МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

" BLOCKCHAIN: ОСНОВИ ТА ПРИКЛАДИ ЗАСТОСУВАННЯ"

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"КІБЕРБЕЗПЕКА"**

Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**англійська**

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Долгова Н.Г., к.т.н., доц. кафедри КІТ,

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри –розробника РПНД	Номер протоколу	Підпис завідувача кафедри

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMIC

"APPROVED"
Vice-rector for educational and methodical work

Karina NEMASHKALO

"BLOCKCHAIN: BASICS AND EXAMPLES OF APPLICATION"

working program of the discipline

Branch of knowledge	***12 Information technologies***
Specialty	***125 Cybersecurity***
Educational level	***first (bachelor's)***
Educational program	***Cybersecurity***

Discipline status	***elective***
Language of instruction, teaching and assessment	***English***

Head of the *Department of cyber security and information technologies* — *Olha STARKOVA*

Kharkiv
2022

APPROVED
at a meeting of the Department of Cybersecurity and Information Technology
Protocol № 1 dated August 27, 2022

Developers:
Dolgova N.G., Ph.D., Assoc. Prof. of the Department of KIT

Renewal and Re-Approval Letter
work program of the academic discipline

Educational year	Date meeting department - developer of RPND	Number protocol	Signature manager department

Annotation of the discipline

Blockchain is the latest technology, interest in which has grown along with the popularity of cryptocurrencies. But there are dozens of other ways to use blockchain in isolation from cryptocurrency. Blockchain technology is considered to be the major technological breakthrough since the invention of the Internet.

The discipline "Blockchain: basics and examples of application" is an academic discipline of free choice (free magmaignor) in all specialties.

The subject of the discipline is theoretical concepts, principles of functioning and application of blockchain technologies.

The purpose of the discipline is to master the theoretical foundations of the use of blockchain technologies, the basics of cryptocurrencies and smart contracts.

The result of studying the discipline is the development of the principles of cryptographic methods in blockchain technologies; knowledge of the basic principles of cryptocurrencies; the main limitations and risks of creating and using cryptocurrencies; familiarization with the methodological foundations of the development and functioning of blockchain platforms.

Characteristics of the discipline

Course	**3**
Semester	**5**
Number of ECTS credits	**5**
Final control form	exam

Structural and logical scheme of studying the discipline

Prerequisites	Post requisites
Fundamentals of mathematical modeling	Complex course project
Fundamentals of cryptographic protection	Fundamentals of steganographic protection information
Information systems and Internet technologies	Organizational support for the protection of information
Security in information and communication Systems	

Competences and learning outcomes in the discipline

Competences	Learning outcomes
to implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; to solve the problems 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 made; to ensure the processes of protection and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge regarding structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with the reflection of relationships and information flows, processes for internal and remote components;	Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy.

use software and hardware systems for the protection of information resources; apply theories and methods of protection to ensuresecurity of information in information and telecommunication systems; to ensure the functioning of special software software to protect information from destructive software influences, destructive codes in information and telecommunication systems; to solve the tasks of providing and maintaining (including: review, testing, accountability) the access control system in accordance with the established security policy in information and information and telecommunication (automated) systems; to solve the problems of managing the procedures of identification, authentication, authorization of processes and users in information and telecommunication systems in accordance with the established information and / or cybersecurity policy; to implement measures to counteract unauthorized access to information resources and processes in information and information and telecommunication (automated) systems; to solve the problems of managing access to information resources and processes in information and information and telecommunication (automated) systems based on access control models (mandatory, discretionary, role-based); to ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information and telecommunication (automated) systems using event logs, their analysis and established protection procedures; to implement measures and ensure the implementation of processes to prevent unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems; to solve the problems of data flow protection in information, information and telecommunication (automated) systems; to analyze and evaluate the effectiveness and level of security of resources of different classes in information and information and telecommunication (automated) systems during tests in accordance with the established information and / or cybersecurity policy; to assess the possibility of potential threats to information processed in information and telecommunication systems and the effectiveness of the use of security systems in the face of threats of various classes; to solve the problems of managing the processes of restoring the normal functioning of information and telecommunication systems using redundancy procedures in accordance with the established security policy; participate in the development and implementation of information security and/or cybersecurity strategy in accordance with the goals and objectives of the organization; to solve the problems of providing and maintaining integrated information security systems, as well as counteracting unauthorized access to information resources and processes in information and information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy; to implement processes of detection, identification, analysis and response to information and/or cybersecurity incidents; apply national and international regulations in the field of information security and/or cybersecurity to investigate incidents; solve problems of ensuring the continuity of business processes of the organization based on the theory of risks and the established information security management system, in accordance with national and international requirements and standards; apply different classes of information security and/or cybersecurity policies based on risk-based controls access to information assets; to analyze and minimize the risks of information processing in information and telecommunication systems; to solve the problems of protecting information processed in information	

and telecommunication systems using modern methods and means of cryptographic protection of information; to implement and support intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunication systems; ensure proper functioning of the system of monitoring of information resources and processes in information and telecommunication systems; ensure the functioning of software and hardware intrusion detection systems of different levels and classes (statistical, signature, statistical-signature); maintain the operability and ensure the configuration of intrusion detection systems in information and telecommunication systems; use tools for monitoring processes in information and telecommunication systems; solve the problems of analyzing program code for possible threats	
to implement processes based on national and international standards, detection, identification, analysis and response to information and/or cybersecurity incidents; analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols; to solve the problems 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 made; to ensure the processes of protection and functioning 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 the reflection of relationships and information flows, processes for internal and remote components; to apply theories and methods of protection to ensure the security of information in information and telecommunication systems; to implement measures to counteract unauthorized access to information resources and processes in information and information and telecommunication (automated) systems; to ensure the introduction of accountability of the system of access control to electronic information resources and processes in information and information and telecommunication (automated) systems using logs to assess the possibility of potential threats to information processed in information and telecommunication systems and the effectiveness of the use of security systems in the face of threats of different classes; to solve the problems of managing the processes of restoring the normal functioning of information and telecommunication systems using backup procedures in accordance with the established security policy; to solve the problems of ensuring the continuity of business processes of the organization based on the theory of risks; participate in the development and implementation of information security and/or cybersecurity strategy in accordance with the goals and objectives of the organization; to solve the problems of providing and maintaining integrated information security systems, as well as counteracting unauthorized access to information resources and processes in information and information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy; ensure the continuity of the process of maintaining logs of events and incidents based on automated procedures; implement processes for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents; apply national and international regulations in the field of information security and/or cybersecurity to investigate incidents; solve the problems of ensuring the continuity of business processes of the organization based on the theory of risks and the established information security management system, in accordance with national and international requirements and standards; apply different classes of information security and/or cybersecurity policies based on risk-based access control to information assets; to analyze and minimize risks of information processing in information and telecommunication systems;	Ability to implement procedures for incident management procedures, conduct investigations, and evaluate them.

to implement and support intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems; to ensure the proper functioning of the system for monitoring information resources and processes in information and telecommunication systems; to ensure the functioning of software and hardware intrusion detection systems of various levels and classes (statistical, signature, statistical-signature); to maintain operability and provide configuration of intrusion detection systems in information and telecommunication systems; use tools for monitoring processes in information and telecommunication systems; to solve the problems of analyzing program code for possible threats	
to solve the problem of protection of programs and information that processed in information and telecommunication systems by software and hardware and assess the effectiveness of the quality of decisions made; to ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems; apply theories and methods of protection to ensure the security of elements of information and telecommunication systems; detect dangerous signals of technical means; measure the parameters of dangerous and interfering signals during instrumental control of information protection processes and determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical protection of information; to interpret the results of special measurements using technical means, control the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the system of technical protection of information; to conduct certification (based on accounting and inspection) of restricted areas (zones), premises, etc. in conditions of secrecy with recording the results in the relevant documents; interpret the results of special measurements using technical means, control characteristics of ITS in accordance with the requirements of regulatory documents of the system of technical protection of information; to solve the problems of protecting information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information; to implement and support intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunication systems information and telecommunication systems;	Ability to apply methods and means of cryptographic and technical protection of information at the objects of information activity.

Program of the discipline

Content module 1: Fundamentals of cryptographic methods in blockchain technologies

Topic 1. Blockchain technology is not only BitCoin

Topic 2. The principle of operation of BitCoin

Topic 3. Application of cryptography in blockchain

Content module 2. Basics of blockchain technologies and examples of application

Topic 4. Rules for forming blocks in the blockchain.

Topic 5. Rules of blockchain in bitcoin

Topic 6. Transactions and key formats in bitcoin

Topic 7. Blockchain and smart contracts

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

Teaching and learning methods

In the course of teaching the discipline, the teacher uses explanatory and illustrative (information and receptive) and reproductive teaching methods. Lectures, presentations, conversations, individual and group mini-projects are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of students.

Buring lectures, the lecturer provides students with a certain amount of theoretical material (topics 1-7), examples of the use of blockchain technology (topics 1-7), with explanations in graphic form (diagrams, tables, presentations) and with examples of specific implementation of modern cryptocurrency projects (topics 1-7). During laboratory classes, students have the opportunity to gain practical skills in finding solutions to problems based on the initial data formulated on the subject of the class (topics 1-7). Practical skills are improved during independent work (topics 1-7).

The above teaching methods are aimed at developing students' ability to solve complex problems using blockchain technology.

The procedure for evaluating learning outcomes

The system for evaluating students' developed competencies takes into account the types of classes that, according to the program of the academic discipline, include lectures and laboratory classes, as well as independent work. Assessment of students' developed competencies is carried out according to a cumulative 100-point system.

The general criteria by which students' extracurricular independent work is assessed are: depth and strength of knowledge, level of thinking, ability to systematize knowledge on separate topics, ability to draw reasonable conclusions, mastery of a categorical apparatus, skills and techniques for performing practical tasks, ability to find necessary information, to carry out its systematization and processing, self-realization in laboratory classes.

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

The distribution of points of the current assessment by type of work is as follows.

Lectures: the level of mastery of theoretical knowledge is determined during the defense of laboratory work, for writing tests (maximum number of points is 20).

Laboratory classes: the level of acquired skills in applying knowledge to solve problems is determined by the correctness of the tasks of laboratory work (maximum number of points is 40).

Independent work: the level of mastering the skills of using the latest knowledge, methodology and methods of conducting scientific research is determined by the degree of preparation of the graduate student to perform laboratory work and writing tests (in the technological map of additional points for this type of work is not provided).

Final control: is carried out taking into account the exam.

The examination paper covers the discipline program and provides for determining the level of knowledge and the degree of mastery of competencies by students. Each examination paper consists of 2 theoretical questions and 1 practical task, which involve solving typical professional tasks of a specialist in the workplace and allow to diagnose the level of theoretical training of the student and the level of his competence in the discipline. Evaluation of each task of the examination ticket is as follows: the first theoretical question is evaluated by 10 points; the second question is evaluated by 10 points; the third practical task is calculated, its implementation is evaluated by 20 points.

The result of the semester examination is evaluated in points (the maximum number is 40 points, the minimum number is 25 points) and is put in the corresponding column of the examination "Record of academic performance". The applicant should be considered certified if the sum of points received as a result of the final/semester examination is equal to or exceeds 60. The minimum possible number of points for current and module control during the semester is 35 and the minimum possible number of points scored at the exam is 25. The final grade in the discipline is calculated taking into account the points obtained during the exam and the points obtained during the current control of the cumulative system. The total result in points for the semester is: "60 and more points - enrolled", "59 and less points - not enrolled" and is entered in the academic "Record of academic performance" of the discipline

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

Rating plan of the discipline

Topic	Forms and types of education		Forms of evaluation	Max ball
Topic 1	***Classroom work***			
	Lecture	Blockchain technology is not only BitCoin		
	Laboratory lesson	*Laboratory work №1. Basics of interaction with the Bitcoin node interface*	perform and defense of the laboratory work	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 2	***Classroom work***			
	Lecture	The principle of operation of BitCoin		
	Laboratory lesson	*Laboratory work №1. Basics of interaction with the Bitcoin interface node*	perform and defense of the laboratory work 1	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Application of cryptography in blockchain		
			express test	5
	Laboratory lesson	*Laboratory work №2. Working with the Ethereum test network*	perform and defense of the laboratory work № 2	8
			Control work 1	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		

Topic 4	***Classroom work***			
	Lecture	Rules for forming blocks in the blockchain		
	Laboratory lesson	*Laboratory work №3. Working with the Monero test network*	perform and defense of the laboratory work № 3	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Rules of blockchain in bitcoin	express test	**5**
	Laboratory lesson	*Laboratory work № 4. Basics of interaction with the interfaces of the EOS test network*	perform and defense of the laboratory work 4	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 6	***Classroom work***			
	Lecture	Transactions and key formats in bitcoin		
	Laboratory lesson	*Laboratory work № 5. Working with decentralized data storage IPFS*	perform and defense of the laboratory work	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Blockchain and smart contracts		
	Laboratory lesson	*Laboratory work № 5. Working with decentralized data storage IPFS*	perform and defense of the laboratory work № 5	**8**
			Control work 2	5
	Individual work			

	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Exam				40

Recommended literature

Basic

1. Kravchenko P. Blockchain and decentralized systems. Part 1 - Kharkiv: PROMART, 2019. - 452 c.
2. Kravchenko P. Blockchain and decentralized systems. Part 3 - Kharkiv: PROMART, 2020. - 306 p.

Additional

3. Global Bitcoin Nodes Distribution [Electronic resource]. - December 2018. - Access mode: https://bitnodes.earn.com/.
4. Mogayar V. Blockchain for business [Electronic resource] / William Mogayar // loveread.ec. 2018. Access mode to the resource: http://loveread.ec/read_book.php?id=71219&p=5.
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto. URL: https://bitcoin.org/bitcoin.pdf.
6. UA Crypto in Ukraine 2021 - players, laws, trends. URL: https://nachasi.com/crypto/2021/05/31/cryptotrends-in-ukraine/[Electronic resource].

Information resources

7. Site of personal training systems of KNEU named after S. Kuznets in the discipline "Blockchain: basics and examples of application" https://pns.hneu.edu.ua/course/view.php?id=8950