**BORYS GRINCHENKO KYIV UNIVERSITY**

«APPROVED»

Decision of the Academic Council,
Borys Grinchenko Kyiv University

23 August 2017, Protocol No.8

The Head of the Academic Council,

Rector
**Viktor Ogneviuk**

# Changes to Programme of Study (Vocational)

## 125.00.01 Security of information and communication systems first (bachelor) level of higher education

| | |
|---|---|
| Field of Knowledge: | **12 Information technology** |
| Specialty: | **125 Cybersecurity** |
| Qualifications**:** | **Bachelor of Cybersecurity** |
| | **3439 Specialist in Information Security** |

Enacted since 01 September 2019
(Order No.509, August-30-2019)

**Kyiv – 2019**

**LETTER OF APPROVAL**
**Changes to Programme of Study**
**(Vocational)**

The Chair of Information and Cybernetic Security of the Faculty of Information Technologies and Management Borys Grinchenko Kyiv University

Protocol No.____,_____2019

The Head of the Chair_____Volodymyr Buriachok

The Academic Council of information and cybernetic security of the Faculty of information technologies and management Borys Grinchenko Kyiv University
Protocol No.___,_____2019

The Head of the Academic Council_____Alla Mykhatska

Scientific and methodological center of standardization and quality of education

The Head of the center_____Olha Leontieva
28 August 2019

The vice-rector for scientific-methodical and educational work
_____Oleksii Zhyltsov
28 August 2019

**PREAMBLE**

The changes to the programme of study (vocational) complies with the Law of Ukraine "On Higher Education", 01.07.2015, No.1556-VII, and the Draft of the Standard for Higher Education of Ukraine in the field of knowledge 125 Cybersecurity.

№_____20

The changes to the programme of study (vocational) was developed by a working group consisting of:

*Viktor Semko, Doctor of Technical Sciences, Associate Professor, Professor of Information and Cybernetic Security Department, Boris Grinchenko Kyiv University*

*Anatoly Bessalov, Doctor of Technical Sciences, Professor, Professor of the Department of Information and Cybernetic Security of Kyiv Boris Grinchenko University*

*Natalia Korshun, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information and Cybernetic Security of Kyiv Boris Grinchenko University*

***Educational and professional program is introduced for the first time***

*Term view of educational and vocational programs_____in_____years*

Actualized:

| | | | |
|---|---|---|---|
| Date of Review of the PS /Amendments to PS | | | |
| Signature:_____ | | | |
| Name of PS Guarantor | | | |

Changes to the Programme of study (Vocational) are due to the need to expand the competencies of future specialists in the context of modern SMART-technologies. The need for the abovementioned competencies has been identified during the analysis of the relevant publications, consultations with employers in various fields of science and economics of the modern high-tech information society (the government, state and business sectors of the state economy, etc.). The competences also satisfy the needs of the community and the city of Kyiv in creating a comfortable and effective digital infrastructure of the city.

These changes relate to the objects of study and activity, content and name of the professional disciplines in order to bring them into the correspondence

with the current state of the industry. The program competencies and expected learning outcomes, resources, forms of final certification, or other parts of the OPP characteristics were not subject to substantial review.

In particular

1) objects of study and activity are specified:

- methods of application of vulnerabilities in wireless, mobile, cloud and SMART-technologies and ways to combat them, methods of organization of secure data transmission in unsecured SMART-environment, means of special network equipment for ensuring the security of corporate networks;

2) professional competences are specified:

PC-2: The ability to use informational, communicative and SMART technologies, modern methods and models of information and / or cyber security;

PC-3: The ability to use software and hardware complexes of information security in IT (automated) and SMART-systems;

PC-5: The ability to protect information that processed in IT (automated) and SMART systems in order to implement the established policy of the information and / or cybersecurity;

PC-6: The ability to restore full-time functioning of IT (automated) and SMART-systems after threats, cyber-attacks, malfunction and failures of different classes and origin;

PC-11: The ability to monitor the functioning of IT (automated) and SMART systems according to the established information and / or cybersecurity policy;

3) programme results are specified:

PLO 1: - to prepare proposals for regulations and documents in order to ensure the established information and / or cybersecurity policy;

- to develop project documentation regarding software and hardware complexes of protection of IT (automated) and SMART-systems;

- to carry on the analysis of the implementation of the adopted informational and / or cybersecurity policy;

PLO 2: - to carry on professional activity on the basis of knowledge of modern information, communication and SMART-technologies;

- to develop and analyze IT and SMART systems projects based on standardized technologies and data transfer protocols;

- to apply knowledge, skills and practices in the professional activity, regarding the structures of modern computer systems, methods and means of information processing, operating system architectures;

- to protect the resources and processes in ITS on the basis of security models (finite state machines, flow control, Bell-LaPadula, Biba, Clark-Wilson, etc.), as well as established modes of safe functioning of IT and SMART systems;

PLO 3: - to provide processes of protection of IT (automated) and SMART-systems by installing and using the correct operation of software and hardware complexes of protection means;

- to ensure the functioning of special software for data protection against destructive software influences, demolishing codes in IT (automated) and SMART systems;

- to carry out the development of operational documentation at the SPA;

PLO 4: - to solve the problems of maintenance (including: review, testing, accountability) of the access control system according to the principles, criteria of access and established security policy in IT (automated) and SMART-systems;

- to implement measures to counteract obtaining unauthorized access to information resources and processes in IT (automated) and SMART systems;

- to solve problems of access control to information resources and processes in IT (automated) and SMART-systems on the basis of models of

access control (mandate, discretionary, role);

- to solve the problems of centralized and decentralized administration of access to informational resources and processes in IT (automated) and SMART-systems;

- to ensure that accountability for the management of access to informational resources and processes in IT and SMART systems is introduced;

PLO 5: - to choose the basic methods and means of information security in accordance with the requirements of modern standards of information and cybersecurity, and the criteria of IT security, applying a systematic approach and knowledge of the basics of information security theory;

- to solve problems of managing the procedures of identification, authentication, authorization, users and processes in information and IT (automated) and SMART-systems;

- to design and implement complex information security systems in the AS of the organization (enterprise) in accordance with the requirements of regulatory documents of the system of technical protection of information;

- to solve problems of data flow protection in information, IT (automated) and SMART systems;

- to determine the level of security of information resources in information and IT (automated) and SMART-systems;

- to use tools to assess the potential for the implementation of potential threats to information processed in IT (automated) and SMART systems;

PLO 7: - to solve problems of support and implementation of complex information security systems, as well as counteracting unauthorized access to resources and processes in information, IT (automated) and SMART systems;

- to assess the level of security of information processed in IT and SMART systems and use tools to assess the presence of potential vulnerabilities;

- to solve the problems of managing the complex system of information protection in information, IT (automated) and SMART-systems;

- to solve the problems of examination, testing of CSIS;

PLO 8: - to solve problems of prevention and detection, identification, analysis and response to incidents in information, IT (automated) and SMART-systems;

- to investigate information and / or cyber security incidents based on national and international regulatory acts, procedures and regulations in the field of information and / or cybersecurity;

- to ensure compliance with the policy of keeping the record of incidents and bugs with the specified level of detail;

PLO 10: - to analyze and determine the possibility of application of technologies, methods and means of cryptographic protection of information;

- to analyze and determine the possibility of application of technologies, methods and means of technical protection of information;

- to detect dangerous signals of technical means;

- to measure the parameters of dangerous and interfering signals during instrumental control of information leakage protection by technical channels;

- to determine the effectiveness of protection of information from leakage by technical channels in accordance with the requirements of regulatory documents of the system of technical protection of information;

- to interpret the results of special measurements using technical means, control of the characteristics of IT and SMART-systems in accordance with the requirements of regulatory documents of the system of technical protection of information;

- to substantiate the possibility of creating technical channels of

information leakage on objects of information activity;

- to implement measures and means of technical protection of information from leakage by technical channels;

PLO 11: - to provide monitoring of access to resources and processes of IT and SMART systems;

- to ensure the configuration and operation of resource and process monitoring systems in IT and SMART systems;

PLO 12: - to implement and support intrusion detection systems and use security complexes to provide the required level of information security in information, information and telecommunications (automated) and SMART systems;

- to analyze the effectiveness of systems for detecting and counteracting unauthorized access to resources and processes in IT and SMART systems;

- to analyze and implement malware protection systems.

4) the discipline was renamed "Security for wireless, mobile and cloud technologies" changed to "Security for wireless, mobile, cloud and SMART technologies".

Thus, the major changes concerned Part 1 “Profile of the Cybersecurity Specialty 125 Specialty Educational Program” in Segments 6 and 7, as well as Part 2 of the OPP in Segments 2.1. «List and distribution of credit volumes of disciplines of the curriculum of preparation of applicants of the second level of higher education - master's degree» and 2.2. "Structural and logical scheme of OPP".

New editions of these parts of the educational and professional program are listed below.

## I. PROFILE OF THE PROGRAMME OF STUDY (VOCATIONAL)

| 6 – Competence of the graduate | | |
|---|---|---|
| **Professional Competences of specialty** | PC-2 | The ability to use information and communication technologies, modern methods and models of information and/or cybersecurity. |
| | PC-3 | The ability to use software and hardware complexes of information security in information and telecommunication (automated) systems. |
| | PC-5 | The ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information policy and/or cybersecurity. |
| | PC-6 | The ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyberattacks, failures of different classes and origin. |
| | PC -11 | The ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. |

| 7 – Programme learning outcomes | |
|---|---|
| PLO 1 | - to prepare proposals for regulations and documents in order to ensure the established information and / or cybersecurity policy;<br>- to develop project documentation, software and hardware complexes of information, information and telecommunication (automated) systems protection;<br>- to perform analysis of the implementation of the adopted information policy and/or cybersecurity; |
| PLO 2 | - to carry out professional activities on the basis of knowledge of modern information and communication technologies;<br>- to develop and analyze ITC projects basing on standardized technologies and data transfer protocols;<br>- to apply in professional activity knowledge, skills and practices regarding the structures of modern computing systems, methods and means of information processing, architectures of operating systems;<br>- to protect resources and processes in ITC based on security models (finite state machines, flow control, Bell-LaPadula, Biba, Clark-Wilson, and others), and established modes of safe operation of ITC;<br>- perform software analysis to assess compliance with established information and/or cybersecurity requirements in the its; |
| PLO 3 | - to provide processes of protection of information and telecommunication (automated) systems by installation and correct operation of software and hardware complexes of means of protection;<br>- to provide the functioning of special software, data protection software from the damaging effects of destructive codes into the information, information and telecommunication (automated) systems;<br>- to carry out development of operational documentation on CMP: |
| PLO 4 | - to solve the tasks of support (including: review, testing, reporting) of access control system according to the principles, access criteria and established security policy in information and information and telecommunication (automated) systems;<br>- to implement measures to prevent unauthorized access to information resources and processes in information and information and telecommunication (automated) systems;<br>- to solve problems of access control to information resources and processes in information and information and telecommunication (automated) systems on the basis of access control models (mandatory, discretionary, role-playing);<br>- to solve the problems of centralized and decentralized administration with access to information resources and processes in information and information and telecommunication (automated) systems which based on access control models (mandatory, discretionary, role-playing);<br>- to ensure accountability of the access control system of information resources and processes in ITC. |
| PLO 5 | - to choose the main methods and means of information security in accordance with the requirements of modern standards of information and cybersecurity, and information technology security criteria, applying a systematic approach and knowledge of the basics of the theory of information security;<br>- to solve problems of management of procedures of identification, authentication, authorization of users and processes in information and |

| | |
|---|---|
| | information and telecommunication (automated) systems<br>- to project and implement complex systems of information security in the AS organization (enterprise) in accordance with the requirements of normative documents of the system of technical protection of information;<br>- to solve problems of data flow protection in information, information and telecommunication (automated) systems;<br>- to determine the level of security of information resources in information and information and telecommunication (automated) systems;<br>- to use tools to assess the possibility of implementation of potential threats to information processed in information and telecommunications (automated) systems; |
| PLO 7 | - to solve the problems of support and implementation of complex systems of information security, and also combating unauthorized access to resources and processes in information and information and telecommunication (automated) systems;<br>- to estimate the level of security of information processed in ITC using the tools to assess the presence of potential vulnerabilities;<br>- to solve problems of management of complex system of information security in information and information and telecommunication (automated);<br>- solve the problems of examination, testing CCISS; |
| PLO 8 | - to solve the problems of prevention and detection, identification, analysis and response to incidents in information, information and telecommunication (automated) systems;<br>- to investigate information and/or cybersecurity incidents based on national and international regulations, procedures and regulations in the field of information and / or cybersecurity;<br>- to ensure compliance with the event and incident logging policy with the specified level of details; |
| PLO 10 | - to analyze and determine the possibility of application of technologies, methods and means of cryptographic protection of information;<br>to analyze and determine the possibility of application of technologies, methods and means of technical protection of information;<br>- to identify dangerous signals of technical means;<br>- to measure the parameters of dangerous and interference signals during the instrumental control of information security from leakage by technical channels;<br>- to determine the effectiveness of information protection from leakage by technical channels in accordance with the requirements of regulatory documents of the technical information protection system;<br>- to interpret the results of special measurements using technical means to control the characteristics of its in accordance with the requirements of normative documents of the system of technical protection of information;<br>- to substantiate the possibility of creating technical channels of information leakage at the objects of information activity;<br>- to implement measures and means of technical protection of information from leakage by technical channels; |

| | |
|---|---|
| PLO 11 | - to ensure the processes of monitoring of access to the resources and processes of ITC;<br>- to ensure the configuration and functioning of systems of monitoring of resources and processes in its; |
| PLO 12 | - to implement and support intrusion detection systems and use protection systems to ensure the necessary level of information security in information, information and telecommunications and automated systems;<br>-to analyze the effectiveness of systems to detect and counter unauthorized access to resources and processes in its<br>- to analyze and implement anti-malware systems. |

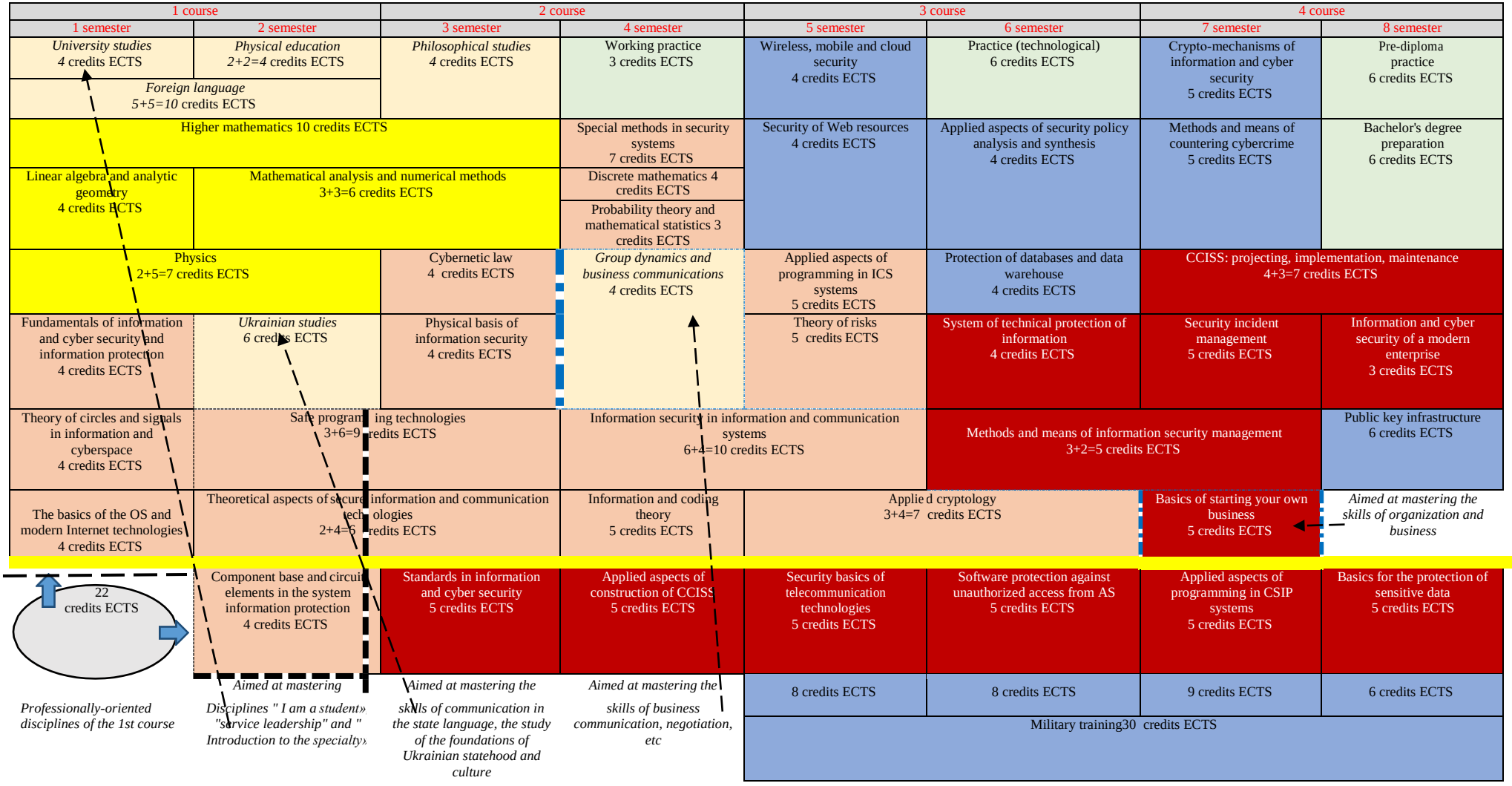
## II. The List of the Components of the Programme of Study (vocational) Social Communications and Their Logical Coherence

2.1. The list and distribution of the volume of credit disciplines of the curriculum of training applicants for the first level of higher education-bachelor, specialty-125 Cybersecurity

| Code | Components of the Programme of Study (academic discipline, practice, degree paper) | Credits | Distribution of class hours for courses and semesters | | | | | | | | The Form of the Final Control |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 course | | 2 course | | 3 course | | 4 course | | |
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| **I. Compulsory components** | | | | | | | | | | | |
| **1. Educational discipline** | | | | | | | | | | | |
| ***Formation of general competencies*** | | | | | | | | | | | |
| ОД3..01 | *University studies* | **4** | 4 | | | | | | | | Credit |
| | *I'm a student* | 1 | * | | | | | | | | |
| | *Leadership service* | 1 | * | | | | | | | | |
| | *Introduction to the specialty* | 2 | * | | | | | | | | |
| ОД3..02 | *Foreign language* | **10** | 5 | 5 | | | | | | | Exam, Credit |
| ОД3..03 | *Physical education* | **4** | 2 | 2 | | | | | | | Credit |
| ОД3..04 | *Ukrainian studies* | **6** | | 6 | | | | | | | Exam |
| ОД3..05 | *Philosophical studies* | **4** | | | 4 | | | | | | Exam |
| ОД3..06 | *Group dynamics and business communications* | **4** | | | | 4 | | | | | Credit |
| | **Amount** | **32** | **11** | **13** | **4** | **4** | **0** | **0** | **0** | **0** | |
| ***The formation of a special (professional, subject-specific) competences*** | | | | | | | | | | | |
| ОДС.01 | Physics | **7** | 2 | 5 | | | | | | | Exam, Credit |
| ОДС.02 | Higher mathematics | **10** | 4 | 3 | 3 | | | | | | Credit,Exam |
| | *Linear algebra and analytic geometry* | 4 | * | | | | | | | | |
| | *Mathematical analysis and numerical methods* | 6 | | * | * | | | | | | |
| ОДС.03 | Fundamentals of information and cyber security and information protection | **4** | 4 | | | | | | | | Credit |
| ОДС.04 | Theory of circles and signals in information and cyberspace | **5** | 5 | | | | | | | | Exam |
| ОДС.05 | The basics of the OS and modern Internet technologies | **4** | 4 | | | | | | | | Credit |
| ОДС.06 | Safe programming technologies | **9** | | 3 | 6 | | | | | | Exam. Credit, term paper |
| ОДС.07 | Theoretical aspects of secure information and communication technologies | **6** | | 2 | 4 | | | | | | Exam, Credit |
| ОДС.08 | Component base and circuit elements in the system.information protection | **4** | | 4 | | | | | | | Exam |
| ОДС.09 | Cybernetic law | **4** | | | 4 | | | | | | Credit |
| ОДС.10 | Physical basis of information security | **4** | | | 4 | | | | | | Exam |
| ОДС.11 | Special methods in security systems | **7** | | | | 7 | | | | | Exam |
| | Discrete mathematics | 4 | | | | * | | | | | |
| | Probability theory and mathematical statistics | 3 | | | | * | | | | | |
| ОДС.12 | Information security in information and communication systems | **10** | | | | 6 | 4 | | | | Exam, Credit term paper |
| ОДС.13 | Information and coding theory | **5** | | | | 5 | | | | | Exam |
| ОДС.14 | Decision making in the information and cyber security | **5** | | | | | 5 | | | | Exam |
| ОДС.15 | Theory of risks | **5** | | | | | 5 | | | | Credit |
| ОДС.16 | Applied cryptology | **7** | | | | | 3 | 4 | | | Exam, Credit |
| ОДС.17 | Wireless, mobile and cloud security | **4** | | | | | 4 | | | | Exam |
| ОДС.18 | Security of Web resources | **4** | | | | | 4 | | | | Exam |
| ОДС.19 | Applied aspects of security policy analysis and synthesis | **4** | | | | | | 4 | | | Exam |
| ОДС.20 | Protection of databases and data warehouse | **4** | | | | | | 4 | | | Exam |
| ОДС.21 | Crypto-mechanisms of information and cyber security | **5** | | | | | | | 5 | | Exam |
| ОДС.22 | Methods and means of countering cybercrime | **4** | | | | | | | 4 | | Exam |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ОДС.23 | Public key infrastructure | **6** | | | | | | | | 6 | Exam |
| | **Amount** | **127** | **19** | **17** | **21** | **18** | **25** | **12** | **9** | **6** | |
| **2. Practice** | | | | | | | | | | | |
| WP.2.01 | Practice (working) | **3** | | | | 3 | | | | | Credit |
| WP.2.02 | Practice (technological) | **6** | | | | | | 6 | | | Credit |
| WP.2.03 | Pre-diploma | **6** | | | | | | | | 6 | Credit |
| | **Amount** | **15** | **0** | **0** | **0** | **3** | **0** | **6** | **0** | **6** | |
| **3. Certification** | | | | | | | | | | | |
| **C.01** | Bachelor's degree preparation | **4,5** | | | | | | | | 4,5 | |
| | Bachelor's thesis defense | **1,5** | | | | | | | | 1,5 | |
| **Amount** | | **6** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **6** | |
| | **Total amount of the optional components** | **180** | **30** | **30** | **25** | **25** | **25** | **18** | **9** | **18** | |
| **II. Optional components** | | | | | | | | | | | |
| **4. Educational discipline** | | | | | | | | | | | |
| **4.1. Specialized block of academic disciplines** | | | | | | | | | | | |
| OC.1.01 | Standards in information and cyber security | **5** | | | 5 | | | | | | Credit |
| OC.1.02 | Applied aspects of construction of CCISS | **5** | | | | 5 | | | | | Exam |
| OC.1.03 | Security basics of telecommunication technologies | **5** | | | | | 5 | | | | Exam |
| OC.1.04 | Software protection against unauthorized access from AS | **5** | | | | | | 5 | | | Exam |
| OC.1.05 | Applied aspects of programming in CSIP systems | **5** | | | | | | | 5 | | Exam |
| OC.1.06 | Basics for the protection of sensitive data | **5** | | | | | | | | 5 | Exam |
| OC.1.07 | System of technical protection of information | **4** | | | | | | 4 | | | Credit |
| OC.1.08 | Methods and means of information security management | **5** | | | | | | 3 | 2 | | Credit |
| OC.1.09 | CCISS: projecting, implementation, maintenance | **7** | | | | | | | 4 | 3 | Exam , term paper |
| OC.1.10 | Security incident management | **5** | | | | | | | 5 | | Credit |
| OC.1.11 | Basics of starting your own business | **5** | | | | | | | 5 | | Credit |
| OC.1.12 | Information and cyber security of a modern enterprise | **4** | | | | | | | | 4 | Credit |
| | **Amount** | **60** | **0** | **0** | **5** | **5** | **5** | **12** | **21** | **12** | |
| | **4.2 Free choice academic disciplines from the course catalogue** | | | | | | | | | | |
| FC 1.01 | Choice from the catalogue | **60** | | | 5 | 5 | 5 | 12 | 21 | 12 | Exam, Credit, term paper |
| | **Total amount of the optional components** | **60** | **0** | **0** | **5** | **5** | **5** | **12** | **21** | **12** | |
| **TOTAL AMOUNT OF THE PROGRAMME OF STUDY** | | **240** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | **30** | |

# 2.2. Structural Logical Scheme of the Programme of Study (Vocational)




| Cycle of disciplines of formation of General competences | | Cycle of disciplines of formation of professional competences | | Cycle of disciplines of professional competence deepening | |
|---|---|---|---|---|---|
| **Compulsory components** | disciplines of humanitarian and socio-economic training – 32 credits ECTS | **Compulsory components** | Disciplines of special training - 79 credits ECTS | **Optional components** | Course subjects – 30 credits ECTS |
| | | | Disciplines of professional specialization -31 credits ECTS | | Disciplines of the specialized course – 30 credits ECTS |
| | | | Disciplines of fundamental and natural-scientific training – 17 credits ECTS | | |
| Practice ( working, technological, pre-diploma) + Bachelor's degree preparation – 21 credits ECTS | | | | | |