Syllabus
Course Program

Information security of the state

Specialty
F5 – Cybersecurity and information protection

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Cybersecurity

Department
Cybersecurity (328)

Level of education
Bachelor's level

Course type
Special (professional), Mandatory

Semester
2

Language of instruction
English

Lecturers and course developers

Oleksandr MILOV

oleksandr.milov@khpi.edu.ua
Doctor of technical sciences, professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 200 scientific and educational and methodological works. Academic supervisor for protected candidate theses, guarantor of the educational and professional program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Mathematical foundations of cryptology and cryptanalysis", "Data structures", "Industrial and office espionage", "Digital forensics", for undergraduate and graduate students, Section "Methodology of scientific and pedagogical activity in the sciences of cyber protection" for postgraduate students.

More about the lecturer on the department's website

Olha KOROL

olha.korol@khpi.edu.ua
Candidate of technical sciences, associate professor, associate professor of the department of cyber security of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 150, of which 14 are textbooks, 48 articles in foreign publications and specialized publications of Ukraine, 8 patents for a useful model, 9 in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management", "State national security", "State information security", "Comprehensive training "Security of web applications"" for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Information security of the state" is a mandatory educational discipline. The discipline is aimed at researching ways, methods, means and channels of threats to national interests at the information level and their timely detection, prevention and neutralization.

Course objectives and goals

Formation of the theoretical foundations of the legislative framework of Ukraine and international society in the field of national and information security of the state, determination of the main requirements for the formation of support and improvement of information security management systems of critical information and communication systems, as well as determination of the place and role of information security in the general system of national security, state and the principles of ensuring information security of the individual, society and the state.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control – test.

Competencies

GC1. Ability to apply knowledge in practical situations.
GC2. Knowledge and understanding of the subject area and understanding of professional activity.
GC3. Ability to communicate in the state language both orally and in writing.
GC4. Ability to communicate in a foreign language.
GC5. Ability to learn and master modern knowledge.
GC6. The ability to realize own rights and responsibilities as a member of society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.
GC7. Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty.
PC-1. PC1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of cybersecurity and information protection.
PC7. Ability to perform professional activities based on the implemented information and cyber security management system.

Learning outcomes

LO1. Freely speak the state language orally and in writing when performing professional duties.
LO2. Communicate in a foreign language in order to ensure the effectiveness of professional communication.
LO3. Apply the principle of inadmissibility of corruption and any other manifestations of dishonesty in professional activity.
LO4. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness.
LO5. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.
LO6. Adapt to new conditions and technologies of professional activity, predict the end result.
LO7. Apply and adapt information and coding theories, mathematical statistics, numbers, cryptography and steganography, signal processing and transmission, etc., principles, methods and concepts of cybersecurity and information protection in training and professional activity.
LO8. Apply knowledge and understanding of mathematics and physics in professional activity, formalize the objectives of the subject area of cybersecurity and protection of information, formulate their mathematical production and choose a rational method of solution.

LO9. To know and apply the legislation of Ukraine and international requirements, practices and standards for the purpose of conducting professional activity in the field of cybersecurity and information protection.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 32 hours, laboratory classes - 32 hours, self-study - 56 hours.

Course prerequisites

Introduction to the specialty. Introductory practice.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1. The concept of information security of the state and components of national interests of Ukraine in the information sphere.
Goals and objectives of the educational discipline "Information security of the state". The place of discipline in the training process of a cyber security specialist. The structure and content of the thematic plan for studying the discipline; educational and methodical literature. Peculiarities of studying the discipline; forms of control of students' knowledge, abilities and skills.
Topic 2. Basic provisions of information security.
The main components of information security of the state. Classification of types of state information security. Types of information security. Threats to information security of Ukraine. Doctrine of information security of Ukraine. State policy priorities in the information sphere.
Topic 3. Information security threats.
Destabilizing factors of information security. Classification of threats to information security. Actual threats to the national security of Ukraine. Manipulation of consciousness, essence and types of manipulation. The role and place of manipulation in national systems of public administration and political systems, as well as in the formation and implementation of international relations. The essence and manifestations of informational violence. Problematic issues of legal prevention of informational violence.
Topic 4. Basics of information warfare.
Basic concepts of information warfare. The concept of information warfare. Basics, forms and principles of cyber intelligence. Basics of cybernetic influence.
Topic 5. Cybernetic weapons.
Classification of cybernetic weapons. The main tasks that rely on cyber weapons. The object of cybernetic influence and its constituent elements. Methods and means of using cybernetic weapons.
Topic 6. Psychological warfare and informational and psychological security of the state.
Basic concepts, goals and objectives of psychological warfare. Types of psychological influence. Forms of psychological warfare. Special methods and techniques of psychological warfare. Basics of informational and psychological security of the state. Principles of security in the psychosphere. Forces and means of information and psychological security.
Topic 7. Information security manager.
A brief overview of the problem of risk management. Integration of risk management in the system development life cycle (sdlc). Life cycle of IT systems. Risk assessment methodology. Risk reduction. General consistency of actions in risk reduction methodology. Profitability analysis and residual risk. Key factors of successful risk management.
Topic 8. Risk management system.
Computer security and incident response team.

Topic 9. Incident management systems.
Statistics. ITIL international standard. ITSM components. Scope of use of ITSM. Principles of ITSM. The main goals of ITSM service support processes. Incident management according to the ITIL standard. The main stages of incident management according to the ITIL standard. Top 5 biggest cyber threats in the world. The concept of building an effective IS incident management system. Structure of a typical automated IS incident management system.
Topic 10. Protection of personal data.
General concepts and definitions. Elements of personal data information systems. Classification of personal data security threats. The composition of the elements of the description of the threats of the NSD. External offender. The internal violator. Vulnerabilities of individual protocols of the TCP/IP protocol stack. General characteristics of threats of NSD in the operational environment of ISPD. General characteristics of threats based on network interaction. Stages of threat implementation. Non-traditional information channels. Social networks.
Topic 11. Principles of information protection when connecting to the Internet.
Evolution of cyber threats. An example of a targeted attack. Death Chain: After infection. ISO/OSI open systems. Dynamics of DDOS attacks by industry. Attack Amplification. Reduction of time for mass hacking. Information threat model for the Internet node when conducting typical remote attacks. Classification of viruses. Information threat model for the Internet node when conducting typical remote attacks. Scheme of creating a TSR connection. The implementation scheme of the "imposing a false route" attack using the ICMP protocol to intercept traffic. The implementation scheme of the "introduction of a false DNS server" attack by intercepting a DNS request. SQL injection. CLICKJACKING technique. ARP-SPOOFING ATTACK. Social engineering. Mechanism of work of antiviruses.

Topics of the workshops

This field is filled in the same way if the curriculum includes workshops.

Topics of the laboratory classes

Topic 1. Comparison of data using a hash.
Topic 2. Methods and ways of collecting and processing information. What was done?
Topic 3. Creating and saving reliable passwords.
Topic 4. Backing up data to external storage.
Topic 5. Information conflict. Who owns your data?
Topic 6. Analytical provision of information security. Explore the risks of your online behavior (teamwork).
Topic 7. Classification of software and cryptographic means of ensuring information security.
Topic 8. Electronic identification of users. Normative provision of information security. Security threats.
Topic 9. System classification and characteristics of technical means of ensuring information security.
Topic 10. International standards and recommendations in the field of information security.

Self-study

A student's independent work is one of the forms of organization of learning, the main form of mastering educational material in free time from classroom training. During independent work, students study lecture material, do individual homework, prepare for tests, tests and exams. Students are also recommended additional materials (videos, articles) for self-study and analysis.

Non-formal education

Within the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the case of independent completion of professional courses/trainings, civic education, online education, vocational training, etc.
In particular, certain topics of this component can be taken into account in case of successful completion of the following CISCO courses:
Cyber Ess
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. Yevseiev S.P., Ostapov S.E., Korol O.H. Cyber security: modern protection technologies: training. manual for students higher education closing Lviv: "Novy Svit-2000", 2019. - 678 p. https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Bogush V. M., Yudin O. K. Information security of the state. - K.: "MK-Press", 2005. - 432 p.
3. Terminological guide on issues of technical protection of information / Kozhenevskyi S.R., Kuznetsov G.V., Khoroshko V.O., Chirkov D.V. / Under the editorship Prof. V.O. Good girl - K.: DUIKT, 2007. - 365 p.
4. Bobalo Yu.Ya., Horbaty I.V. (ed.) Information security. Tutorial. — Lviv: Publishing House of Lviv Polytechnic, 2019. — 580 p. — ISBN 978-966-941-339-0. https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
5. Information security of the state: education. manual for students special 6.170103 "Information security management", 125 "Cyber security"/ V.I. Guryev, D.B. Mehed, Yu.M. Tkach, I.V. Firsova. – Nizhin: FOP Lukyanenko V.V. TPK "Orkhideya", 2018. - 166 p.

Additional literature:

1. On the protection of information in information and telecommunication systems: Law of Ukraine dated 07.05.1994 No. 80/94-VR. Date of update: 12/31/2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI. Update date: 10/27/2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Decree of the President of Ukraine: On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine dated May 6, 2015 No. 287/2015. Date of update: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
4. On national security: Law of Ukraine dated June 21, 2018 No. 2469-VIII. Date of update: 03/31/2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. . ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/ru/contents/data/standard/08/28/82875.html
6. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html
7. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html.
8. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Points are awarded according to the following ratio:
- laboratory work: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- test: 40% of the semester grade.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic integrity and course policy

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU "KhPI": to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed in academic groups with a lecturer, and if it is impossible to resolve the conflict, they should be brought to the attention of the Institute's management.
Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU "KhPI" are available on the website: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by

17.01.2025 — Head of the department
Serhii YEVSEIEV

17.01.2025 — Guarantor of the educational program
Serhii YEVSEIEV