

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ  
ІМЕНІ СЕМЕНА КУЗНЕЦЯ



"ЗАТВЕРДЖУЮ"

Проректор з навчально-методичної роботи

Каріна НЕМАЦКАЛО

**ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ МІКРОПРОЦЕСОРНИХ СИСТЕМ**

робоча програма навчальної дисципліни

Галузь знань *12 Інформаційні технології*  
Спеціальність *125 Кібербезпека*  
Освітній рівень *перший (бакалаврський)*  
Освітня програма *Кібербезпека*

Статус дисципліни *обов'язкова*  
Мова викладання, навчання та оцінювання *англійська*

Завідувач кафедри  
*кібербезпеки та  
інформаційних технологій*

*Сергій ЄВСЄВ*

Харків  
2021



APPROVED

at a meeting of the Department of Cybersecurity and Information Technologies  
Protocol № 1 dated 27.08.2021

Developers:

Stanislav MILEVSKYI, Ph.D., Associate professor of CIT dept.

**Update and re-approval sheet  
for course curriculum**

Academic year	Date of the meeting at the department- developer of the course curriculum	Record number	Head of Department signature

## Abstract of the discipline

Principles of functioning of microprocessor systems. As part of the study of the discipline, methods of designing microprocessor systems based on microcontrollers are proposed.

Microprocessor technology is the fastest growing field of electronics at this stage. To successfully master it, it is necessary to master the modern principles of organization of microprocessor systems from the very beginning. Mastering the key concepts of microprocessor technology is the main task of the course. Only a comprehensive approach to hardware and software design can bring success. Features of systems of different levels of complexity and various purposes, principles of architectural decisions, ways and means of the organization of an information exchange are considered. Particular attention is paid to the principles of personal computers, as the most complex and flexible microprocessor systems that allow you to solve the most complex problems.

Another task of the course is to teach the skills of designing systems based on microcontrollers, as the most common type of microprocessor systems. For its realization descriptions of microcontrollers of family AVR, and also special software of designing are given, examples of the decision of problems of designing of several devices are considered.

It is assumed that most of the concepts introduced in this course will be the subject of more detailed consideration in other, special courses.

The thematic plan of the discipline and its content by modules and topics, plans of lectures and laboratory classes, material on consolidation of knowledge (tasks for independent work, control questions), methodical recommendations and assessment of students' knowledge are given.

**The purpose of the discipline: the purpose** teaching the discipline "Fundamentals of construction and operation of microprocessor systems" is teaching students the basics of knowledge needed by future practitioners in the field of microprocessor technology, building comprehensive information security systems based on a synthesis of organizational and technical measures in today's cyber threats.

## Characteristics of the discipline

Course	<b>2</b>
Semester	<b>1</b>
Number of ECTS credits	<b>4</b>
Form of final control	<b>Credit test</b>

## Structural and logical scheme of studying the discipline

Prerequisites	Postrequisites
Physics	Fundamentals of cryptographic protection
Higher mathematics	Information security management
	Security in information and communication systems

### Competences and learning outcomes in the discipline:

Competences	Learning outcomes
CC 1. Ability to apply knowledge in practical situations.	LO 10 - perform analysis and decomposition of information and telecommunication systems; LO 11 - perform analysis of connections between information processes on remote computer systems; information resources; LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems; LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems; LO 53 - to solve the problem of analysis of program code for the presence of possible threats.
CC 2. Knowledge and understanding of the subject area and understanding of the profession	LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge, concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components
CC 4. Ability to identify, pose and solve problems in a professional direction	LO 53 - to solve the problem of analysis of program code for the presence of possible threats.
CC 5. Ability to search, process and analyze information.	LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols
PC 2. Ability to use information and communication technologies, modern methods and models of information security and / or cybersecurity.	LO 10 - perform analysis and decomposition of information and telecommunication systems; LO 11 - perform analysis of connections between information processes on remote computer systems; LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions; LO 15 - use modern software and hardware of

	<p>information and communication technologies;  LO 17 - to ensure the processes of protection and operation of information and telecommunication (automated) systems based on practices, skills and knowledge of structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with display of relationships and information flows, processes for internal and remote components;  LO 18 - use software and software and hardware systems for the protection of information resources;  LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems;  LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems;  LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information;  LO 53 - to solve the problem of analysis of program code for the presence of possible threats.</p>
<p>PC 3. Ability to use software and software-hardware complexes of information protection means in information-telecommunication (automated) systems.</p>	<p>LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions;  LO 15 - use modern software and hardware of information and communication technologies;  LO 17 - to ensure the processes of protection and operation of information and telecommunication (automated) systems based on practices, skills and knowledge of structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with display of relationships and information flows, processes for internal and remote components;  LO 18 - use software and software and hardware systems for the protection of information resources;  LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information;  LO 53 - to solve the problem of analysis of</p>

	program code for the presence of possible threats.
PC 4. Ability to ensure business continuity in accordance with established information and / or cybersecurity policies.	<p>LO 17 - to ensure the processes of protection and operation of information and telecommunication (automated) systems based on practices, skills and knowledge of structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with display of relationships and information flows, processes for internal and remote components;</p> <p>LO 27. - solve problems of data flow protection in information, information and telecommunication (automated) systems</p> <p>LO 53 - to solve the problem of analysis of program code for the presence of possible threats.</p>
PC 5. Ability to ensure the protection of information processed in information and telecommunications (automated) systems in order to implement the established policy of information and / or cybersecurity.	<p>LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols;</p> <p>LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions;</p> <p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 18 - use software and software and hardware systems for the protection of information resources;</p> <p>LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems;</p> <p>LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of</p>

	<p>modern methods and means of cryptographic protection of the information;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>PC 6. Ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyberattacks, failures and failures of various classes and origins.</p>	<p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems;</p> <p>LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems;</p> <p>LO 37 - to measure the parameters of dangerous and interference signals during the instrumental control of information protection processes and to determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information protection system;</p> <p>LO 38 - interpret the results of special measurements using technical means, control the characteristics of information and telecommunications systems in accordance with the requirements of regulatory documents of the system of technical protection of information;</p> <p>LO 48 - implement and maintain intrusion</p>



	<p>detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>PC 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.</p>	<p>LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols;</p> <p>LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions;</p> <p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible</p>

<p>PC 10. Ability to apply methods and means of cryptographic and technical protection of information on the objects of information activities.</p>	<p>threats.</p> <p>LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions;</p> <p>LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems;</p> <p>LO 37 - to measure the parameters of dangerous and interference signals during the instrumental control of information protection processes and to determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information protection system;</p> <p>LO 38 - interpret the results of special measurements using technical means, control the characteristics of information and telecommunications systems in accordance with the requirements of regulatory documents of the system of technical protection of information;</p> <p>LO 47 - to solve problems of protection of the information processed in information and telecommunication systems with use of modern methods and means of cryptographic protection of the information;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.</p>
<p>PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and / or cybersecurity.</p>	<p>LO 10 - perform analysis and decomposition of information and telecommunication systems;</p> <p>LO 11 - perform analysis of connections between information processes on remote computer systems;</p> <p>LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols;</p> <p>LO 14 - to solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions;</p> <p>LO 15 - use modern software and hardware of information and communication technologies;</p> <p>LO 17 - to provide processes of protection and</p>

	<p>functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 18 - use software and software and hardware systems for the protection of information resources;</p> <p>LO 19 - apply theories and methods of protection to ensure information security in information and telecommunications systems;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and / or cybersecurity policies.</p>	<p>LO 13 - to analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>

## Curriculum

### Content module 1 General principles of devices and operation of microcontrollers

Topic 1. *Programmable logic integrated circuits, general information, working principle, development tools, scope.*

Topic 2. *Software and hardware architecture of IA-32 Intel processors.*

Topic 3. *Principles of using number systems.*

Topic 4. *Assembler programming language.*

Topic 5. *Assembler syntax.*

## **Content module 2. ATMEL AVR microcontroller programming.**

Topic 6. *ATMEL microcontrollers of the Mega family.*

Topic 7. *Ports of AVR ATMEL microcontrollers of the Mega family*

Topic 8. *Timers of ATMEL microcontrollers of the Mega family*

Topic 9. *Analog-to-digital converter (ADC) ATMEL family Mega*

Topic 10. *Universal serial receiver ATMEL family Mega*

Topic 11 *Implementation of standard P, PI, PID regulators on MK*

Topic 12. *Microprocessor implementation of transfer functions*

Topic 13. *Basic operations of digital signal processing (DSP)*

The list of laboratory classes, as well as questions and tasks for independent work is given in the table "Rating-plan of the discipline".

### **Teaching and learning methods**

In the course of teaching the discipline the teacher uses explanatory-illustrative (information-receptive) and reproductive teaching methods. Lectures (1-13), presentations (1-13) are used as teaching methods that are aimed at activating and stimulating the educational and cognitive activities of applicants.

### **The procedure for evaluating learning outcomes**

The system of assessment of formed competencies in students takes into account the types of classes, which according to the curriculum of the discipline include lectures and laboratory classes, as well as independent work. Assessment of the formed competencies of students is carried out according to the accumulative 100-point system. Control measures include:

1) current control, which is carried out during the semester during lectures and laboratory classes and is estimated by the amount of points scored (maximum amount - 100 points; the minimum amount that allows a student to set off - 60 points);

2) final / semester control, which is conducted in the form of a test, in accordance with the schedule of the educational process.

The procedure for the current assessment of students' knowledge.

Assessment of student knowledge during lectures and laboratory classes is carried out according to the following criteria:

- be able to describe the principles of construction, operation and application of microprocessors

- demonstrate the ability to apply methods and tools for software development of electronic devices based on microprocessors

- to design the hardware of electronic devices with microprocessors and microcomputers;

- Demonstrate knowledge of the principles of operation of microprocessors and microcontrollers.

- Practically demonstrate the features of work: with I / O ports, interruption of microprocessor systems, microcontroller timers, analog-to-digital conversion of microcontrollers, interfaces for connecting external devices.

- To develop the circuit solution of the microprocessor system according to the task.

- Offer microprocessor system software.

- Program the microcontroller.

- Check the functionality of the system using the appropriate software and prototype.

The discipline provides the following methods of current formative assessment: questioning and oral comments of the teacher on his results, instructions of teachers in the process of laboratory tasks, the formation of self-assessment skills and discussion of students completed laboratory tasks, control of independent performance of an individual task.

All work must be done independently in order to develop a creative approach to solving problems.

**Lectures:** the maximum number of points is 36 (work on lectures - 12, express survey - 24).

**Laboratory occupation:** the maximum number of points is 64 (defense of laboratory works - 40, control works - 24), and the minimum - 50.

**Individual work:** consists of the time that the applicant spends on preparation for laboratory work and on preparation for express surveys of lectures and tests for laboratory work of the discipline, in the technological map points for this type of work are not allocated.

**Final control:** is based on the scores obtained during the semester.

A student should be considered certified if the sum of points obtained from the results of the final / semester performance test is equal to or exceeds 60.

The final grade in the discipline is calculated taking into account the points obtained during the current control of the accumulative system. The total result in points for the semester is: "60 or more points - credited", "59 or less points - not credited" and is entered in the test "Statement of performance" of the discipline.

The final grade is set according to the scale given in the table "Grade scale: national and ECTS".

Forms of assessment and distribution of points are given in the table "Rating-plan of the discipline".

#### Assessment scale: national and ECTS

The sum of points for all types of educational activities	Rating ECTS	Score on a national scale	
		for exam, course project (work), practice	for offset
90 - 100	AND	perfectly	credited
82 - 89	B	fine	
74 - 81	C		
64 - 73	D		
60 - 63	E	satisfactorily	not credited
35 - 59	FX	unsatisfactorily	

#### Rating plan of the discipline

Topic	Forms and types of education		Forms of evaluation	Max ball
Topic 1	<b>Classroom work</b>			
	Lecture	Lecture "Programmable logic integrated circuits, general information, working principle, development tools, scope"	Work on lectures	1
	Laboratory lesson	Laboratory work №1. Familiarity with software products AVR studio, Proteus	performing laboratory work	
	<b>Individual work</b>			
	Questions and tasks for	Search, selection and review of		

	self-study	literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 2	<b>Classroom work</b>			
	Lecture	Lecture " <i>Software and hardware architecture of IA-32 Intel processors</i> "	Work on lectures	1
			Express survey	3
	Laboratory lesson	<i>Laboratory work №1. Features of programming in the Assembler language. Compiler directives. Stack memory. Interrupt vectors</i>	Protection of laboratory works № 1	
	<b>Individual work</b>			
Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks			
Topic 3	<b>Classroom work</b>			
	Lecture	Lecture " <i>Principles of using number systems</i> "	Work on lectures	2
			Express survey	3
	Laboratory lesson	Laboratory work № 2. Microcontroller command system. Types of operands and main flags of the result	Protection of laboratory works № 2	
	<b>Individual work</b>			
Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks			
Topic 4	<b>Classroom work</b>			
	Lecture	Lecture " <i>Assembler programming language</i> "	Work on lectures	1
	Laboratory lesson	Laboratory work №3. Interception of control. Interrupt handling	performing laboratory work	
	<b>Individual work</b>			
Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks			
Topic 5	<b>Classroom work</b>			
	Lecture	Lecture " <i>Interception of control. Interrupt handling</i> "	Work on lectures	2
			Express survey	3
Laboratory lesson	Laboratory work №3. Assembler programming language integration	Protection of laboratory works № 3		

	<b>Individual work</b>			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
<b>Topic 6</b>	<b>Classroom work</b>			
	Lecture	Lecture "ATMEL microcontrollers of the Mega family"	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 4. The main commands of the microcontroller. Data addressing.	Protection of laboratory work № 4	
			Test work 1	10
	<b>Individual work</b>			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
<b>Topic 7</b>	<b>Classroom work</b>			
	Lecture	Lecture "Ports of AVR ATMEL microcontrollers of the Mega family"	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 5. Work with external interrupts MK AVR	Protection of laboratory work № 5	5
	<b>Individual work</b>			
		Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks	
<b>Topic 8</b>	<b>Classroom work</b>			
	Lecture	Lecture "Timers of ATMEL microcontrollers of the Mega family"	Work on lectures	1
	Laboratory lesson	Laboratory work № 6. Search, selection and review of literary sources on a given topic. Preparation for laboratory classes	Express survey	3
			Protection of laboratory work № 6	5
	<b>Individual work</b>			
		Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks	
<b>Topic 9</b>	<b>Classroom work</b>			
	Lecture	Lecture "Analog-to-digital converter (ADC) ATMEL family Mega"	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 7. Work with MK AVR timers / counters	Protection of laboratory work № 7	5

			Test work № 2	10
	<b>Individual work</b>			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
<b>Topic 10</b>	<b>Classroom work</b>			
	Lecture	Lecture " <i>Universal serial receiver ATMEL family Mega</i> "	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 8. Analog-to-digital converter MK AVR	Protection of laboratory work № 8	5
	<b>Individual work</b>			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
<b>Topic 11</b>	<b>Classroom work</b>			
	Lecture	Lecture " <i>Implementation of standard P, PI, PID regulators on MK</i> "	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 9. Connection of the universal serial receiver ATMEL of the Mega family	Protection of laboratory work № 9	5
	<b>Individual work</b>			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
<b>Topic 12</b>	<b>Classroom work</b>			
	Lecture	Lecture " <i>Microprocessor implementation of transfer functions</i> "	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 10. Wire interface and temperature sensor DS18B20 3	Protection of laboratory work № 10	5
	<b>Individual work</b>			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
<b>Topic 13</b>	<b>Classroom work</b>			
	Lecture	Lecture " <i>Basic operations of digital signal processing (DSP)</i> "	Work on lectures	1



Laboratory lesson	Laboratory work № 11. The main directions of digital signal processing (DSP)	Protection of laboratory work № 11	5
<b><i>Individual work</i></b>			
Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		

### **Recommended Books**

#### **Basic**

1. Encyclopedia of Microcomputers Volume 1 - Access Methods to Assembly Language and Assemblers Edited By Allen Kent, James G. Williams 2021 by CRC Press 448 Pages
2. Evolutionary Optimization Algorithms By Altaf Q. H. Badar 2021 by CRC Press 273 Pages

#### **Optional**

3. Blockchain and IoT Integration Approaches and Applications Edited By Kavita Saini 2021 by Auerbach Publications 207 Pages
4. Assembly-Language Developer System, Version 6.1, for MS-DOS and Windows Operation System Microsoft Corporation.
5. Applied Learning Algorithms for Intelligent IoT Edited By Pethuru Raj Chelliah, Usha Sakthivel, Susila Nagarajan 2021 by Auerbach Publications 368 Pages

#### **Information resources on the Internet**

6. Work with the SPI hardware interface of microcontrollers of the AVR and MCS51 families on the example of data exchange with non-volatile memory chips of the DataFlash family (<http://www.atmel.ru/Spec/spi.htm>).
7. Site of distance learning of KhNEU named after S. Kuznets of the discipline "Fundamentals of construction and operation of microprocessor systems" <https://pns.hneu.edu.ua/course/view.php?id=8118>
8. 8-bit AVR Instruction Set Manual (<http://www.atmel.com/images/doc08S6.pdf>).