

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

A.A. Porokhnya

**DISCIPLINE ASSESSMENT TOOLS FUND**  
**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                                                                     |

## Introduction

1. Purpose: The fund of assessment tools is designed to provide a methodological basis for the organization and conduct of current control in the discipline "Network intrusion detection systems based on artificial intelligence". Current control in this discipline is a type of systematic testing of students' knowledge, skills, and abilities. The tasks of current control are to obtain primary information about the progress and quality of mastering competencies, as well as to stimulate regular purposeful work of students. To form a certain level of competencies.

2. FOS is an appendix to the program of the discipline "Network intrusion detection systems based on artificial intelligence"

3. Developer: Peleshenko V.S., Associate Professor of the Department of Computational Mathematics and Cybernetics of the Faculty of Mathematics and Computer Science named after Professor N.I. Chervyakov.

4. An examination of the FOC was carried out.

Members of the expert group:

Chairman: N.Y. Bratchenko, Chairman of the CMT of the Institute of Advanced Engineering, Associate Professor of the Department of Digital, Robotic Systems and Electronics of the Institute of Advanced Engineering.

Members of the Commission:

V.P. Mochalov, 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 assessment criteria at various stages of their formation, description of assessment scales**

| Competency(s),<br>indicator(s)                                                                                                                                                                                                                                                                                                              | Levels of competence formation(s),                                                                                                                                    |                                                                                                                                                    |                                                                                                                                                       |                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                             | The minimum level has not been reached (Unsatisfactory)<br>2 points                                                                                                   | Minimum level (satisfactory)<br>3 points                                                                                                           | The minimum level has not been reached (Unsatisfactory)<br>2 points                                                                                   | High level (excellent)<br>5 points                                                                                                             |
| <i>Competency: UK-3 Able to carry out social interaction and fulfill his role in the team</i>                                                                                                                                                                                                                                               |                                                                                                                                                                       |                                                                                                                                                    |                                                                                                                                                       |                                                                                                                                                |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-1 <sup>UK-3</sup> participates in interpersonal and group interaction, using an inclusive approach, effective communication                                                                                                                                        | Does not participate in interpersonal and group interaction, using an inclusive approach, effective communication                                                     | Partially participates in interpersonal and group interaction, using an inclusive approach, effective communication                                | participates in interpersonal and group interaction, using an inclusive approach, effective communication                                             | Actively participates in interpersonal and group interaction, using an inclusive approach, effective communication                             |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-2 <sup>UK-3</sup> 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 | Does not implement effective methods of teamwork to obtain optimal work results and analyze them. Poorly applies information technologies and foresight technologies. | Partially applies effective methods of teamwork to obtain optimal work results and their analysis. Applies information and foresight technologies. | Applies effective methods of teamwork to obtain optimal work results and their analysis. Applies information technologies and foresight technologies. | Fully applies effective methods of teamwork to obtain optimal work results and their analysis. Applies information and foresight technologies. |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-3 <sup>UK-3</sup> ensures the fulfillment of tasks based on monitoring teamwork and timely response to significant deviations                                                                                                                                      | Does not perform the assigned tasks of the practice, and also does not ensure their implementation based on monitoring of teamwork.                                   | He does not fulfill the tasks of the practice insufficiently, and also partially ensures their implementation based on the monitoring of teamwork. | Performs the assigned tasks of the practice, as well as ensures their implementation based on the monitoring of teamwork.                             | Independently performs the assigned tasks of the practice, and also fully ensures their implementation based on the monitoring of teamwork.    |
| <i>Competence: UK-4 Able to carry out business communication in oral and written forms in the state language of the Russian Federation and foreign language(s)</i>                                                                                                                                                                          |                                                                                                                                                                       |                                                                                                                                                    |                                                                                                                                                       |                                                                                                                                                |

|                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Learning outcomes in the discipline (module):</p> <p><i>Indicator:</i></p> <p>ID-1 <sup>UK-4</sup> 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;</p>                                                           | <p>Does not cope with the fulfillment of the tasks of practice and the choice of 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</p>                       | <p>Partially 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</p>                                     | <p>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</p>                                                                   | <p>Fulfills the tasks of the practice in full, 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</p>                               |
| <p>Learning outcomes in the discipline (module):</p> <p><i>Indicator:</i></p> <p>ID-2 <sup>UK-4</sup> 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;</p> | <p>Does not sufficiently search 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 increase the effectiveness of professional interaction</p> | <p>Partially 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 increase the efficiency of professional interaction</p> | <p>Applies effective methods of searching 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 increase the efficiency of professional interaction</p> | <p>Fully 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 increase the efficiency of professional interaction</p> |
| <p>Learning outcomes in the discipline (module):</p> <p><i>Indicator:</i></p> <p>ID-3 <sup>UK-4</sup> evaluates the effectiveness of the applied communication technologies in professional interaction in the state and foreign languages, and selects the optimal ones.</p>                                                                     | <p>Does not fulfill the tasks of practice, and also does not evaluate the effectiveness of the applied communicative technologies in professional interaction in the state and foreign languages,</p>                                                                           | <p>Does not sufficiently fulfill the tasks of practice, and also partially evaluates the effectiveness of the applied communicative technologies in professional interaction in the state and foreign languages, makes a choice of optimal</p>                     | <p>Fulfills the tasks of the practice, and also evaluates the effectiveness of the applied communication technologies in professional interaction in the state and foreign languages, and selects the optimal</p>                                                                      | <p>Independently performs the assigned tasks of practice, as well as fully ensures the assessment of the effectiveness of the applied communicative technologies in professional interaction in the state and foreign languages,</p>                           |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | makes a choice of optimal                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                       | makes a choice of optimal                                                                                                                                                                                                                   |
| <i>Competency: UK-5 Able to perceive the intercultural diversity of society in socio-historical, ethical and philosophical contexts</i>                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>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;                                                                                                                                                                                                                                                                         | Does not cope with the search for the information necessary to solve the tasks, the identification and analysis of information about the cultural characteristics and traditions of various social groups, for the choice of a strategy for interaction with their carriers | Partially 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 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 | Fully 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 interaction with their carriers |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>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; | Does not sufficiently fulfill the tasks of practice, does not demonstrate respect for the historical heritage and socio-cultural traditions of various social groups                                                                                                        | Partially fulfills the tasks of the practice, demonstrates respect for the historical heritage and socio-cultural traditions of various social groups                                                                                           | Fulfilling the tasks of the practice, he demonstrates a respectful attitude to the historical heritage and socio-cultural traditions of various social groups                                                                         | Fully fulfilling the tasks of the practice, he demonstrates a confident and respectful attitude to the historical heritage and socio-cultural traditions of various social groups                                                           |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-3 UK-5 chooses ways of constructive interaction with people,                                                                                                                                                                                                                                                                                                                                                                                                                | Does not fulfill the tasks of practice, and also does not choose ways of                                                                                                                                                                                                    | Does not fulfill the tasks of the practice insufficiently, and also partially chooses ways of                                                                                                                                                   | Fulfilling the tasks of the practice, chooses ways of constructive interaction with                                                                                                                                                   | Independently performs the tasks of the practice, as well as confidently and correctly                                                                                                                                                      |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                      |                                                                                                                                                                                          |                                                                                                                                                                      |                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| taking into account their socio-cultural characteristics, in order to successfully perform professional tasks and strengthen social integration;                                                                                                                                                                                                                                                                                               | constructive interaction with people, taking into account their socio-cultural characteristics in order to successfully perform professional tasks and strengthen social integration | constructive interaction with people, taking into account their socio-cultural characteristics, in order to successfully perform professional tasks and strengthen social integration    | people, taking into account their socio-cultural characteristics in order to successfully perform professional tasks and strengthen social integration               | 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 |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-4 <sup>UK-5</sup> 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, understands the relationship between the diversity of worldviews and the course of development of history, science, human ideas about nature, society, cognition and oneself. | Does not analyze 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         | Does not confidently analyze 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 and the prospects for its development | Independently and confidently 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   |
| <i>Competency: PC-7. Capable of administering remote access security tools (operating systems and specialized protocols)</i>                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                      |                                                                                                                                                                                          |                                                                                                                                                                      |                                                                                                                                                                                                      |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-1PC-7 understands and uses the basic principles, protocols and software cryptographic tools for ensuring the information security of network devices                                                                                                                                                                                                                  | Does not understand and does not use the basic principles, protocols and software cryptographic tools for ensuring the information security of network devices                       | Partially understands and insufficiently uses the basic principles, protocols and software cryptographic tools for ensuring the information security of network devices                  | Understands and uses the basic principles, protocols, and software cryptographic tools for ensuring the information security of network devices                      | Clearly and confidently understands and uses the basic principles, protocols and software cryptographic tools to ensure the information security of network devices                                  |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-2PC-7 understands the general principles of operation and                                                                                                                                                                                                                                                                                                             | Does not understand the general principles of operation and architecture of                                                                                                          | Partially understands the general principles of operation and architecture of hardware,                                                                                                  | Understands the general principles of functioning and architecture of hardware,                                                                                      | Fully understands the general principles of operation and architecture of                                                                                                                            |

|                                                                                                                                                                                                                                                           |                                                                                                                                                                              |                                                                                                                                                                                      |                                                                                                                                                                               |                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| architecture of hardware, software and hardware of the administered network; protocols of the channel, network, transport and application levels of the model of interaction of open systems                                                              | hardware, software and hardware of the administered network; protocols of the channel, network, transport and application layers of the open systems interaction model       | software, and software and hardware of the administered network; protocols of the channel, network, transport and application layers of the open systems interaction model           | software and software and hardware of the administered network; protocols of the channel, network, transport and application layers of the open systems interaction model     | 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                |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>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 | Does not use software, hardware and software and hardware to protect network devices from unauthorized access;                                                               | Partially 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 | Actively uses software, hardware and software and hardware to protect network devices from unauthorized access; confidently adjusts the parameters of modern software and hardware firewalls       |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-4PC-7 connects and configures modern remote access security tools (operating systems and specialized protocols); works with control and measurement hardware and software.       | Does not connect and configures modern remote access security tools (operating systems and specialized protocols); works with control and measurement hardware and software. | Partially able to connect and configure modern remote access security tools (operating systems and specialized protocols); works with control and measurement hardware and software. | Connects and configures modern remote access security tools (operating systems and specialized protocols); works with control and measurement hardware and software.          | Independently and confidently connects and configures modern remote access security tools (operating systems and specialized protocols); works with control and measurement hardware and software. |
| Learning outcomes in the discipline (module):<br><i>Indicator:</i><br>ID-5PC-7 installs additional software products to ensure remote access security and parameterization.                                                                               | Does not install additional remote access security products and parameterize them.                                                                                           | Partially installs and parameterizes additional remote access security software.                                                                                                     | Installs and parameterizes additional remote access security software.                                                                                                        | Actively and independently installs additional software products to ensure remote access security and parameterizes them.                                                                          |

Assessment of the level of competence in the discipline is carried out on the basis of the "Regulation on the current monitoring of progress and intermediate certification of students in educational programs of higher education - bachelor's programs, specialist programs, master's programs - in the Federal State Autonomous Educational Institution of Higher Education "North Caucasus Federal University" in the current edition.

## ASSESSMENT TOOLS FOR CHECKING THE LEVEL OF COMPETENCE FORMATION

| Job Number | Correct answer | Content of the question                                                                                                                                                                                                                                      | Competence             |
|------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|            |                | <b>Form of study: full-time, 6th semester</b>                                                                                                                                                                                                                |                        |
| 2.         | b              | What is the main advantage of intelligent IDS over signature IDS?<br>a) Faster packet processing speed<br>b) Ability to detect zero-day attacks<br>c) Easy to set up rules manually                                                                          | UK-3, UK-4, UK-5, PK-7 |
| 3.         | b              | What is the essence of the anomalous intrusion detection method?<br>a) In search of exact matches with the database of known viruses<br>b) Identification of deviations from the profile of normal network behavior<br>c) Blocking all encrypted connections | UK-3, UK-4, UK-5, PK-7 |
| 4.         | a              | What stage in the work of AI allows you to form a space of signs of legitimate activity?<br>a) Training phase<br>b) Inference stage<br>c) Packet capture phase                                                                                               | UK-3, UK-4, UK-5, PK-7 |
| 5.         | b              | What is the process of converting raw traffic (.pcap) into a structured view for AI called?<br>a) Defragmentation<br>b) Feature Extraction<br>c) Encapsulation                                                                                               | UK-3, UK-4, UK-5, PK-7 |
| 6.         | in             | Which Python library is most commonly used for primary processing of network data and working with tables?<br>a) Matplotlib<br>b) PyTorch<br>c) Pandas                                                                                                       | UK-3, UK-4, UK-5, PK-7 |
| 7.         | a              | Why is network data normalized before being fed into the neural network?<br>a) To bring different numerical features to a single range (for example, [0, 1])<br>b) To remove payload from traffic<br>c) To encrypt IP addresses                              | UK-3, UK-4, UK-5, PK-7 |
| 8.         | b              | What is One-Hot Encoding in the context of preparing a dataset?<br>a) Removing duplicates from the training sample                                                                                                                                           | UK-3, UK-4, UK-5, PK-7 |

|     |   |                                                                                                                                                                                                                                         |                        |
|-----|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|     |   | b) A method for converting categorical data (e.g., protocol names) into numeric vectors<br>c) Data Compression to Save Disk Space                                                                                                       |                        |
| 9.  | a | What is the most common data problem for network security?<br>a) Strong class imbalance (norms are much higher than attacks)<br>b) Lack of protocols in traffic<br>c) Excess encrypted data                                             | UK-3, UK-4, UK-5, PK-7 |
| 10. | b | What is meant by the term "Flow"?<br>a) One single IP packet<br>b) Statistics of a group of packets within one session (IP, ports, protocol)<br>c) Internet speed in megabits                                                           | UK-3, UK-4, UK-5, PK-7 |
| 11. | b | What is the most informative sign of traffic for detecting a SYN-flood DDoS attack?<br>a) IP header length<br>b) Frequency of packets with the SYN flag set<br>c) HTTP protocol version number                                          | UK-3, UK-4, UK-5, PK-7 |
| 12. | a | What is the packet payload entropy calculation used for?<br>a) To identify encrypted botnet control channels<br>b) To determine the geographical location of the server<br>c) To check the integrity of the cable system                | UK-3, UK-4, UK-5, PK-7 |
| 13. | b | What is the "curse of dimensionality" in machine learning?<br>a) Too large a .pcap file<br>b) A decrease in speed and accuracy due to an excessive number of unimportant features<br>c) In the physical limitation of the amount of RAM | UK-3, UK-4, UK-5, PK-7 |
| 14. | a | Which classical machine learning algorithm builds logical rules based on features?<br>a) Decision Tree<br>b) Method of k-nearest neighbors<br>c) Logistic regression                                                                    | UK-3, UK-4, UK-5, PK-7 |
| 15. | b | What is Random Forest?<br>a) Visualization of the network structure<br>b) An ensemble of many decision trees<br>c) Method of accidental removal of suspicious packets                                                                   | UK-3, UK-4, UK-5, PK-7 |
| 16. | a | What is the problem of the Support Vector Method (SVM) in IDS?<br>a) Search for the optimal boundary (hyperplane) between the "norm" and "attack"                                                                                       | UK-3, UK-4, UK-5, PK-7 |

|     |   |                                                                                                                                                                                                                                                                                                                     |                        |
|-----|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|     |   | <p>classes</p> <p>b) Automatic generation of new passwords</p> <p>c) Counting the number of active nodes in the network</p>                                                                                                                                                                                         |                        |
| 17. | b | <p>Why might the Accuracy metric be useless for evaluating IDS?</p> <p>a) It is too difficult to calculate</p> <p>b) It can show a high result with a complete omission of rare attacks against the background of a large volume of the norm</p> <p>c) It does not take into account the speed of the processor</p> | UK-3, UK-4, UK-5, PK-7 |
| 18. | b | <p>What metric shows the system's ability to find all real attacks?</p> <p>a) Precision</p> <p>b) Recall</p> <p>c) Speed</p>                                                                                                                                                                                        | UK-3, UK-4, UK-5, PK-7 |
| 19. | b | <p>What is a False Positive?</p> <p>a) Missed attack that the system considers normal</p> <p>b) Mistakenly blocking a legitimate user mistaken for an attacker</p> <p>c) Successful intrusion detection</p>                                                                                                         | UK-3, UK-4, UK-5, PK-7 |
| 20. | a | <p>What kind of error (False Negative) is considered the most critical for security?</p> <p>a) Mistake of the second type (omission of a real attack)</p> <p>b) Error of the first type (false alarm)</p> <p>c) Interface configuration error</p>                                                                   | UK-3, UK-4, UK-5, PK-7 |
| 21. | b | <p>What characterizes the area under the ROC curve (AUC value)?</p> <p>a) Amount of RAM required for the model</p> <p>b) A universal indicator of classification quality that does not depend on the probability threshold</p> <p>c) Number of layers in a neural network</p>                                       | UK-3, UK-4, UK-5, PK-7 |
| 22. | b | <p>Which neural network architecture is best suited for analyzing sequences of actions (transaction chains)?</p> <p>(a) Convolutional Network (CNN)</p> <p>b) Recurrent network (RNN/LSTM)</p> <p>c) Linear regression</p>                                                                                          | UK-3, UK-4, UK-5, PK-7 |
| 23. | a | <p>Why do deep neural networks use a Dropout layer?</p> <p>a) To prevent overlearning by accidentally shutting down neurons during learning</p>                                                                                                                                                                     | UK-3, UK-4, UK-5, PK-7 |

|     |    |                                                                                                                                                                                                                                               |                        |
|-----|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|     |    | b) To speed up packet transmission through the network card<br>c) To remove viruses from traffic                                                                                                                                              |                        |
| 24. | b  | What is tokenization in the context of web application security?<br>(a) Issuance of digital keys to users<br>b) Converting text queries (for example, SQL) into a numerical format for a neural network<br>c) Session Time Limitation         | UK-3, UK-4, UK-5, PK-7 |
| 25. | in | At what level of the OSI model does the intelligent IDS analyze the contents (payload) of packets?<br>a) On the network (L3)<br>b) On transport (L4)<br>c) On the application (L7)                                                            | UK-3, UK-4, UK-5, PK-7 |
| 26. | a  | What technology allows AI to detect hidden data channels within permitted protocols?<br>a) Entropy and tunneling analysis<br>b) MAC address verification<br>c) Filtering by Ports                                                             | UK-3, UK-4, UK-5, PK-7 |
| 27. | b  | What is "Model Drift"?<br>a) Physical server failure<br>b) Decrease in AI accuracy over time due to changing network traffic patterns<br>c) Signature database overflow                                                                       | UK-3, UK-4, UK-5, PK-7 |
| 28. | b  | What is Active Learning?<br>a) In training a neural network without human participation<br>b) In the transfer of dubious traffic samples for marking to a human expert for additional training of the model<br>c) In Continuous Port Scanning | UK-3, UK-4, UK-5, PK-7 |
| 29. | b  | What is the adversarial attack aimed at the AI training phase called?<br>a) Evasion attack<br>b) Poisoning attack<br>c) Social engineering                                                                                                    | UK-3, UK-4, UK-5, PK-7 |
| 30. | a  | What is an Adversarial Example in network traffic?<br>a) A packet modified so that the AI classifies the attack as the norm<br>b) A package with an incorrect checksum<br>c) Case study from the official dataset                             | UK-3, UK-4, UK-5, PK-7 |

|     |  |                                                                                                               |                        |
|-----|--|---------------------------------------------------------------------------------------------------------------|------------------------|
| 31. |  | What is the fundamental difference between signature and anomalous intrusion detection methods?               | UK-3, UK-4, UK-5, PK-7 |
| 32. |  | What are the main modules included in the Intelligent IDS architecture?                                       | UK-3, UK-4, UK-5, PK-7 |
| 33. |  | Why are intelligent systems considered more effective against zero-day attacks?                               | UK-3, UK-4, UK-5, PK-7 |
| 34. |  | Which datasets are the industry standards for training AI in network security?                                | UK-3, UK-4, UK-5, PK-7 |
| 35. |  | Why do you need to preprocess the data (clean and normalize) before you start training the model?             | UK-3, UK-4, UK-5, PK-7 |
| 36. |  | Why can't categorical features (for example, protocol names) be submitted to the neural network in text form? | UK-3, UK-4, UK-5, PK-7 |
| 37. |  | What is class imbalance in network traffic and how does it affect the quality of AI training?                 | UK-3, UK-4, UK-5, PK-7 |
| 38. |  | What is the difference between packet traffic analysis and network flows-based analysis?                      | UK-3, UK-4, UK-5, PK-7 |
| 39. |  | What are the statistical signs of traffic that allow AI to identify a DDoS attack?                            | UK-3, UK-4, UK-5, PK-7 |
| 40. |  | How does calculating payload entropy help detect hidden botnet control channels?                              | UK-3, UK-4, UK-5, PK-7 |
| 41. |  | What is the advantage of the Random Forest algorithm over a single Decision Tree?                             | UK-3, UK-4, UK-5, PK-7 |
| 42. |  | What role does the Support Vector Method (SVM) play in the classification of network states?                  | UK-3, UK-4, UK-5, PK-7 |
| 43. |  | Why is the Accuracy metric not objective for evaluating intrusion detection systems?                          | UK-3, UK-4, UK-5, PK-7 |
| 44. |  | What is a "False Positive" and what consequences does it have for the network?                                | UK-3, UK-4, UK-5, PK-7 |
| 45. |  | Which mistake is considered more critical for security: missing a real attack or a false alarm?               | UK-3, UK-4, UK-5, PK-7 |
| 46. |  | What are the benefits of using Deep Learning to analyze HTTP requests?                                        | UK-3, UK-4, UK-5, PK-7 |

|     |  |                                                                                           |                        |
|-----|--|-------------------------------------------------------------------------------------------|------------------------|
| 47. |  | Why are recurrent neural networks (RNN and LSTM) used in database protection?             | UK-3, UK-4, UK-5, PK-7 |
| 48. |  | What is Model Drift and why does the intelligent IDS need to be retrained regularly?      | UK-3, UK-4, UK-5, PK-7 |
| 49. |  | What are Adversarial Attacks on artificial intelligence systems?                          | UK-3, UK-4, UK-5, PK-7 |
| 50. |  | How does Adversarial Training help improve the resilience of IDS to traffic manipulation? | UK-3, UK-4, UK-5, PK-7 |

### Description of the grading scale

Students' progress in each discipline is assessed during current control and intermediate certification.

### Criteria for assessing competencies

An "excellent" grade is given to a student if he/she analyzes the standard tasks of professional activity, taking into account the basic requirements of information security; Performs actions to solve standard tasks of professional activity, taking into account the basic requirements of information security. Selects tasks and methods for the selection and work with personnel in the interests of ensuring information security at the facility; Selects means and methods for identifying threats when solving the tasks of professional activity.

A "good" grade is given to a student if he/she analyzes the standard tasks of professional activity and does not take into account all the basic requirements of information security; Does not perform all actions to solve standard tasks of professional activity, taking into account the basic requirements of information security. Does not choose all tasks and methods of selection and work with personnel in the interests of ensuring information security at the facility; Selects means and methods for identifying threats when solving the tasks of professional activity.

A "satisfactory" grade is given to a student if he/she analyzes standard tasks of professional activity without taking into account the basic requirements of information security; Does not perform actions to solve standard tasks of professional activity, taking into account the basic requirements of information security. Does not choose all tasks and methods of selection and work with personnel in the interests of ensuring information security at the facility; Chooses few means and methods for identifying threats when solving problems of professional activity.

The grade "unsatisfactory" is given to the student, does not analyze the standard tasks of professional activity, taking into account the basic requirements of information security; Does not perform actions to solve standard tasks of professional activity, taking into account the basic requirements of information security. Does not choose the tasks and methods of selection and work with personnel in the interests of ensuring information security at the facility; Does not choose means and methods for identifying threats when solving the tasks of professional activity.