

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



"ЗАТВЕРДЖУЮ"

Проректор з навчально-методичної роботи

Каріна НІМАЙКАЛО

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

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 ЄВСЕЄВ

Харків
2021

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



"APPROVED"

Vice-rector for educational and methodical work


Karina NEMASHKALO

INFORMATION SECURITY OF THE STATE

working program of the discipline

Field of knowledge *12 Information technologies*
Specialty *125 Cybersecurity*
Education level *first (bachelor's)*
Education programme *Cybersecurity*

Type of discipline *basic*
Language of instruction, teaching and assessment *English*

Head of Department
*cybersecurity and
information technologies*  *Serhii YEVSEIEV*

Kharkiv
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:

With the advent of new information technologies based on the widespread introduction of computer technology, communications, information and communication systems, information security of the state becomes a constant and necessary attribute of the state, legal entities, public associations and even ordinary citizens. Indeed, electronic document management systems in public institutions, the electronic payment system, the card system for paying for telephone calls, the TV with teletext or telephone and videophone conversations over the Internet have already become a part of everyday life.

Another side of these processes is the increase in the amount of valuable information that is processed in automated systems, the quality, reliability and efficiency of which depends on most important decisions made at various levels – from the head of state to the citizen. As a result, the normal life of society increasingly depends on the proper functioning of such information systems. Moreover, they become the most important object for attack by forces hostile to society (or an individual state). The information sphere is becoming not only one of the most important areas of international cooperation, but also an object of rivalry.

Information influence on the state, society, citizen is now more effective and economical than political, economic and even military. Countries with more developed information infrastructure, setting technological standards and providing customers with their resources, determine the conditions for the formation and operation of information structures in other countries, have a significant impact on the development of their information spheres. When forming the state information policy and program of entering the information society, one of the highest priorities is the development and guarantee of information security on the basis of the creation of the state information security system.

The purpose of teaching the discipline "Information Security of the State" is to determine the place and role of information security in the overall system of national security, the state and principles of information security of the individual, society and state.

The results of studying this discipline are the acquisition of theoretical foundations of the legal framework of Ukraine and the international community in the field of national and information security, determining the basic requirements for the formation of support and improvement of information security management systems of critical information and communication systems.

Characteristics of the discipline

Course	1
Semester	1
Number of ECTS credits	5
Form of final control	Exam

Structural and logical scheme of studying the discipline

Prerequisites	Postrequisites
Disciplines of legal field (school programme)	Security in information and communication systems
Informatics (school programme)	Fundamentals of national security
	Ensuring of information security

Competences and learning outcomes in the discipline

Competences	Learning outcomes
<p>OC 2. Knowledge and understanding of the subject area and understanding of the profession.</p>	<p>LO 1 - apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;</p> <p>LO 2 - to organize own professional activity, to choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, to estimate their efficiency;</p> <p>LO 3 - use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity;</p> <p>LO 4 - analyze, argue, make decisions in solving complex specialized problems and practical problems in professional activities, which are characterized by complexity and incomplete definition of conditions, be responsible for decisions;</p> <p>LO 5 - to adapt to frequent changes in the technology of professional activity, to predict the end result;</p> <p>LO 6 - critically comprehend the basic theories, principles, methods and concepts in teaching and professional activities;</p> <p>LO 7 - to act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and / or cybersecurity;</p> <p>LO 8 - prepare proposals for regulations to ensure information and / or cybersecurity;</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 43 - apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents;</p> <p>LO 54 - to be aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.</p>
<p>PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and / or cybersecurity.</p>	<p>LO -7 to act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and / or cybersecurity;</p> <p>LO -8 to prepare proposals for regulations to ensure information and / or cybersecurity;</p> <p>LO -9 to implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO -16 to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents;</p> <p>LO -33 to solve problems of ensuring the continuity of business processes of the organization on the basis of risk theory;</p> <p>LO -34 to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization;</p> <p>LO -35 to solve the problem of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy;</p> <p>LO -43 to apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents;</p> <p>LO -44 to solve problems of ensuring the continuity of business processes of the organization on the basis of risk theory and the established system information security management, in accordance with domestic and international requirements and standards.</p>

Competences	Learning outcomes
<p>PC 3. Ability to use software and software-hardware complexes of information security in information and telecommunication (automated) systems.</p>	<p>LO -9. Implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO -14. Solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and evaluate the effectiveness of the quality of decisions;</p> <p>LO -15. Use modern software and hardware information and communication technologies;</p> <p>LO -16. Implement comprehensive information security systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents;</p> <p>LO -17. To provide processes of protection and functioning of information and 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 streams, processes for internal and remote components;</p> <p>LO -18. Use software and hardware-software systems for protection of information resources;</p> <p>LO -20. Ensure the operation of special software to protect information from destructive software influences, destructive codes in information and telecommunications systems;</p> <p>LO -29. Carry out assessment of the possibility of realization of potential threats of information processed in information and telecommunication systems and efficiency of use of complexes of means of protection in the conditions of realization of threats of different classes;</p> <p>LO -35. Solve the problem of providing and maintaining comprehensive information security systems, as well as counteracting unauthorized access to information resources and processes in information and information and telecommunications (automated) systems in accordance with the established policy of information and / or cybersecurity;</p> <p>LO -47. Solve problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information;</p> <p>LO -50. Ensure the functioning of software and software-hardware systems for detecting intrusions of different levels and classes (statistical, signature, statistical-signature);</p> <p>LO -53 to solve the problem of analysis of program code for the presence of possible threats.</p>
<p>PC 9. Ability to carry out professional activities on the basis of the implemented information and / or cybersecurity management system.</p>	<p>LO -9 to implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO -21 to solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information and information and telecommunications (automated) systems;</p> <p>LO -24 to solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role);</p> <p>LO -25 to ensure the introduction of accountability of the control system for access to electronic information resources and processes in information and information-telecommunication (automated) systems using event logs, their analysis and established protection procedures;</p> <p>LO -28 to analyze and evaluate the effectiveness and level of protection of resources of different classes in information and information-telecommunication (automated) systems during testing in accordance with the established policy of information and / or cybersecurity;</p> <p>LO -29 to assess the feasibility of potential threats to information processed in information and telecommunications systems and the effectiveness of the use of complexes of means of protection in the implementation of threats of different classes;</p> <p>LO -33 to solve problems of ensuring the continuity of business processes of</p>

Competences	Learning outcomes
	<p>the organization on the basis of risk theory;</p> <p>LO -34 to participate in the development and implementation of information security and / or cybersecurity strategies in accordance with the goals and objectives of the organization;</p> <p>LO -35 to solve the problem of providing and maintaining complex information protection systems, as well as counteracting unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established information and / or cybersecurity policy;</p> <p>LO -42 to implement processes of detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO -43 to apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents;</p> <p>LO -44 to solve the problem of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards;</p> <p>LO -45 to apply various classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets;</p> <p>LO -46 to analyze and minimize the risks of information processing in information and telecommunications systems.</p>
<p>PC 11. Ability to monitor the functioning of information, information and telecommunications (automated) systems in accordance with the established policy of information and / or cybersecurity.</p>	<p>LO -9. Implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</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>RN-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols;</p> <p>LO -14. Solve the problem of protection of programs and information processed in information and telecommunication systems by software and hardware and evaluate the effectiveness of the quality of decisions;</p> <p>LO -15. Use modern software and hardware information and communication technologies;</p> <p>LO -17. To provide processes of protection and functioning of information and 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 streams, processes for internal and remote components;</p> <p>LO -18. Use software and hardware-software systems for 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 -21. Solve the tasks of providing and maintaining (including: review, testing, accountability) access control system in accordance with the established security policy in information and information and telecommunications (automated) systems;</p> <p>LO -22. 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 policy of information and / or cybersecurity;</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 -24. Solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role);</p> <p>LO -25. Ensure the introduction of accountability of the access control system to electronic information resources and processes in information and information-telecommunication (automated) systems using event logs, their</p>

Competences	Learning outcomes
	analysis and established protection procedures; LO -26. Implement measures and ensure the implementation of processes to prevent unauthorized access and protection of information, information and telecommunications (automated) systems based on the reference model of open systems interaction; LO -32. To solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy; LO -41. Ensure continuity of the process of keeping logs of events and incidents on the basis of automated procedures; LO – 42. Implement processes for detecting, identifying, analyzing and responding to information and / or cybersecurity incidents; LO – 43. Apply national and international regulations in the field of information security and / or cybersecurity to investigate incidents; 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; LO -49. Ensure proper functioning of the system of monitoring information resources and processes in information and telecommunication systems; LO -50. Ensure) the functioning of software and software-hardware systems for detecting intrusions of different levels and classes (statistical, signature, statistical-signature); LO -51. Maintain the efficiency and ensure the configuration of intrusion detection systems in information and telecommunications systems; LO -52. Use tools to monitor processes in information and telecommunications systems. LO -53 to solve problems of analysis of program code for the presence of possible threats.

Curriculum

Content module 1. Modern foundations of information security of the state.

- Topic 1. The concept of information security of the state and components of national interests of Ukraine in the information sphere
- Topic 2. Basic provisions of information security
- Topic 3. Threats to information security
- Topic 4. Fundamentals of information confrontation
- Topic 5. Psychological warfare, information and psychological security of the state
- Topic 6. Fundamentals of state information policy

Content module 2. Fundamentals of information technology security

- Topic 7. Basic concepts of ISO/IEC 27000 standards: “Information technology. Security methods ”
- Topic 8. Types of personal data in the state. Principles of personal data protection in the state
- Topic 9. Fundamentals of information resources security
- Topic 10. Fundamentals of information security management

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

When teaching the discipline, instructor uses explanatory-illustrative (information-receptive) and reproductive teaching methods. Lectures (1-10), presentations (1-10) are used as teaching methods that are aimed at activating and stimulating the educational and cognitive activities of students.

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 - 60 points; the minimum amount that allows a student to take the exam - 35 points);

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

The procedure for the continuous assessment of students' knowledge.

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

-understanding, the degree of mastering the theory and methodology of the problems under consideration;

-degree of mastering the actual material of the discipline;

-acquaintance with the recommended literature, and also with the modern literature on the considered questions;

-ability to combine theory with practice when considering production situations, solving problems, making calculations in the process of performing individual tasks and tasks submitted for consideration in the audience;

-logic, structure, style of presentation of material in written works and in speeches in the audience, the ability to justify their position, to generalize information and draw conclusions;

-arithmetic correctness of individual and complex calculation task;

-ability to conduct a critical and independent assessment of certain issues; the ability to explain alternative views and the presence of their own point of view, position on a particular issue;

-application of analytical approaches;

-quality and clarity of reasoning;

-logic, structuring and validity of conclusions on a specific problem;

-independence of work performance, literacy of material presentation, use of comparison methods, generalization of concepts and phenomena, design of work.

The general criteria for assessing extracurricular independent work of students are: depth and strength of knowledge, level of thinking, ability to systematize knowledge on individual topics, ability to draw sound conclusions, mastery of categorical apparatus, skills and techniques of practical tasks, ability to find necessary information, carry out its systematization and processing, self-realization in practical and seminar classes.

The final control of knowledge and competencies of students in the discipline is carried out on the basis of credit, which is considered passed if the student scored 60 or more points during the semester.

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

Lectures: the maximum number of points is 15 (work on lectures).

Laboratory classes: the maximum number of points is 45 (defense of laboratory works - 35, control works - 10), and the minimum - 27.

Individual work: consists of the time that the applicant spends on preparation for laboratory work and preparation for control work, in the technological map points for this type of work are not allocated.

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

The examination paper covers the program of the discipline and provides for the determination of the level of knowledge and the degree of mastery of competencies by students.

Each exam paper consists of 3 practical situations (one stereotypical, one diagnostic and one heuristic task), which involve solving typical professional tasks in the workplace and allow to diagnose the level of theoretical training of the student and his level of competence in the discipline. Evaluation of each task of the examination ticket is as follows: the first task is 20 test tasks of the closed form, its performance is estimated by 20 points; the second task is devoted to the

development of a scheme that ensures the authentication and reliability of information being prepared for transmission by telecommunication channels, its implementation is estimated at 10 points; the third task is calculated, its performance is estimated at 10 points.

The result of the semester exam is evaluated in points (maximum number - 40 points, minimum number of credits - 25 points) and is affixed in the appropriate column of the examination "Information of performance".

A student should be considered certified if the sum of points obtained from the final / semester test is equal to or exceeds 60. The minimum possible number of points for current and modular control during the semester is 35 and the minimum possible number of points scored in the exam is 25.

The final grade in the discipline is calculated taking into account the scores obtained during the exam and the scores 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.

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 test
90 - 100	AND	excellent	credited
82 - 89	B	good	
74 - 81	C		
64 - 73	D	satisfactorily	
60 - 63	E		
35 - 59	FX	unsatisfactorily	not credited

Rating plan of the discipline

Topic	Forms and types of education		Forms of evaluation	Max score
Topic 1	<i>Classroom work</i>			
	Lecture	INTRODUCTION. Lecture. The concept of information security of the state and components of national interests of Ukraine in the information sphere	Work on lectures	1
Topic 2.	<i>Classroom work</i>			
	Lecture	Lecture. Basic provisions of information security	Work on lectures	1
	Laboratory lesson	Laboratory work "Information for decision making"	Defense of laboratory work	3
	<i>Individual work</i>			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 3	<i>Classroom work</i>			
	Lecture	Lecture. Information security threats	Work on lectures	1
	Laboratory lesson	Laboratory work "Methods and ways	Defense of	3

		of collecting and processing information"	laboratory work	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Performing tasks on methods and ways of collecting and processing information		
Topic 4	Classroom work			
	Lecture	Lecture. Fundamentals of information confrontation	Work on lectures	1
	Laboratory lesson	Laboratory work "The need for information protection"	Defense of laboratory work	3
	Individual work			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 5	Classroom work			
	Lecture	Lecture. Psychological war and information and psychological security of the state	Work on lectures	1
			Express survey	
	Laboratory lesson	Laboratory work "Information confrontation"	Protection of laboratory work	3
		Test work 1	15	
Topic 6	Classroom work			
	Lecture	Lecture. Fundamentals of state information policy	Work on lectures	1
	Laboratory lesson	Laboratory work "Analytical support of information security"	Defense of laboratory work	3
	Individual work			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic.		
Topic 7	Classroom work			
	Lecture	Lecture. Basic concepts of ISO / IEC 27000 standards: "Information technology. Security methods "	Work on lectures	1
	Laboratory lesson	Laboratory work "Classification of technical tools of information security"	Defense of laboratory work	3
	Individual work			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Execution of laboratory tasks		

Topic 8	<i>Classroom work</i>			
	Lecture	Lecture. Types of personal data in the state. Principles of personal data protection in the state	Work on lectures	1
	Laboratory lesson	Laboratory work "Classification of software and cryptographic tools of information security"	Defense of laboratory work	3
	<i>Individual work</i>			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 9	<i>Classroom work</i>			
	Lecture	Lecture. Fundamentals of information resources security	Work on lectures	1
	Laboratory lesson	Laboratory work "System classification and characteristics of technical means of information security"		
	<i>Individual work</i>			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 10	<i>Classroom work</i>			
	Lecture	Lecture. Fundamentals of information security management	Work on lectures	
			Test work 2	15
	Laboratory lesson	Laboratory work "Electronic user identification. Regulatory information security "	Defense of laboratory work	
	<i>Individual work</i>			
	Questions and tasks for self-study	Search, selection and review of recommended reading on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
	Exam			40

Recommended Books

Basic

1. Tikk E., Kerttunen M. (ed.). Routledge Handbook of International Cybersecurity. – Routledge, 2020.
2. Christen M., Gordijn B., Loi M. The ethics of cybersecurity. – Springer Nature, 2020. – C. 384.
3. Guiora A. N. Cybersecurity: Geopolitics, law, and policy. – Routledge, 2017.
4. Caravelli J., Jones N. Cyber security: Threats and responses for government and business. – ABC-CLIO, 2019.
5. Daimi K. et al. (ed.). Computer and network security essentials. – Springer, 2018.
6. Gupta B. B. (ed.). Computer and cyber security: principles, algorithm, applications, and perspectives. – CRC Press, 2018.

7. Corradini I. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. – Springer Nature, 2020. – T. 284.
8. Li K. C., Chen X., Susilo W. (ed.). Advances in Cyber Security: Principles, Techniques, and Applications. – New York, NY, USA : Springer, 2019.
9. Alsmadi I., Easttom C. The NICE Cyber Security Framework. – Springer International Publishing, 2020.
10. Death D. Information security handbook: develop a threat model and incident response strategy to build a strong information security framework. – Packt Publishing Ltd, 2017.
11. Sarfraz M. (ed.). Developments in Information Security and Cybernetic Wars. – IGI Global, 2019.
12. George R. Z. Intelligence in the National Security Enterprise: An Introduction. – Georgetown University Press, 2020.

Optional

13. Law of Ukraine “On Information Protection in Information and Telecommunication Systems” (1994);
14. Law of Ukraine “On Personal Data Protection” (2010)
15. STRATEGY OF NATIONAL SECURITY OF UKRAINE (approved by the Decree of the President of Ukraine of May 26, 2015 № 287/2015)
16. Law of Ukraine “On National Security (2018)
17. ISO / IEC 27001. "Information technology. Security methods. Information security management systems.
18. ISO / IEC 27002. "Information technology. Security methods. Practical rules for information security management."
19. ISO / IEC 27005. "Information technology. Security methods. Information security risk management

Information resources

20. Site of personal educational systems of Simon Kuznets KhNUE, page of the discipline "Information Security of the State" <https://pns.hneu.edu.ua/course/view.php?id=4948>.