

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 Dean of the Faculty of Mathematics  
and Computer Sciences named after  
Professor N.I. Chervyakov  
T.V. Grobova

**WORK PROGRAM ON THE DISCIPLINE (MODULE)**  
INFORMATION SECURITY THEORY AND TECHNOLOGY / ТЕОРИЯ И ТЕХНОЛОГИИ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

|                             |                                               |
|-----------------------------|-----------------------------------------------|
| Training program            | 02.04.01 Mathematics and Computer<br>Sciences |
| Directivity (profile)       | Training Program for Electronic Information   |
| Year of admission           | 2026                                          |
| Mode of study               | intramural                                    |
| Implemented in the semester | 1                                             |

**Developed by**

Associate Professor of the Department  
of Information Security Organisation  
and Protection  
Orel D. V.

### 1. The purpose and objectives of mastering the discipline (module)

The purpose of mastering the discipline "Information Security Theory and Technology / Теория и технологии информационной безопасности" is to form an understanding of the Information security of the future master in the Training program 02.04.01 Искусственный интеллект..., to study basic concepts, such as methods of violating the confidentiality, integrity and availability of information; causes, types, channels of leakage and distortion of information; study of methods and means of ensuring information security.

Discipline objectives:

1. to lay the terminological foundation;
2. to teach how to properly analyze threats to information security;
3. to perform the main stages of solving information security problems;
4. to acquire skills in information security threat analysis;
5. to consider the basic general methodological principles of information security theory;
6. to study methods and means of ensuring information security, methods of violating the confidentiality, integrity and availability of information.

### 2. The place of the discipline (module) in the structure of the educational program

The discipline "Information Security Theory and Technology" refers to the mandatory part 02.04.01 Искусственный интеллект....

### 3. List of planned learning outcomes in the discipline (module) correlated with the planned outcomes of the educational program

| Competency code, description                                                                                                                                                | Indicator code, description                                                                                                                                                                                                                          | Planned learning outcomes in the discipline (module) characterizing the stages of competencies and indicators formation                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GPC-3</b><br>Capable of independently developing application software based on modern information technologies and network resources, including those of domestic origin | ID-1 <sub>GPC-3</sub> Independently creates application software products<br>ID-2 <sub>GPC-3</sub> Knows how to identify modern information technologies - including those of domestic origin - necessary for creating application software products | Independently creates application software products<br>Knows how to identify modern information technologies -including those of domestic origin - necessary for creating application software products |
| <b>UC-6</b><br>Capable of identifying and implementing priorities for one's own activities and ways to improve them based on self-assessment                                | ID-1 <sub>UC-6</sub> Prepared for self-development, self-realization, and the utilization of creative potential<br>ID-2 <sub>UC-6</sub> Identifies and implements priorities for their own activities                                                | Prepared for self-development, self-realization, and the utilization of creative potential, Identifies and implements priorities for their own activities                                               |

### 4. The scope of the academic discipline (module) and control forms\*

|                            |                    |
|----------------------------|--------------------|
| c.u. 4                     | Acad. Hours<br>144 |
| of them classroom lessons: | -                  |
| Lectures                   | -                  |
| Laboratory works           | -                  |
| Practical lessons          | -                  |

|                  |     |
|------------------|-----|
| Independent work | 112 |
| Control forms:   |     |
| Control work     | 32  |

### 5. Content of the discipline (module), structured by topics (sections) with an indication of the number of hours and types of training sessions

| No.        | Section (topic) of the discipline                           | Implemented competencies, indicators      | Contact work of students with a teacher, hours |                   |                  | Independent work, hours |
|------------|-------------------------------------------------------------|-------------------------------------------|------------------------------------------------|-------------------|------------------|-------------------------|
|            |                                                             |                                           | Lectures                                       | Practical lessons | Laboratory works |                         |
| 1 semester |                                                             |                                           |                                                |                   |                  |                         |
| 1          | Overview of international information security legislation  | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 4.00                    |
| 2          | Exploring a class of knowledge-based authentication methods | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 8.00                    |
| 3          | Exploring a class of ownership-based authentication methods | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 4.00                    |
| 4          | Research of the biometric class of authentication methods   | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 6.00                    |
| 5          | Hash functions and their application                        | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 6.00                    |
| 6          | Differentiation of access rights in Linux                   | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 6.00                    |
| 7          | File Attributes in Linux                                    | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 2.00                    |
| 8          | ACLs in Linux                                               | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | -                                              | 2                 | -                | 2.00                    |

|    |                                                                                                       |                                           |   |   |   |      |
|----|-------------------------------------------------------------------------------------------------------|-------------------------------------------|---|---|---|------|
| 9  | Protecting a Windows Server-based server                                                              | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 4.00 |
| 10 | Organizing a Linux web server and protecting it                                                       | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 8.00 |
| 11 | Analysis of major Web Application Vulnerabilities (OWASP Top 10)                                      | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 4.00 |
| 12 | Methods of protection against SQLInjection, XSS and other attacks, secure web application development | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 4.00 |
| 13 | Web Server vulnerability research using the OWASP ZAP tool                                            | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 8.00 |
| 14 | Development of measures to improve the security of the web server                                     | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 2.00 |
| 15 | Configuring an SSHconnection to a Linux server                                                        | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 4.00 |
| 16 | Protecting SSH connection to a Linux server                                                           | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 6.00 |
| 17 | Exploring the capabilitiesснифераof the Wireshark Network Packet Sniffer<br>Wireshark                 | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 2.00 |
| 18 | Exploring the Ethernet protocol using Wireshark                                                       | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 2.00 |
| 19 | Exploring IP packets using Wireshark                                                                  | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 4.00 |
| 20 | Network protection based on the Mikrotik firewall                                                     | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 6.00 |
| 21 | Configuring the Huawei Next-Generation Firewall                                                       | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2 | - | 8.00 |

|    |                                                  |                                           |   |    |   |        |
|----|--------------------------------------------------|-------------------------------------------|---|----|---|--------|
| 22 | Data Leakage Prevention systems                  | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2  | - | 4.00   |
| 23 | Security Incidents and Events Management systems | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2  | - | 4.00   |
| 24 | Security Orchestration and Automation systems    | ID-1 GPC -1<br>ID-2 GPC -1<br>ID-3 GPC -1 | - | 2  | - | 4.00   |
|    | TOTAL for the 1st semester                       |                                           | - | 32 | - | 112.00 |
|    | TOTAL                                            |                                           | - | 32 | - | 112.00 |

## **6. Assessment Tools Fund for the continuous monitoring of progress and intermediate certification of students in the discipline (module)**

The Assessment Tools Fund (ATF) for continuous monitoring of progress and intermediate certification of students in the discipline (module) "Information Security Theory and Technology / Теория и технологии информационной безопасности" is based on a list of mastered competencies with an indication of their formation stages in the process of mastering the discipline (module). ATF provides objective monitoring of the achievement of planned learning outcomes. ATF includes:

- description of indicators and criteria for assessing competencies at various stages of their formation, description of assessment scales;
- methodological materials determining the procedures for assessing knowledge, skills and (or) experience of activity that characterize the stages of competencies formation;
- standard control tasks and other materials necessary for assessing knowledge, skills and the level of the competencies formed while mastering the discipline (module).

ATF is an application to this discipline (module) program.

## **7. Methodological guidelines for students on mastering the discipline**

Getting started, each student should take into account the following provisions.

The discipline (module) is built according to the topics principle, each topic is a logically completed section.

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

Practical classes are aimed at consolidating the learned information, acquiring the skills of 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 lessons, as well as the performance of all types of independent work.

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

## **8. Teaching and learning materials on the discipline**

8.1. List of essential and supplementary literature necessary for mastering the discipline (module)

8.1.1. List of essential literature:

1. Information System Security Technologies: Textbook: A. L. Marukhlenko, L. O. Marukhlenko, M. A. Efremov [et al.]. – Moscow; Berlin: Direct Media, 2021. – 209 p.
2. Balanov A. N. Protection of information systems. Cybersecurity: a textbook for universities / A. N. Balanov. — Saint Petersburg: Lan, 2024. — 280 p.
3. Howard Rick. Cybersecurity: Key Principles. — St. Petersburg: Piter, 2024. — 320 p.: ill.

8.1.2. List of supplementary literature:

1. NIST Special Publication 800-207. Zero Trust Architecture. — <https://doi.org/10.6028/NIST.SP.800-207>
2. ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements».
3. MITRE ATT&CK® Framework "MITRE ATT&CK Matrix for Enterprise". // <https://www.thetechplatform.com/post/the-top-ten-mitre-att-ck-techniques>
4. Cybersecurity: textbook. manual / E. S. Abramov, E. S. Basan, O. Yu. Peskova, O. P. Khabarov, A. V. Epishkina, K. G. Kogos. - St. Petersburg: GUAP, 2021. - 169 p.: il. ISBN 978-5-8088-1673-2.

5. Brazhuk A. I. Network tools for Linux. 2nd ed., ispr. Moscow: National Open University "INTUIT", 2016. 148 p. Access mode: [http://biblioclub.ru/index.php?page=book\\_red&id=428794&sr=1](http://biblioclub.ru/index.php?page=book_red&id=428794&sr=1).
6. Goncharuk S. V. Administration of the Linux OS. 2nd ed., ispr. Moscow: National Open University "INTUIT", 2016. 165 p. Access mode: [http://biblioclub.ru/index.php?page=book\\_red&id=429014&sr=1](http://biblioclub.ru/index.php?page=book_red&id=429014&sr=1).
7. Belkin P. Yu., Mikhalsky O. O., Pershakov A. S. et al., Software and hardware tools for ensuring information security: Protection of programs and data: textbook, manual for universities, Moscow: Radio and Communications, 2014, 448 p. - 978-5-89035-719-9. <http://www.iprbookshop.ru/45260.html>.
8. Software and hardware tools for ensuring information security. Practicum /A.V. Dushkin, O. M. Barsukov, E. V. Kravtsov, et al. Edited by A.V. Dushkin, Moscow: Goryachaya liniya-Telekom, 2019, 412 p. (in Russian).
9. H. Karau, B. Chambers, M. Zaharia. Learning Spark: Lightning-Fast Data Analytics. - O'Reilly Media, 2020. – 373 p.
10. Poltavtseva M. A., Lavrova D. S. High-performance intrusion detection systems: a textbook. - Infra-Engineering, 2023. - 152 p.
11. Platonov V. V. Machine learning technologies in cybersecurity: textbook. manual, Moscow: Infra-Engineering, 2024, 140 p.
12. M. Collins, K. Daley. Analyze network traffic using open source tools. - "DMK Press", 2020. - 308 p.
13. Google's Secure AI Framework (SAIF). // <https://safety.google/safety/saif/>
14. NIST AI Risk Management Framework. // <https://www.nist.gov/itl/ai-risk-management-framework>
15. GDPR (General Data Protection Regulation). // <https://gdpr-info.eu/>
16. NIST SP 800-137 — "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" // <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf>
17. M. Bowen, P. Kim, D. Rocchi, D. Stringhini. Machine Learning for Cybersecurity Cookbook. – GFZ, 2019. – 68 p.

8.2. List of teaching and learning materials for independent work of students in the discipline (module)

1. 1. Methodical Guidelines for students' Independent work in the discipline "Fundamentals of information security", in electronic form.

8.3. List of the Internet resources necessary for the development of the (module)

1. <https://www.intuit.ru>, "Основы информационной безопасности / Fundamentals of information security" course

## **9. list of information technologies used in the course of educational process in the discipline (module), including a list of software and information reference systems**

For lectures, computer technology is used, presentation multimedia materials are demonstrated. In seminars and practical classes, students provide presentations prepared during self-study hours.

Information reference systems:

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

|   |                                                                                                                  |
|---|------------------------------------------------------------------------------------------------------------------|
| 1 | <a href="http://www.consultant.ru">www.consultant.ru</a> - "Consultant Plus" Reference legal system              |
| 2 | <a href="http://www.biblioclub.ru">www.biblioclub.ru</a> - "University Library Online" Electronic library system |
| 3 | <a href="https://www.iprbookshop.ru/">https://www.iprbookshop.ru/</a> - "IPRbooks" Electronic library system     |
| 4 | <a href="http://elibrary.ru">http://elibrary.ru</a> - «eLIBRARY.RU»: [Scientific electronic library].            |

Software:

|   |                                                                                                           |
|---|-----------------------------------------------------------------------------------------------------------|
| 1 | Operating system: Microsoft Windows 8: Perpetual license. Agreement No. 01-ea/13 dated February 25, 2013. |
|---|-----------------------------------------------------------------------------------------------------------|

|   |                                                                                                                                    |
|---|------------------------------------------------------------------------------------------------------------------------------------|
| 2 | Operating system: Microsoft Windows 10: Perpetual license. Agreement No. 544-21 dated 06/08/2021.                                  |
| 3 | Basic package of Microsoft Office programs (Word, Excel, PowerPoint). Microsoft Office Standard 2013: Agreement No. 01-ea/13 dated |

#### **10. Description of the material and technical support necessary for the educational process in the discipline (module)**

The material and technical base provides for all types of disciplinary and interdisciplinary training, laboratory, research work of students (portable laptop, portable projector, computers with the necessary software and Internet access).

|                   |                                                                                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lectures          | The classroom for lecture-type classes is equipped with specialized furniture and technical teaching aids that serve to present educational information to a big audience: laptop, projector. Educational and visual aids in the form of thematic presentations corresponding to the work programs of the disciplines. |
| Practical lessons | The classroom for seminar-type classes is equipped with specialized furniture and technical teaching aids that serve to present educational information: projector, interactive whiteboard. There is a connection to the Internet, access to the educational network of the university.                                |
| Independent work  | The room for independent work of students is equipped with computers with the Internet connection and access to the electronic information and educational environment.                                                                                                                                                |

#### **11. Features of mastering the discipline (module) 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 (helper) who provides students with the necessary technical assistance, as well as the services of sign language interpreters and typhoid language interpreters.

Mastering a discipline (module) by students with disabilities can be organized together with other students, as well as in separate groups.

The development of a discipline (module) by students with disabilities is carried out taking into account the characteristics of psychophysical development, individual capabilities and health status.

In order to obtain higher education according to an educational program for persons with disabilities, when mastering a discipline (module), the following is provided:

1) for people with visual impairments:

- the presence of an assistant, who provides the student with the necessary technical help, taking into account individual characteristics (helps to take a workplace, move around, read and complete a task, including recording under dictation),

- written assignments, as well as guidelines for their implementation, are made out in enlarged type,

- special textbooks, teaching aids and didactic materials (with large print or audio files),

- individual uniform illumination of at least 300 lux,

- if necessary, the student is provided with a magnifying device to complete a task;

2) for people with hearing disabilities:

- the presence of an assistant, who provides the student with the necessary technical help, taking into account individual characteristics (helps to take a workplace, move around, read and complete a task, including recording under 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;

- appropriate sound means of information reproduction are provided;

3) for persons with disabilities who have disorders of the musculoskeletal system (including those with severe impairment of motor functions of the upper limbs or the absence of upper limbs):

- written assignments are performed on a computer with specialized software or dictated to the assistant;
- at the request of the student, tasks can be performed orally.

## **12. Features of the implementation of the discipline with the use of distance learning technologies and e-learning.**

According to Part 1 of Article 16 of Federal Law No. 273-FZ of December 29, 2012 "On Education in the Russian Federation", e-learning refers to 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 its processing, ensuring the transmission of this information via communication lines, the interaction of students and teaching staff. Distance educational technologies are understood as educational technologies implemented mainly with the use of information and telecommunication networks with the indirect (at a distance) interaction of students and teaching staff.

The implementation of the discipline can be carried out using distance learning technologies and e-learning in whole or in part. The components of the curriculum of the discipline (the work program of the discipline, evaluation and methodological materials, forms of certification), implemented with the use of distance learning technologies and e-learning, contain an indication of their use.

When organizing educational activities with the use of distance learning technologies and e-learning, asynchronous and synchronous ways of implementing the interaction of participants in educational relations through the Internet information and telecommunications network can be provided.

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

When organizing intermediate certification with the use of distance educational technologies and e-learning, Methodological recommendations are used for the use of technical means that ensure the objectivity of the results when conducting intermediate and state final certification for educational programs of higher education - bachelor's degree programs, specialty programs and master's degree programs with the use of distance educational technologies (Letter of the Ministry of Education of the Russian Federation dated 07.12.2020 No. MN-19/1573-AN "On the direction of methodological recommendations").

The implementation of the discipline with the use of e-learning and distance learning technologies is carried out using the NCFU electronic information and educational environment, to which students have access via the Internet information and telecommunications network, or using the resources of other organizations, including platforms that provide services for videoconferencing, online meetings and distance learning (Bigbluebutton, Microsoft Teams, as well as using the capabilities of social networks to communicate students and teachers.

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

