670_Zaschita_informatsii_Konspekt_leksii_Uchebnoe_posobie.html

3. Sychev Y. N., *Fundamentals of Information Security. Educational and Practical Manual* - Moscow: Eurasian Open Institute, 2010. - 328 p. http://old.biblioclub.ru/90790_Osnovy_informatsionnoi_bezopasnosti_Uchebno_prakticheskoe_posobie.html

4. Shangin V. F., *Protection of Computer Information. Effective Methods and Means* - Moscow: DMK Press, 2010. - 544 p. APPROVED BY the UMO of universities on university polytechnic education as a textbook for students of higher educational institutions. http://old.biblioclub.ru/86475_Zaschita_kompyuternoii_informatsii_Effektivnye_metody_i_sredstva.html

8.2. List of educational and methodological support for students' independent work in the discipline

1. Federal Law "On Information, Information Technologies and Information Protection"
2. The concept of national security
3. Federal Law of the Russian Federation "On Security"

8.3. List of resources of the information and telecommunication network "Internet" necessary for mastering the discipline

1. <http://biblioclub.ru/> – University Library Online "Biblioclub"

9. List of information technologies used in the implementation of the educational process in the discipline, including a list of software and information reference systems

When giving lectures, computer equipment is used, demonstration of presentation multimedia materials. In practical classes, students defend reports on the work that they perform independently or in a team using computer equipment and Internet technologies

Information reference systems:

Information and reference and information and legal systems used in the study of the discipline:

Information and reference and information and legal systems used in the study of the discipline:

1. <http://catalog.ncfu.ru/catalog/ncfu> – Official website of the Scientific Library of the FGAOU HE NCFU.
2. <http://www.consultant.ru> – Official website of Consultant Plus
3. <https://www.mnr.gov.ru> – Official website of the Ministry of Natural Resources and Environment of the Russian Federation
4. Information and Legal Portal "Garant" - <http://www.garant.ru/>

Software:

1. Viola Workstation 10
2. Alt Workstation K
3. Viola "Server"
4. Office software package - P7-Office

10. Description of the material and technical base necessary for the implementation of the educational process in the discipline

Lectures	Classroom for training sessions, equipped with multimedia equipment and technical teaching aids.
Practical exercises	The computer class is equipped with educational furniture for 15 seats and technical teaching aids: a magnetic marker board, a projector, personal computers. There is a necessary set of licensed software.
Independent work	Room for independent work of students, equipped with computer equipment with the ability to connect to the Internet and the ability to access the electronic information and educational environment of the university
Practical training	It is carried out in the structural divisions of the university and (or) in organizations that carry out activities in the profile of the relevant educational program, including its structural subdivision

11. Features of mastering the discipline by persons with disabilities

Students with disabilities are provided with special textbooks, teaching aids and didactic materials, special technical teaching aids for collective and individual use, the services of an assistant (assistant) who provides students with the necessary technical assistance, as well as the services of sign language interpreters and typhlo-sign interpreters.

The development of the discipline by students with disabilities can be organized together with other students, as well as in separate groups.

The development of the discipline by students with disabilities is carried out taking into account the peculiarities of psychophysical development, individual capabilities and health status.

In order to ensure the accessibility of higher education under the educational program by persons with disabilities when mastering the discipline, the following is ensured:

- 1) for visually impaired persons:
 - the presence of an assistant who provides the student with the necessary technical assistance, taking into account individual characteristics (helps to take a workplace, move, read and complete the task, including by writing down by dictation),
 - written tasks, as well as instructions on the procedure for their implementation, are drawn up in enlarged font,
 - special textbooks, teaching aids and didactic materials (with large print or audio files),
 - individual uniform lighting of at least 300 lux,
 - if necessary, the student is provided with a magnifying device to complete the task;
- 2) for persons with hearing disabilities:
 - the presence of an assistant who provides the student with the necessary technical assistance, taking into account individual characteristics (helps to take a workplace, move, read and complete the task, including by writing down by dictation),
 - the availability of sound-amplifying equipment for collective use is ensured, if necessary, the student is provided with sound-amplifying equipment for individual use;
 - is provided with appropriate sound means of reproducing information;
- 3) for persons with disabilities with musculoskeletal disorders (including those with severe disorders of the motor functions of the upper extremities or the absence of upper limbs):
 - written tasks are performed on a computer with specialized software or dictated to an assistant;
 - At the request of the student, tasks can be performed orally.

12. Features of the implementation of the discipline using distance educational technologies and e-learning

According to Part 1 of Article 16 of the Federal Law of December 29, 2012 No 273-FZ "On Education in the Russian Federation", e-learning is understood as the organization of educational activities with the use of information contained in databases and used in the implementation of educational programs and information technologies, technical means, as well as information and telecommunication networks that ensure the transmission of this information through communication lines, the interaction of students and teachers. Distance educational technologies are understood as educational technologies implemented mainly with the use of information and telecommunication networks with indirect (at a distance) interaction of students and teachers.

The discipline can be implemented using distance learning technologies and e-learning in whole or in part. The components of the discipline's teaching materials (the discipline's work program, assessment and methodological materials, forms of certification), implemented using distance learning technologies and e-learning, contain an indication of their use.

When organizing educational activities with the use of distance educational technologies and e-learning, asynchronous and synchronous ways of interacting with participants in educational relations through the information and telecommunication network "Internet" may be provided.

When using distance learning technologies and e-learning, the schedule for the discipline indicates: ways of interaction between participants in educational relations through the information and telecommunication network "Internet" (videoconferencing, ET - electronic testing); links to the electronic information and educational environment of NCFU, to educational platforms and resources of other organizations to which open access is provided through the information and telecommunication network "Internet"; for synchronous learning - the time of online classes and teachers; for asynchronous learning - the authors of online courses.

When organizing intermediate certification using distance educational technologies and e-learning, the Methodological Recommendations for the Use of Technical Means Ensuring the Objectivity of Results in Conducting Interim and State Final Certification in Educational Programs of Higher Education - Bachelor's Degree Programs, Specialist Programs and Master's Degree

Programs with the Use of Distance Educational Technologies (Letter of the Ministry of Education and Science of Russia dated 07.12.2020 No MN-19/1573-AN "On the Direction of Methodological Recommendations") are used.

The implementation of the discipline using e-learning and distance learning technologies is carried out using the electronic information and educational environment of NCFU, to which students have access through the information and telecommunication network "Internet", or using the resources of other organizations, including platforms that provide services for video conferences, online meetings and distance learning (MTS-Link), as well as using the capabilities of social networks for communication between students and teachers.

Educational and methodological support of the discipline implemented with the use of e-learning and distance educational technologies includes a work program, teaching aids or a course of lectures presented in electronic form, guidelines for the implementation of various types of educational activities of students provided for by the discipline, and other educational materials posted in the information and educational environment of NCFU.