Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Department of Applied Radio Electronics

[RE-347] INFORMATION SECURITY IN INTELLIGENT RADIO ELECTRONIC SYSTEMS

Curriculum of the academic discipline (Syllabus)

Course details

Level of higher education	First (bachelor's)
Field of knowledge	G Engineering, Manufacturing and Construction
Specialization	G5 Electronics, Electronic Communications, Instrument Engineering and Radio Engineering
Educational program	Intelligent technologies of radio electronics
Discipline status	Regulatory
Form of higher education	Full-time
Year of training, semester	4th year, spring semester
Scope of the discipline	4 credits (Lectures 20 hours, Practical 30 hours, Laboratory hours, Independent work 70hours)
Semester control/control measures	Credit
Class schedule	https://schedule.kpi.ua
Language of instruction	Ukrainian
Information about the course coordinator/teachers	Lecturer: D. O. Navrotsky, Practical instructor: M. M. Stepanov
Course location	

Curriculum

1. *Description of the academic discipline, its purpose, subject matter, and learning outcomes*

The course "Information Protection in Intelligent Radio-Electronic Systems" is designed to provide students with knowledge and skills in ensuring the protection of information that circulates and is processed in intelligent radio-electronic systems and telecommunications systems and networks in order to implement established information security policies. This is achieved by studying the theoretical foundations of the construction and practical application of methods and means of information protection in intelligent systems in order to prevent unauthorized access, leakage, destruction, and modification of information of various categories through the implementation of policies and the creation of comprehensive corporate information protection systems.

The discipline provides the following general, professional competencies, and program learning

outcomes:

GC 01 Ability to think abstractly, analyze, and synthesize

GC 02 Ability to apply knowledge in practical situations.

GC 04 Knowledge and understanding of the subject area and understanding of professional

activity.

GC 07 Ability to learn and master modern knowledge.

PC 01 Ability to understand the essence and significance of information in the development of a modern information society

PC 02 Ability to solve standard tasks of professional activity based on information and bibliographic culture with the use of information and communication technologies and taking into account the basic requirements of information security

PC 03 Ability to use basic methods, techniques, and tools for obtaining, transmitting, processing, and storing information

PC 14 Readiness to study scientific and technical information, domestic and foreign experience on the subject of investment (or other) projects in telecommunications and radio engineering.

PC 18 Ability to assess the place and advantages of introducing elements of intelligent technologies and intelligent radio electronics into various fields of human activity

PC 20 Ability to select methods and means of information processing using intelligent technologies.

PC 24 Ability to develop algorithms and implement them in software-configurable radio-electronic systems

PLO 01 Analyze and make informed decisions when solving specialized tasks and practical problems in telecommunications and radio engineering, which are characterized by complexity and incomplete certainty of conditions

PLO 13 Apply fundamental and applied sciences to analyze and develop processes occurring in telecommunications and radio engineering systems

PLO 18 Find, evaluate, and use information from various sources necessary to solve professional tasks, including reproducing information through electronic search

PLO 21 Ensure reliable and high-quality operation of information and communication networks, telecommunications and radio engineering systems

PLO 24 Implement digital signal processing methods at the software and hardware levels

PLO 25 Select and implement means and methods of information transmission in communication networks and apply network technologies

PLO 27 Apply basic methods and techniques for obtaining information

2. *Prerequisites and post-requisites of the discipline (place in the structural-logical scheme of training under the relevant educational program)*

The discipline "Information Protection in Intelligent Radio-Electronic Systems" is based on the disciplines: "Communication Means in Intelligent Radio-Electronic Systems".

As a result of studying the discipline "Information Protection in Intelligent Radio-Electronic Systems," students acquire the skills of qualified specialists in information protection and will be able to use them in "Diploma Design."

3. *Contents of the course*

Topic 1. Information security issues

Lab1 Identification of threats to economic activity

Topic 2. Characteristics of information security threats. Unauthorized access.

Lab2 Development of threat models

Lab3 Development of intruder models

Topic 3. Ways to ensure information security

Lab4 Enterprise security management system.

Lab5 Secure programming methods.

Lab6 Identification and elimination of security

vulnerabilities.

Topic 4. Information security policy.

Lab7 Information security policy as a component of information and communication systems security.

Lab8 Security policy models.

Topic 5. Cryptographic methods of information protection.

Lab9 Block ciphers.

Lab10 RSA encryption algorithm

Topic 6. Assessment of the security of information and communication

systems.

Lab11 Protection of systems against confidentiality breaches

Lab12 Protection of systems against availability breaches

4. *Teaching materials and resources Basic literature*

1. Zhilin, A. V. Information protection technologies in information and telecommunications systems: textbook. / A. V. Zhilin, O. M. Shapoval, O. A. Uspensky; ISZSI Igor Sikorsky KPI. – Kyiv: Igor Sikorsky KPI, Polytechnika Publishing House, 2021. – 213 p.

https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf

2. Demchynskyi, V. V. Fundamentals of Information Security Technologies [electronic resource]: V. V. Demchynskyi, M. V. Hraivoronskyi, O. V. Kireienko/Textbook/ Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2022. 107 p.

https://ela.kpi.ua/bitstream/123456789/53203/1/OTZI_Practices_plan_v115.pdf

3. Kushneryov, O. S. Information Security [Electronic resource]: lecture notes / O. S. Kushneryov. — Sumy: SumDU, 2021. — 99

p. https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf

Supplementary literature

4. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. –Springer International Publishing, 2017. – ISBN 978-3-319-46528-9 (print); 978-3-319-46529-6 (online). 127 p.

5. Tarnavskyi Yu.A. Information Protection Technologies [electronic resource]: textbook for students majoring in 122 "Computer Science"/ Kyiv: KPI, 2018. 162 p. https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

Information resources on the Internet

1. State Service for Special Communications and Information Protection of Ukraine -https://cip.gov.ua/ua

2. Obodyak V.K. Materials of the training course "Information Protection Technologies" on the MIH platform - https://mix.sumdu.edu.ua/textbooks/66503/index.htm

Educational content

5. *Methodology for mastering the academic discipline (educational component)*

Topic 1. Information protection issues

Periods of development of information security theory in computer systems and networks. Basic approaches to considering issues of information security theory. Basic principles of information security. Ensuring compliance with the requirements of confidentiality, integrity, authenticity, and availability of information. OSI network model. General characteristics of security problems in distributed intelligent systems. Models of distributed systems in access control processes.

Lab1 Identification of threats to economic activity Identification of threats to economic activity

Topic 2. Characteristics of information security threats. Unauthorized access.

Security violators. Characteristics of information security threats. Violation of confidentiality, integrity, and availability of information. Classification of information security threats. Threat of disclosure. Methods of unauthorized access. Threat of integrity violation. Threat of denial of service. Security violators. Violator model.

Lab2 Development of threat models. Development of information security threat models.
Lab3 Development of attacker models.Development of intruder models in the information environment

Topic 3. Ways to ensure information security. Ways to ensure information security. Principles of creating secure software. The concept of information protection. Information protection strategy and architecture. Use of a set of measures aimed at preventing and eliminating software vulnerabilities.

Lab4 Enterprise security management system. Enterprise security management (security system structure and security concept structure).
Lab5 Secure programming methods. Use of secure programming methods. Their combination with a secure execution environment.
Lab6 Identification and elimination of security flaws. Use of static and dynamic analysis tools to identify and eliminate security flaws.

Topic 4. Information security policy. Information security policy. Security policy models. Information security policies. Security policy measures. Security policy implementation. Security policy support. Discretionary security policy. Mandatory security policy. Role-based security policy. Security monitor.

Lab7 Information security policy is a component of the security of information and communication systems. Development of information security policy.
Lab8 Security policy models. Protecting software from unauthorized access.

Topic 5. Cryptographic methods of information protection. Fundamentals of encryption theory. Block ciphers. Asymmetric data encryption. Basic provisions and definitions. Characteristics of encryption algorithms. The concept of block ciphers and the principles of their construction. Feistel schemes. Advanced Encryption Standard (AES). Implementation of AES. Block cipher operating modes. Mathematical foundations of RSA encryption. RSA key generation. RSA-based electronic signatures. RSA implementation. Diffie-Hellman functions.Hellman functions.
Lab9 Block ciphers.Modeling a code book attack. Block cipher rounds. Substitution-permutation networks and Feistel schemes.
Lab10 RSA encryption algorithm. Generation of RSA keys.

Topic 6. Assessment of the security of information and communication systems.
Assessment of the security of information and communication systems. System of standards for integrated information protection and information security management systems.
Use of standards for designing and assessing comprehensive information protection systems. General criteria for assessing the security of information technologies. Methods for assessing the reliability of information protection systems against unauthorized access in automated systems

Lab11 Protection of systems against confidentiality breaches. Methodology for evaluating the effectiveness of information protection systems against unauthorized access to ensure data confidentiality

Lab12 Protection of systems against availability breaches. Methodology for assessing the level of readiness of information protection systems against unauthorized access to ensure data availability

6. *Independent work of the student*

Lecture-based learning — in particular, multimedia lectures with detailed presentation of the educational material, combining passive learning methods with elements of active and interactive approaches — is the basis for the formation of independent learning skills in higher education students.

Lectures are supplemented by practice-oriented forms of work, in particular laboratory tasks performed on personal computers. This approach allows students to apply the theoretical knowledge they have acquired to solve specific practical situations.

An important role in the development of independence is played by preparation for lectures and laboratory work, as well as taking into account the teacher's comments when analyzing completed tasks or the work of other students. This contributes to the formation of self-learning skills, improves the ability to plan time effectively, set priorities, and distinguish between the main and secondary.

In addition, students must learn to use the results of their own research, analysis, and synthesis of information from various sources, which develops critical thinking and provides a foundation for further professional growth.

Policy and control

7. *Academic discipline (educational component) policy*

System of requirements for students:

Academic integrity. Compliance with academic integrity by students requires:

• independent completion of educational tasks, current and final assessment tasks
learning outcomes (for persons with special educational needs, this requirement applies taking into account their individual needs and abilities);
• references to sources of information when using ideas, developments, statements, information;

• compliance with copyright and related rights legislation;
• provision of reliable information about the results of one's own educational (scientific, creative) activities, research methods used, and sources of information.

The following are considered violations of academic integrity:

• academic plagiarism - the publication (in whole or in part) of scientific (creative) results obtained by other persons as the results of one's own research (creativity) and/or the reproduction of published texts (published works of art) by other authors without indicating authorship;
• self-plagiarism - the publication (in whole or in part) of one's own previously published scientific results as new scientific results.

For violations of academic integrity, students may be subject to the following academic penalties:

• - retaking an assessment (test, exam, credit, etc.);
• - retaking the relevant educational component of the educational program. **Late** submission **policy.** Late assignments will be penalized by 10 points from the total number of points for that assignment.

Note: Exceptions may be made for assignments submitted late for valid reasons.

Attendance policy. Attendance at classes is mandatory. For objective reasons (e.g., pandemic, illness, international internship), training may take place online in agreement with the course instructor. Lectures and practical classes are held in accordance with the current regulations of Igor Sikorsky KPI. Attendance is mandatory. To pass the exam automatically, you need to score more than 60 points, which can be obtained by completing mandatory tasks (completing coursework, practical work, and writing a module test) and systematically attending lectures (passing a quick test based on the lecture materials). Points for work during the lecture are awarded based on a quick quiz. Each test contains two questions on the lecture material, and the correct answer to each question is worth two points.

The modular test is conducted in writing. Each task in the test contains 2 theoretical questions and 1 problem, the correct answers to which will earn up to 100 points for each theoretical question and 100 points for the practical question. The final grade is the average of the points received.

An individual assignment (DKR) consists of solving 5 homework assignments during the semester (one assignment for each subsequent class), the correct solution of which will earn up to 100 points for each assignment. It is completed in writing during independent work hours.

The exam is written. The exam ticket consists of 3 tasks (2 theoretical questions and 1 task) on the topics covered in the classroom and separate questions for independent study.

8. *Types of assessment and the learning outcomes assessment rating system (LOAS)*

A student's grade in a subject consists of the points they receive during the semester:

1. the average number of points for attendance and answers in lectures;
2. average score for completing modular, independent, and homework assignments;
3. average score for completing and defending laboratory and practical work;
4. the sum of bonus and penalty points.

Completion and defense of all practical and laboratory work, as well as a positive grade on tests on individual sections, are required for admission to the final exam.

Practical, laboratory, modular, homework, and independent assignments:

"excellent", comprehensive answer (at least 95% correct information) from 95 to 100 points;

"Very good," complete answer, minor inaccuracies possible (at least 85% correct information) from 85 to 94 points;

"good", complete answer, minor inaccuracies possible (at least 75% correct information) from 75 to 84 points;

"satisfactory", incomplete answer (but not less than 60% correct information) and minor errors from 60 to 74 points;

"unsatisfactory," unsatisfactory answer (incorrect solution to the problem), requires mandatory rewriting at the end of the semester, 0 to 59 points.

The average score out of 100 is calculated for all work throughout the semester.

Bonus points

In total, no more than 10:

– for completing creative work from the credit module (e.g., participation in faculty and institute academic competitions, participation in contests, preparation of reviews of scientific works, etc.); successful completion of a recommended distance learning course (corresponding to the topics of the discipline) with the receipt of a corresponding certificate; for active participation in lectures (important questions, additions, comments on the lecture topic) from 1 to 5 points;

– presentation on the topic of independent study – from 1 to 5 points.

Credit:

The condition for admission to the exam is the completion of all laboratory and practical work, and a semester starting rating of $54 \leq R_{average} \leq 80$.

Students who have fulfilled the admission requirements may take the exam if they are not satisfied with their overall (average) grade for the semester.

Exam grading system:

The exam is graded on a scale of R_{exam} to 40 points. The exam consists of four tasks. Each task is graded according to the following criteria:

"excellent" – comprehensive answer (at least 95% correct information), relevant reasoning provided – 10 points;

"Good" – complete answer (at least 80% correct information) that meets the requirements for the "skills" level, or contains minor inaccuracies – 8 points;

"Satisfactory" – incomplete answer (at least 60% correct information and some errors) – 6 points;

"Unsatisfactory" – no correct answer – 0 points.

The rating sum ($R_{total}=R_{average}+R_{credit}+R_{incentive}-R_{penalty}$) is converted to a grade according to the table:

Table of correspondence between rating points and grades on the university scale

Number of points	*Rating*
100-95	Excellent
94	Very good
84	Good
74-65	Satisfactory
64-60	Sufficient
Less than 60	Unsatisfactory
Admission requirements not met	Not admitted

9. *Additional information on the discipline (educational component)*

1. General issues of information and radio-electronic security

1. Define information security in radio-electronic intelligent systems and its main components.
2. What are technical channels of information leakage and what are their main classes?
3. Describe radio-electronic systems as objects of influence by radio-electronic warfare means.
4. What are the main types of threats to information in radio-electronic systems?
5. Explain the concept of "radio-electronic reconnaissance" and its capabilities for intercepting signals.

2. *Signals and models in radio-electronic systems*

1. What are the main signal parameters that affect its detectability in noisy conditions?
2. Explain the model for detecting a deterministic signal against a background of white noise.
3. What is the signal-to-noise ratio (SNR) and how does it affect the noise immunity of the system?
4. List the main methods of spectral analysis of signals and their application in information protection.
5. Explain the features of processing non-stationary signals (STFT, Wavelet).

3. *Methods of radio signal protection*

1. List the main methods for reducing the probability of radio signal interception.
2. The essence of signal masking in radio channels. What is the principle of noise-like signal generation?
3. What is frequency hopping spread spectrum (FHSS) and where is it used?
4. Explain the principle of Direct Sequence Spread Spectrum (DSSS) and its advantages.
5. What types of artificial interference are used to protect information?

4. *Radio-electronic warfare and countermeasures*

1. How do electronic warfare (EW) means work to suppress communication channels?
2. What parameters affect the effectiveness of radio communication channel suppression?
3. Explain the methods for improving the noise immunity of receivers.
4. Describe the principles of assessing radio signal interception by RTR means.
5. What are the features of protecting sensor networks from signal interception?

5. *Cryptographic and hardware protection methods*

1. What is the significance of cryptography in radio-electronic intelligent systems?
2. Explain the difference between symmetric and asymmetric encryption methods in radio channels.
3. What hardware can be used to protect communication channels?
4. What are TPM and HSM, and what is their role in ensuring cyber and radio security?

5. What are the advantages and disadvantages of signal protection by reducing its reception area?

6. *Monitoring, analysis, and security assessment*

1. Methods for assessing the probability of signal interception in radio intelligence conditions.
2. What metrics are used to evaluate signal masking effectiveness?
3. How does mathematical modeling help in assessing the security of radio-electronic systems?
4. Tell us about statistical methods for signal analysis and detection of hidden transmissions.
5. What are the principles of forming secure channels in intelligent radio-electronic systems?

Description of the material, technical, and informational support for the discipline

Multimedia, video and audio playback, projection equipment (video cameras, projectors, screens, smart boards, etc.). Computer lab for laboratory classes, computers, computer systems, and networks. Software to support distance learning.

Work program for the academic discipline (syllabus):
Compiled by D. O. Navrotsky; M. M. Stepanov;
Approved by the PRE Department (Minutes No. 06/2025 dated 06/24/2025)
Approved by the methodological commission of the faculty/research institute (protocol No. 06/2025 dated 26.06.2025)