

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Порохня Андрей Алексеевич
Должность: И.о. директора института перспективной инженерии
Дата подписания: 22.10.2026 13:25:38
Уникальный программный ключ:
990bea3aeec48c23bd8699e48288f8d1960c600

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION
Federal State Autonomous Educational Institution
Higher Education
"NORTH CAUCASUS FEDERAL UNIVERSITY"

APPROVED BY
Acting Director of the Institute
Advanced Engineering
Cand. Tech. Sci., Associate Professor
A.A. Porokhnya

DISCIPLINE ASSESSMENT TOOLS FUND

"Principles and Techniques of Information Security"

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

Introduction

1. Purpose

The fund of assessment tools for the discipline "Principles and Techniques of Information Security" is intended for an objective assessment of the level of competence formation.

2. The FAT is an appendix to the program of the discipline "Principles and Techniques of Information Security".

3. The developer is O.Kh. Shayakhmetov, Associate Professor of the Department of Digital, Robotic Systems and Electronics of the Institute of Advanced Engineering.

4. An examination of the FOC was carried out.

Members of the expert group:

Chairman: V.P. Mochalov, Professor of the Department of Digital, Robotic Systems and Electronics of the Institute of Advanced Engineering.

Members of the Commission:

S.V. Yakovlev, Associate Professor of the Department of Digital, Robotic Systems and Electronics of the Institute of Advanced Engineering.

S.V. Melnikov, Senior Researcher of the Interdisciplinary Training and Research Center for Agricultural Technologies, Associate Professor of the Department of Digital, Robotic Systems and Electronics of the Institute of Advanced Engineering.

Representative of the employer's organization:

Mironov V.A., General Director of Orintex LLC.

Expert opinion: The FAT for the discipline allows you to assess the level of competence formation. Start approbation.

5. The validity period of the FAT is determined by the period of implementation of the educational program.

1. Description of the criteria for assessing competence at various stages of their formation, description of assessment scales

Competency(s), indicator(s)	Levels of competence formation(s),			
	The minimum level has not been reached (Unsatisfactory) 2 points	Minimum level (satisfactory) 3 points	Intermediate level (good) 4 points	High level (excellent) 5 points
<i>Competence:</i> OPK-3. Able to apply methods of searching, storing, processing, analyzing and presenting information from various sources and databases in the required format, while observing the basic requirements of information security				
ID-1 OPK-3 understands the basic patterns of information transmission in infocommunication systems, the main types of signals used in telecommunication systems, the features of the transmission of various signals through channels and paths of telecommunication systems.	Unable to complete tasks related to this competency achievement indicator	Performs tasks at the reproductive level related to this indicator of competence achievement	Performs tasks related to this indicator of competence achievement in standard situations, making minor mistakes	Fully performs tasks related to this indicator of competence achievement, including in non-standard situations
ID-2 OPK-3 understands the principles, basic algorithms and devices of digital signal processing; the principles of building telecommunication systems of various types and methods of information distribution in communication networks.	Unable to complete tasks related to this competency achievement indicator	Performs tasks at the reproductive level related to this indicator of competence achievement	Performs tasks related to this indicator of competence achievement in standard situations, making minor mistakes	Fully performs tasks related to this indicator of competence achievement, including in non-standard situations
ID-3 OPK-3 solves data processing problems using computer technology.	Unable to complete tasks related to this competency achievement indicator	Performs tasks at the reproductive level related to this indicator of competence achievement	Performs tasks related to this indicator of competence achievement in standard situations,	Fully performs tasks related to this indicator of competence achievement

			making minor mistakes	t, including in non-standard situations
ID-4 OPK-3 builds probabilistic models for specific processes, carries out the necessary calculations within the framework of the built model.	Unable to complete tasks related to this competency achievement indicator	Performs tasks at the reproductive level related to this indicator of competence achievement	Performs tasks related to this indicator of competence achievement in standard situations, making minor mistakes	Fully performs tasks related to this indicator of competence achievement, including in non-standard situations
ID-5 OPK-3 has methods and skills for ensuring information security.	Unable to complete tasks related to this competency achievement indicator	Performs tasks at the reproductive level related to this indicator of competence achievement	Performs tasks related to this indicator of competence achievement in standard situations, making minor mistakes	Fully performs tasks related to this indicator of competence achievement, including in non-standard situations

ASSESSMENT TOOLS TO CHECK THE LEVEL OF FORMATION OF COMPETENCIES

Job Number	Correct answer	Content of the question	Competence
Form of study: Full-time Semester 6			
1.	in	Who is the main person responsible for determining the level of classification of information? a) Middle manager; b) Senior management; c) Owner; d) User	OPK -3
2.	a	Which category is the most risky for the company in terms of likely fraud and security breaches? a) Employees; b) Hackers; c) Attackers; d) Counterparties (persons working under a contract)	OPK -3
3.	in	If different groups of users with different levels of access need access to the same information, which of the following actions should management take? a) Reduce the level of security of this information to ensure its accessibility and ease of use; b) Require the signing of special permission each time a person needs access to this information; c) Improve control over the security of this information; d) Reduce the level of classification of this information	OPK -3
4.	b	What is the most important thing for management to think about when classifying data? a) The types of employees, contractors and customers who will have access to the data; b) The required level of availability, integrity and confidentiality; c) Assess the level of risk and remove countermeasures; d) Access control, which should protect the data	OPK -3
5.	g	Who is ultimately responsible for ensuring that data is classified and protected? a) Data Owners; b) Users; c) Administrators; d) Management	OPK -3
6.	in	Legal methods that ensure information security include: a) Development of hardware for providing legal data; b) Development and installation of action logs in all computer legal networks; c) Development and specification of legal regulations for ensuring security	OPK -3
7.	b	The main sources of information security threats are all listed above: a) Theft of hard drives, network connection, insiderism; b) Interception of data, theft of data, change of system architecture; c) Theft of data, bribery of system administrators, violation of work regulations	OPK -3

8.	a	The goals of information security are the timely detection and prevention of: a) unauthorized access, influence in the network; b) insider in the organization; c) emergencies	OPK -3
9.	a	The main objects of information security: a) Computer networks, databases; b) Information systems, psychological state of users; c) Business-oriented, commercial systems	OPK -3
10.	in	The main risks of information security are: a) Distortion, reduction of volume, recoding of information; b) Technical interference, disabling of network equipment; c) Loss, distortion, leakage of information	OPK -3
11.	a	The basic principles of information security include: a) Economic efficiency of the security system; b) Multi-platform implementation of the system; c) Strengthening the security of all links of the system	OPK -3
12.	b	The main subjects of information security are: a) executives, managers, administrators of companies; b) legal, state, business bodies; c) network databases, firewalls	OPK -3
13.	a	The main functions of the security system include all of the above: a) Establishing regulations, auditing the system, identifying risks; b) Installing new office applications, changing the hosting company; c) Implementing authentication, verifying user contact details	OPK -3
14.	a	The principle of information security is the principle of prevention: a) Unjustified restrictions when working in the network (system); b) Risks to the security of the network, system; c) Presumption of secrecy	OPK -3
15.	b)	The principle of the information security policy is the principle of: a) Inability to bypass the protective means of the network (system); b) Strengthening the main link of the network, system; c) Complete blocking of access in risk situations	OPK -3
16.		The concept of information security. The main components of information security.	OPK -3
17.		Basic concepts of threats.	OPK -3
18.		Legislative level of information security.	OPK -3
19.		Standards and specifications in the field of information security.	OPK -3
20.		Administrative level of information security.	OPK -3
21.		Procedural level of information security.	OPK -3
22.		Basic concepts of the software and hardware level of information security.	OPK -3
23.		Security system architecture.	OPK -3

24.		Basic principles of cryptographic protection of information.	OPK -3
25.		Asymmetric cryptosystems.	OPK -3
26.		Symmetric cryptosystems.	OPK -3
27.		Basic concepts and classification of malware. Basics of combating malware.	OPK -3
28.		Typical remote attacks in global computer networks.	OPK -3
29.		What do engineering and technical means of information security include?	OPK -3
30.		Ensuring the security of systems that are part of global computer networks.	OPK -3

2. Description of the rating scale

Within the framework of the rating system, students' progress in each discipline is assessed during current control and intermediate certification.

3. Criteria for assessing competencies

An "excellent" grade is given to a student if he/she fully and accurately performs the tasks of assessment tools in the discipline related to this competence (indicators of competence achievement), while demonstrating at a high level the ability to solve standard and non-standard applied practical tasks in the field of information security in information and communication systems.

A grade of "good" is given to a student if he/she, making minor mistakes, performs the tasks of assessment tools in the discipline related to this competence (indicators of competence achievement), while demonstrating at an average level the ability to solve only standard applied practical tasks in the field of information security in information and communication systems.

A "satisfactory" grade is given to a student if he/she performs the tasks of assessment tools in the discipline related to this competence (indicators of competence achievement), while demonstrating at a minimum level the ability to solve standard applied practices in the field of information security in information and communication systems.

An "unsatisfactory" grade is given to a student if he/she, performing the tasks of assessment tools in the discipline, does not reach the minimum level of competence formation (indicators of competence achievement), while not demonstrating the ability to solve standard applied practical tasks in the field of information security in information and communication systems, makes gross mistakes that he cannot correct even with the help of leading questions from the teacher.