Syllabus
Course Program

Fundamentals of building and protecting microprocessor systems

Specialty
125 – 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
5

Language of instruction
English

Lecturers and course developers

Serhii POHASII

Serhii.Pohasii@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 95, including 2 utility model patents, 6 monographs, of which 4 are collective monographs, 4 teaching aids, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 65 articles in foreign publications and specialized publications of Ukraine, with 11 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Analog and digital electronic devices", "Internet of things and services", "Security of cloud technologies", "Fundamentals of construction and protection of modern operating systems", "Modeling of critical infrastructure systems", "Fundamentals of construction and protection of microprocessor systems ", "Security of smart technologies and Internet of things", "Information and communication systems in the field of national security" for undergraduate and graduate students, Section "Information security of cloud services", "Modern methods of protection of socio-cyber-physical systems", "Modeling of mechanisms cyber security" for graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Fundamentals of building and protecting microprocessor systems" is a mandatory educational discipline. The discipline is aimed at teaching students the skills of designing systems based on microcontrollers, as the most common type of microprocessor systems. For its implementation, descriptions of microcontrollers of the AVR family, as well as special software design tools, are given, examples of solutions to the design problems of several devices are considered.

Course objectives and goals

Teaching students the basics of knowledge needed by future specialists-practitioners in the field of microprocessor technology, building complex information protection systems based on the synthesis of organizational and technical measures in the conditions of modern cyber threats.

Format of classes

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

Competencies

GC-1. Ability to apply knowledge in practical situations.
GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-4. Ability to identify, state and solve problems in a professional manner.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems.
PC-4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and refusal of various classes and origins.
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.

Learning outcomes

LO-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LO-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LO-3. Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity.
LO-4. 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.
LO-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LO-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LO-7. 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 cyber security.
LO-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LO-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LO-10. Perform analysis and decomposition of information and telecommunication systems.

LO-11. Perform analysis of connections between information processes on remote computer systems.
LO-12. Develop threat and intruder models.
LO-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by hardware and software tools and evaluate the effectiveness of the quality of the decisions made.
LO-15. Use modern hardware and software of information and communication technologies.
LO-16. Implement complex information security systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. Ensure the processes of security 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 security of electronic information resources with a reflection of relationships and information flows, processes for internal and remote components.
LO-18. Use software and software-hardware complexes for the security of information resources.
LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LO-21. Solve tasks of provision and support (including: review, testing, accountability) of the access control system according to the stated security policy in information and telecommunication (automated) systems.
LO-22. Solve the management procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and/or cyber security.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LO-24. Solve the problems of managing access to information resources and processes in information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based).
LO-25. Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and telecommunication (automated) systems using event registration logs, their analysis and stated protection procedures.
LO-26. Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems.
LO-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.
LO-29. Evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means under the conditions of realization of threats of various classes.
LO-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.
LO-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LO-32. Solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the stated security policy.
LO-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LO-34. Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization.
LO-35. Solve the tasks of providing and supporting complex information security systems, as well as countering unauthorized access to information resources and processes in information and information-

telecommunication (automated) systems in accordance with the stated policy of information and/or cyber security.
LO-36. Detect dangerous signals of technical means.
LO-37. Measure the parameters of dangerous and interfering signals during the instrumental control of information security processes and determine the effectiveness of information security against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system.
LO-38. Interpret the results of special measurements using technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information security system.
LO-39. Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents.
LO–40. Interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information security system.
LO-41. Ensure the continuity of the event and incident logging process based on automated procedures.
LO-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LO-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LO-44. Solve the problems of ensuring the continuity of the organization's business processes on the basis of risk management theory and the stated information security management system, in accordance with national and international requirements and standards.
LO-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LO-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LO-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
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 the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.
LO-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LO-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LO-52. Use tools for monitoring processes in information and telecommunication systems.
LO-53. Solve problems of software code analysis for the presence of possible threats.
LO-54. Be aware of 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.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 16 hours, laboratory classes - 32 hours, self-study - 72 hours.

Course prerequisites

Programming tools.

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. Programmable logic integrated circuits, general information, principle of operation, development tools, scope of application.
Differences between microprocessors and FPGAs, the structure of microprocessors. General information about PLIS. FPGA structure, CPLD structure, FPGA structure. Scope of FPGA application. Development tools. Application of FPGAs for digital signal processing. The cost of FPLIS. The main companies are manufacturers of FPGAs.
Topic 2. Software and hardware architecture of IA-64 Intel processors.
Computer architecture. Architecture IA-64. Variants of the microarchitecture of Intel processors. Program model IA-64.
Topic 3. Principles of using number systems.
General information of the binary, hexadecimal, decimal number system. Translation of numbers from one number system to another. Translation of fractional numbers. Translation of numbers with a sign.
Topic 4. Assembler programming language.
General information about the assembly language. Data types. Stages of creating an Assembler program.
Topic 5. Assembler syntax.
Assembler syntax. Operands Expression operands. Segmentation directives. Simple assembly data types.
Topic 6. Microcontrollers ATMEL Mega family.
General information about microcontrollers. RISC and CISC microcontroller architectures. The structure of the atmega16 microcontroller. Development tools.
Topic 7. Ports of AVR ATMEL microcontrollers of the Mega family.
General information about microcontroller ports, functional and principle diagram of the port. Atmega16 microcontroller input/output registers.
Topic 8. ATMEL microcontroller timers of the Mega family.
General information about the timer. The structure of timers, operating modes. Timer programming.
Topic 9. Analog-to-digital converter (ADC) ATMEL Mega family.
Types of ADC. The structure and principle of operation of the built-in ADC MK atmega 16. Description of the registers MK atmega16.
Topic 10. Universal ATMEL serial receiver of the Mega family.
The structure and principle of operation of the built-in USART microcontroller. Description of the USART registers of the AVR ATMEL Mega family microcontroller.
Topic 11. Implementation of typical P, PI, PID regulators on MK.
SPR structure. Implementation of a digital integrator and differentiation link. Digital proportional (P), proportional-integral (PI), proportional-integral-differential (PID) regulators.
Topic 12. Microprocessor implementation of transmission functions.
Mathematical model, transfer function (PF), discrete transfer function. Implementation of the transfer function in the Assembler programming language.
Topic 13. Basic operations of digital signal processing (DSP).
The most frequently used operations in Central Hospital.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Acquaintance with software products AVR studio, Proteus.
Topic 2. Work in FASM software.
Topic 3. Input/output of data in binary, eight-year and sixteen-year numbering systems.
Topic 4. Features of assembly language programming. Compiler directives. Stack memory. Interrupt vectors.
Topic 5. Microcontroller command system. Operand types and basic result flags.

Topic 6. Control interception. Interrupt processing.
Topic 7. Integration of the Assembler programming language.
Topic 8. Basic microcontroller commands. Data addressing.
Topic 9. Work with external interrupts MK AVR.
Topic 10. Working with timers/counters MK AVR.
Topic 11. MK AVR analog-digital converter.
Topic 12. Connection of a universal ATMEL serial receiver of the Mega family.
Topic 13. 1-Wire interface.
Topic 14. Temperature sensor DS18B20 3.
Topic 15. Main directions of digital signal processing (DSP).

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. Zhuykov V.Ya., Tereshchenko T.O., Peterger Yu.S. etc. "Microprocessors and microcontrollers" - Electronic textbook [Electronic resource]. – Access mode: http://www.kaf-pe.ntu-kpi.kiev.ua/. - Zhytomyr: Publication of ZhDU named after I. Franka, 2015. - 226 p.
2. Schematics of electronic systems. Volume 3. Microprocessors and microcontrollers / V.I. Boyko, O.M. Gurzhii, V.Ya. Zhuykov, O.O. Zori, Yu.S. Petergera, V.M. Spivak, T.O. Tereshchenko, Yu. Yakymenko .AND. - K.: Higher School, 2004. - 399 p.: illustrations.
https://pdf.lib.vntu.edu.ua/books/2015/Boiko_P3_2004_399.pdf
3. Yevseev S.P., Smirnov O.O., Korol O.G., Kovalenko O.V. Architecture of microprocessors and computer components. Kirovohrad: Ed. V.F. Lysenko, 2015. - 550 p.
4. 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/file/d/1fTWF7v4v-aaCL_oHMSHsyIJOrNlEu9v-/view.

Additional literature:

1. Microprocessor devices: training. a manual for students of the "Electronics" specialty / T. O. Tereshchenko, V. A. Todorenko, L. M. Batrak, Yu. S. Yamnenko. - K.: Department, 2017. - 244 p. ISBN 978-617-7301-37-9
https://ela.kpi.ua/server/api/core/bitstreams/70ca26dd-6e59-4e5d-878f-7f5e89d943c8/content
2. 8-bit AVR Instruction Set Manual [Electronic resource]. – Access mode: (http://www.atmel.com/images/doc08S6.pdf).
3. Knut Donald Ege. The art of programming. T. 2. Received algorithms. - Kyiv: William, 2005
http://lib.ysu.am/disciplines_bk/f0f17bee2596e0d913b92ae336317ffa.pdf.

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

28.08.2024

Head of the department
Serhii YEVSEIEV

28.08.2024

Guarantor of the educational program
Serhii YEVSEIEV