Syllabus
Course Program

Physical bases of technical intelligence means

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

Stanislav MILEVSKYI

Stanislav.Milevskyi@khpi.edu.ua
Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 100 scientific and educational and methodological works. Scientific Guarantor of the educational and scientific program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Fundamentals of Mathematical Modeling of Security Systems", "English in Academic Applications", "Modeling of Cyber-Physical Actions" for undergraduate and graduate students.

More about the lecturer on the department's website

Roman KOROLEV

roman.korolev@khpi.edu.ua
Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 80, including 12 utility model patents, 1 collective monograph, 2 training manuals, 65 articles in foreign publications and specialized publications of Ukraine, 5 of them in the Scopus scientometric database. Leading lecturer in the disciplines: "Wireless and mobile security", "Fundamentals of steganography", "Business intelligence", "Physical foundations of technical means of intelligence" for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Physical foundations of technical means of intelligence" is a mandatory educational discipline. The discipline is aimed at the student's acquisition of theoretical knowledge and practical skills regarding the physical foundations of technical means of intelligence in the field of cyber defense.

Course objectives and goals

Mastering by students of the system of fundamental theoretical knowledge, applied skills of using the basic fundamental physical ideas about the products of information technology and various technical means of intelligence, practical work with a wide range of modern physical and electronic devices, the development of independent thinking of students, necessary for their future, career.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - exam.

Competencies

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.
GC5. Ability to learn and master modern knowledge.
GC-5. Ability to search, process and analyze information.
PC 9. Ability to apply methods and means of technical protection of information at objects of information activity.

Learning outcomes

LO1. Freely speak the state language orally and in writing when performing professional duties.
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.
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.
LO20. Identify the threats of creation of technical channels of leakage of information on the objects of information activity; to implement the means and measures of technical protection of information from leakage by technical channels, to maintain and control the status of hardware means of information protection and complexes of technical protection of information.

Student workload

The total volume of the course is 150 hours (5 ECTS credits): lectures - 32 hours, laboratory classes - 32 hours, self-study - 86 hours.

Course prerequisites

Higher mathematics, Basics of programming.

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. Physical foundations of information protection.
Protection of information from leakage through technical channels. Engineering and technical protection of information. Technical means of protecting language information.
Topic 2. Principles of functioning of cyber intelligence channels of unauthorized information acquisition.
Principles of cyber intelligence.
Topic 3. Principles of functioning of cyber intelligence channels of unauthorized information acquisition.
Channels of unauthorized receiving of information.
Topic 4. Acoustic reconnaissance.
Classification of acoustic channels of information leakage. Physical nature, medium of distribution and method of interception of information. Physical converters. Impact of dangerous acoustic signals on technical systems.
Topic 5. Directions of ensuring information security.
Classification of technical channels of information leakage. Channels of computer information leakage. Material channels of information. Communication lines.
Topic 6. Methods and means of information destruction.
Industrial obstacles. Special force effect. Special force influence on the power supply network. Viral methods of destroying information.
Topic 7. Technical methods and means of information protection.
Classification of technical means of protection. Protection from radio bookmarks. Methods and means of protection against radio microphones. Protection from laser acoustic reconnaissance systems. Protection of communication lines. Methods of detecting information interception equipment. Equipment for the protection of telephone channels. Screening of premises. Means of information protection. Principles of building information protection systems. Information protection software.
Topic 8. Software methods of information protection.
External protection programs. Problems of regulating the use of resources. Software protection programs. The method of determining the fact of information intervention.
Topic 9. Ways and means of unauthorized obtaining of information from automated systems.
Unauthorized obtaining of information from automated systems. Protection of information in automated systems. Information protection methods.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Physical foundations of information protection.
Topic 2. Principles of functioning of cyber intelligence channels of unauthorized information acquisition.
Topic 3. Acoustic reconnaissance.
Topic 4. Directions of ensuring information security.
Topic 5. Methods and means of information destruction.
Topic 6. Technical methods and means of information protection.
Topic 7. Software methods of information protection.
Topic 8. Ways and means of unauthorized obtaining of information from automated systems.

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.
Subjects are not considered for this component in case of successful completion of the courses.

Course materials and recommended reading

Basic literature:

1. Laptev O.A., Savchenko V.A., Shuklin G.V. Identification and blocking of means of covertly obtaining information at the objects of information activity: Training manual. - Kyiv: DUT, 2020. - 126 p. https://f.eruditor.link/file/3323808/
2. Ivanchenko S.O., Havrylenko O.V., Lipskyi O.A., Shevtsov A.S. Technical channels of information leakage. Procedure for creating complexes of technical protection of information: Training manual. - Kyiv: NTUU, 2016. - 104 p.
https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content
3. Jacobson D., Idziorek J. Computer security literacy: staying safe in a digital world. - CRC Press, 2016. Sloan R., Warner R. Unauthorized access: The crisis in online privacy and security. - Taylor & Francis, 2017. - P. 401.
https://api.pageplace.de/preview/DT0400.9781439856192_A24452808/preview-9781439856192_A24452808.pdf
4. Iniewski K. (ed.). Semiconductor radiation detection systems. - CRC press, 2018.
https://www.taylorfrancis.com/books/edit/10.1201/9781315218373/semiconductor-radiation-detection-systems-krzysztof-iniewski
5. Mitra S., Gofman M. (ed.). Biometrics in a data-driven world: trends, technologies, and challenges. - CRC Press, 2016.
https://www.perlego.com/book/2051516/biometrics-in-a-data-driven-world-trends-technologies-and-challenges-pdf
6. Digital circuitry and architecture of microprocessors: a study guide / Yevseev S.P., Zhenyuk N.V., Okhrimenko M.Yu. etc. - Kharkiv, - Lviv: Publishing House of PP "Noviy Svit - 2000", 2023. -513 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Yevseyev S.P. CYBER SECURITY: LABORATORY PRACTICUM ON THE FUNDAMENTALS OF CRYPTOGRAPHIC PROTECTION / S.P. Yevseev, O.V. Milov, O.G. Korol - Lviv: "New World-2000", 2020. - 241 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Additional literature:

1. Petersen J.K., Taylor P. Handbook of surveillance technologies. - CRC press, 2012.
https://books.google.com.ua/books/about/Handbook_of_Surveillance_Technologies.html?id=Cj_3DwAAQBAJ&redir_esc=y
2. Ball K., Haggerty K., Lyon D. Routledge handbook of surveillance studies. - Routledge, 2012.
https://books.google.com.ua/books/about/Routledge_Handbook_of_Surveillance_Studi.html?id=F8nhCfrUamEC&redir_esc=y
3. Military intelligence: textbook / compilers: D. V. Zaitsev, A. P. Nakonechny, S. O. Pakharev, I. O. Lutsenko; edited by V. B. Dobrovolsky. - Kyiv: Publishing and Printing Center "Kyiv University", 2016. - 335 p.
4. Chen L., Gong G. Communication system security. - CRC press, 2012.
https://books.google.com.ua/books/about/Communication_System_Security.html?id=nmjRBQAAQBAJ&redir_esc=y
5. Mallett X., Blythe T., Berry R. (ed.). Advances in forensic human identification. - CRC Press, 2014.
https://api.pageplace.de/preview/DT0400.9781439825167_A23982999/preview-9781439825167_A23982999.pdf
6. Dardari D., Falletti E., Luise M. (ed.). Satellite and terrestrial radio positioning techniques: a signal processing perspective. - Academic Press, 2012.

7. Sapse D., Kobilinsky L. (ed.). Forensic science advances and their application in the judicial system. - CRC Press, 2011.
https://books.google.com.ua/books/about/Forensic_Science_Advances_and_Their_Appl.html?id=mXMVCzZZxIwC&redir_esc=y
8. Murphy M. J. (ed.). Adaptive motion compensation in radiotherapy. - CRC Press, 2011.
https://books.google.com.ua/books/about/Adaptive_Motion_Compensation_in_Radiothe.html?id=qVPRBQAAQBAJ&redir_esc=y.

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;
- exam: 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