***Final control program for the discipline***

***“****Machine learning to detect online threats****”***

***for the 2023/2024 academic year***

*spring semester​*

**Faculty of** *\_\_Information Technologies \_\_\_*

**Department** *\_\_Information Systems\_\_\_\_\_\_*

**Code and name of the educational program “***7M06301 – Information Security Systems”*

**Department**: *English*

**The level of education** *master*

**Course***: 1*

**Teacher**: *Vladislav Karyukin*

**The form of final control** is \_*oral* \_

**Exam format is** *offline*

***THEMATIC PROGRAM OF THE DISCIPLINE BASED ON THE TOPICS OF MODULES, LECTURES, SEMINARS***

1. Introduction to Network Threat Analysis
2. Network threat detection technologies
3. Performing network threat data processing operations
4. Performing an operation to retrieve data from a network threat dataset
5. Performing the vectorization operation of text data of network threats
6. Preparing network threat data for classification by machine learning models
7. Classification of network threats machine learning models
8. Classification of network threats with neural networks
9. Classification of network threats using ensemble models
10. Data analysis and processing using ChatGPT queries
11. Determination of the basic requirements for web applications
12. Preparing machine learning models for web applications
13. Configuring the web application database
14. Visualization of web application network threat detection methods
15. Complete design and testing of the web applications

***METHODOLOGICAL INSTRUCTIONS FOR COMPLETING THE FINAL CONTROL TASK ACCORDING TO THE CHOSEN FORM***

**Standard exam:** *oral*

**The exam format is** *offline***.**

About the total number of exam questions in the discipline: 15

This form is intended for final control in disciplines that develop the student’s skills to present answers and evidence of positions orally, conduct discussions with the examination committee, justify their point of view, give arguments and reasons, and contribute to the development of the student’s communicative competence. This form allows you to establish direct contact between the examination committee and the student, during which the student demonstrates the level of mastery of the educational material. Carrying out practical tasks in hardware/software development involves the use of computers and laboratory equipment to assemble and run hardware modules.

An individual survey requires detailed, coherent answers from students to a question related to the educational material being studied. Therefore, it serves as an important means of distinguishing students’ speech, memory, and thinking. To make such a test more in-depth, it is necessary to pose questions to students that require a detailed answer. Questions must be clear, precise, specific, succinct, and of an applied nature.

- purpose and expected results of the task

- the purpose – gaining skills in detecting Internet threats using machine learning models and neural networks, highlighting Internet threat anomalies, phishing, and SQL injections.

* expected results – understanding basic and advanced concepts of Internet threats, analyzing featues of Internet threat detection methods, applying application development methods with the use of machine learning models against Internet threats, building skills in working with machine learning libraries, and developing methods for analyzing the accuracy of Internet threat detection.

- form of presentation of the completed task (templates/structures, etc.)

Extended oral answers to the questions and presentation of programming code

***MAIN STEPS OF WORK ACCORDING TO INSTRUCTIONS***

**Duration**

Preparation time is 20 min

The time to answer is 15 min

The exam card contains 3 questions: 2 theory questions and 1 practical question. The corresponding maximum score is indicated in parentheses for each question and expressed as a percentage.

*Organizing an offline oral exam*

- upon entering the exam room, the student is required to provide the examiner with an identification card and sign the appearance form;

- inserting and/or changing places, leaving the audience before completing your answer to the ticket during the exam is prohibited;

- during an oral examination, the exam ticket is chosen by the examinee himself;

- at the invitation of the teacher, the student receives an examination ticket one by one;

- if necessary, there will be an opportunity to prepare to answer the questions on the exam card during preparation. And if the student is fully prepared for the questions on the exam paper, he can answer immediately;

- the examiner has the right, in order to more deeply clarify the student’s level of knowledge, to ask him additional questions and offer tasks and examples within the framework of the questions on the exam card.

**Requirements for passing the exam:**

- according to the schedule ;

- You can answer questions in any order.

- if it is discovered that unauthorized materials are being used or that students are receiving other tips, the exam may be canceled.

***GRADING POLICY – GRADING RUBRICATOR***

**Template: RUBRICATOR FOR CRITERIA ASSESSMENT OF FINAL CONTROL**

*(for standard oral/written forms)*

**Discipline:** Machine learning to detect online threats. **Form:** oral offline **Platform:** IS Univer

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.**  question | **Point**    **Criterion** | **DESCRIPTORS** | | | | |
| **"Great"** | **"Fine"** | **"Satisfactorily"** | **"Unsatisfactory"** | |
| **90-100** % | **70-89** % | **50-69** % | * 1. % | **0-24** % |
| **1-2** | Knowledge and understanding of course theory and concepts | The questions are answered comprehensively, justified, and illustrated with clear examples where necessary; the answers are presented in literate scientific language and all commands, tools, and concepts of the basic elements and operations of Internet threat detection with machine learning. | The questions were generally answered correctly but with some inaccuracies that are not of a fundamental nature. Not all basic elements and operations of big data analysis and processing are used correctly; the presentation has some incorrect statements and grammatical/stylistic errors. The answers are not adequately illustrated with examples. | Answers to questions are abstract characters; correct conclusions alternate with incorrect ones. Content blocks of all basic elements and operations of Internet threat detection with machine learning are required for  full disclosure of the topic.  Student as a whole  oriented to the topic  training course, but  has problems with  disclosure of specific  questions. | The answers are not  correspond  content of questions.  Key for educational  concept course,  contained in the questions are interpreted  wrong. | Answers on questions  absent;  ignorance revealed  or misunderstanding  student greater or  the most important part  educational material.  Breaking the rules  holding the final  control. |
| **3** | Evaluating and analyzing the applicability of the chosen method to the proposed practical problem, justifying the result obtained | The ability to integrate, validate, and analyze methods and technologies on a specific topic, basic elements and operations of Internet threat detection with machine learning, illustrating with examples and visual materials, and writing code demonstrates the ability to conduct a dialogue and engage in scientific discussion. | Integration and analysis of the application of course methods and technology with  subsequent use of visual materials to reinforce your reasoning through the use of all basic elements and operations of Internet threat detection with machine learning when reproducing knowledge; analyze the direction of the exam question. | Superficial justification of all basic elements and operations of Internet threat detection with machine learning, poor application of the main body of material in accordance with the training program with difficulties in reproducing it independently and the requirement of leading questions; | Lack of validity and analysis of the application of methods and technology of the course, difficulty in providing answers to questions of a reproducing nature. | Lack of ability to apply the course methodology when giving examples and using visual materials;  Violation of the Rules for final control. |

***REFERENCE LIST***

# Python for Everybody: Exploring Data in Python 3 by Dr. Charles Russell Severance, Sue Blumenberg, Elliott Hauser, Aimee Andrion, 2016.

# Python Cookbook: Recipes for Mastering Python 3 3rd Edition, Kindle Edition by David Beazley, Brian K. Jones, 2013.

# Programming in C# for beginners. Basic information. Alexey Vasiliev, 2018.

# C# 7 programming language and .NET and .NET Core platforms. Andrew Troelsen , Philip Jepix , 2022.

# Learning Python 5ed: Powerful Object-Oriented Programming, Mark Lutz, 2013.

# Fluent Python: Clear, Concise, and Effective Programming, Luciano Ramalho, 2015.

1. Natural Language Processing with Python and Spacy: A Practical Introduction, Yuli Vasiliev, 2021
2. Learning Scientific Programming with Python, Christian Hill, 2021