National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Department of Computer Engineering

SOFTWARE SECURITY

Syllabus

Details of the academic discipline

Level of higher education	*First (bachelor's)*
Field of Study	*12 Information technologies*
Specialty	*121 Software Engineering*
Education Program	*Computer Systems Software Engineering*
Type of Course	*Normative (cycle of professional training)*
Mode of Studies	*full-time (full-time), part-time*
Year of studies, semester	*4th year, autumn semester*
ECTS workload	*4 credits/120 hours*
Testing and assessment	*Exam, Modular control work*
Course Schedule	*http://rozklad.kpi.ua/Schedules/ScheduleGroupSelection.aspx*
Language of Instruction	*English*
Course Instructors	*Associate professor, Ph.D. , Volokita Artem Mykolayovych, artem.volokita@kpi.ua* *Assistant professor, Ivanishchev Bohdan Vyacheslavovich , callidus.iv@gmail.com*
Access to the course	*https://campus.kpi.ua* *https://bbb.comsys.kpi.ua/b/art-ts2-8vd-fs0 Access Code : 718630* *https://t.me/+z5IajtX47k0xMGVi*

Program of educational discipline

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

The syllabus of the educational component "Software security" is compiled in accordance with the educational programs of bachelors' training "Computer systems software engineering", "Software information computer systems engineering" in specialty 121 "Software engineering" of the first (bachelor's) level of higher education knowledge 12 Information technologies.

***The purpose of the academic discipline is to form and consolidate the following professional** competencies in students :*

- *PC01 Ability to identify, classify and formulate software requirements.*
- *PC03 Ability to develop architectures, modules and components of software systems.*
- *PC06 Ability to analyze, choose and apply methods and tools to ensure information security (including cyber security).*
- *PC07 Knowledge of information data models, ability to create software for storing, extracting and processing data.*
- *CP14 Ability to algorithmic and logical thinking.*

The purpose of studying the credit module is for the student to acquire practical design and programming skills when creating complex systems or special hardware and software subsystems to protect information from unauthorized access based on:

- *the ability to formalize and use the legal framework for information protection in automated systems, methods and means of access management to distinguish the rights of users to information with limited access,*
- *assimilation of standard means and encryption algorithms for the construction of software and technical support for cryptographic protection of particularly important information and the formation of the necessary key encryption base.*
- *ability to solve analytical problems of generation of large prime numbers, calculation of keys and cryptoresistance of modern symmetric and asymmetric encryption systems and determination of their basic characteristics.*
- *acquisition of techniques for creation and maintenance of appropriate software and technical support for protection of information resources of automated systems.*

The subject of the academic discipline *is methods and means of managing access to information carriers and databases, modern standards and means of encryption for building complex systems for protecting computer systems and networks from intrusions. The credit module is designed to study design methods and techniques for configuring software and technical means of protection of operating systems, which ensure the creation of highly protected distributed computer systems.*

Program learning outcomes, the formation and improvement of which is aimed at discipline:

- *PLO01 Analyze, purposefully search for and select information and reference resources and knowledge necessary for solving professional tasks, taking into account modern achievements of science and technology.*
- *PLO18 Know and be able to apply information technologies for data processing, storage and transmission.*
- *PLO21 To know, analyze, choose, competently apply the means of ensuring information security (including cyber security) and data integrity in accordance with the applied tasks being solved and the software systems being created.*

Knowledge:

the main concepts of creating demonstrably sufficient information protection systems, Adept , Bella-Lapadula and other models, existing mechanisms for implementing protection models implemented in various operating systems based on "mandate lists" and "access lists", ways of implementing the principles of "expanding access rights" and "minimum privileges", standards, algorithms and modes of implementation of cryptographic protection of information, methods and means of generating encryption keys, protocols and stages of authentication of subjects and messages in open communication channels, protocols for conducting conferences and open orders, structure and characteristics of electronic payment systems and plastic payment cards, requirements of well-known standards regarding classification and criteria for protection of computer systems against unauthorized access to information in terms of confidentiality, integrity, availability, controllability.

Skills:

perform the final stages of design when creating or modifying information protection subsystems against unauthorized access and preventing intrusions into computer systems, take into account the requirements for passwords and evaluate the basic characteristics of password protection systems, write a set of programs for discrete management of access to information on media or the site, determine evaluations the complexities of software or hardware implementation of symmetric and asymmetric algorithms of cryptographic protection, evaluate the cryptographic resistance of algorithms, apply methods and algorithms for the formation of digital signatures and key certificates, develop a graphical interface for the security administrator, debug information protection programs, organize their placement and execution on workstations and computers computer network.

2. Prerequisites and postrequisites of the discipline

In order to successfully master the discipline, students are required to master the following educational components: "Programming Fundamentals", "Discrete mathematics", "System programming", "Algorithms and Data Structures", "Software engineering components", "Operating systems", "Computer Systems and Networks Fundamentals".

Competences, knowledge and skills acquired during the study of the educational component can be used for further study of the educational components: "Pre-diploma practice", "Diploma design".

3. Content of the academic discipline

Chapter 1. Introduction

Topic 1.1 Problems of information protection in computer systems and networks (CSM).

Topic 1.2 Main directions of threats to the NSD and channels of information leakage from the KSM. Targets, subjects and schemes of active and passive invasions

Chapter 2. A comprehensive approach to the creation of information protection systems in computer systems.

Topic 2.1 Regulatory framework of information protection. The main directions and means of information protection in KSM.

Topic 2.2 Models of provably sufficient information protection systems. Adept conceptual models . Denning , Landwehr .

La Padula protection system . Concept of subject, rights vector and access manager. Extension of access rights.

Topic 2.4. Model of the KSM safety monitoring system. Concept of threat factor and statistical anomaly.

Section 3. Identification of subjects and access control based on the password system.

Topic 3.1 User identification based on the password system. Password requirements. Password storage scheme in Unix OS .

Topic 3.2 Analysis of the characteristics of the system of simple passwords. Anderson's formula . Examples .

Topic 3.3 Modifications of the password system. Confirmation of access rights based on the one-way and two-way "handshake" procedure.

Topic 3.4 Logs: registration and operational. Logging-based security monitoring on Unix and Windows

Chapter 4. Discrete delimitation of subjects' access to information in the limited matrix model of the protection system.

Topic 4.1 Access lists and formation of user categories. Inheritance of rights. Locks, keys and access conditions in the OS.

Topic 4.2 Mandate lists and implementation of the "minimum privileges" principle. Mandatory access in the Unix OS .

Chapter 5. Computer approaches to cryptographic protection of information with limited access.

Topic 5.1 Encryption based on one and many alphabetic substitutions. Concept of cipher and secret key. Caesar's Cipher

Topic 5.2 Encryption based on permutations. Problems of decryption and cryptanalysis

Topic 5.3 Bigram ciphers. Viginer cipher and Wheatstone squares . Encryption machines

Topic 5.4 Stream Ciphers with Unlimited Key Length. Encryption by "throwing".

Chapter 6. Symmetric encryption in communication systems with open communications.

Topic 6.1 Organization of data transfers in secret systems according to Shannon . Means of entropy maximization.

Topic 6.2 Encryption based on alternating permutations and substitutions. Lucifer system .
Topic 6.3 Federal encryption standard DataEncryption Standard. (DES). General scheme and masking function with keywords.
Topic 6.4 Key management unit in DES. 3-DES algorithm and four modes of implementation of DES-based cryptographic protection.

Chapter 7. Asymmetric encryption systems based on public and secret keys.
Topic 7.1 New direction in cryptography according to Diffie and Hellman . Irreversible functions in encryption. Three schemes and tasks of cryptoprotection .
Topic 7.2 The RSA system. Modular arithmetic. Algorithm of fast discrete potentiation . The processor is an RSA accelerator.
Topic 7.3. The problem of generating large prime numbers (LPG). Rabin's test and Fermat's little theorem. Simplicity checks.
Topic 7.4. Key calculation schemes and algorithms for the RSA system. Classical and advanced algorithms of Euclid. Examples
Control work from chapters 2 - 7

Chapter 8. Increasing cryptoresistance in asymmetric encryption systems.
Topic 8.1 Estimates of cryptoresistance of the RSA algorithm. Comparison with DES and 3-DES schemes. Examples
Topic 8.2 The El-Gamal Cipher System . Key calculation schemes and algorithms for the El-Gamal system . Examples of encryption and decryption

Chapter 9. Authentication of subjects and establishment of "trust" relationship in distributed systems and networks.
Topic 9.1 Establishing "trust" of subjects based on symmetric encryption systems. Communication establishment protocols.
Topic 9.2. Establishing "trust" of subjects based on asymmetric encryption systems. The concept of a public key certificate.
Topic 9.3 Establishing message integrity based on symmetric and asymmetric encryption systems. Concept of digital signature.
Topic 9.4 Organization of "trust" communication in protocols of "open orders". The concept of electronic checks and receipts.

Chapter 10. Electronic payment systems. Means of increasing the "trust" of virtual relations.
Topic 10.1 Plastic cards as a basis for the organization of electronic payments. Issuing banks and acquiring banks .
Topic 10.2 Structure of the electronic payments system. POS terminals. Functions and organization of the processing center.
Topic 10.3 Multi- level organization of formation and use of encryption keys.
Topic 10.4 Electronic trade based on E-business technology. SSL and SET protocols. Hierarchy of signatures in trust relations.

4. Educational materials and resources

Basic literature

1. *Video recordings from the course of lectures for the 2021-2022 academic year. https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
2. *Volokita A.M., Ivanishchev B.V. Security of programs and data: Theory and practice. Recommended by the Methodical Council of KPI named after Igor Sikorskyi as a study guide for bachelor's degree holders in the specialty 121 Software engineering. The fretboard was provided by the Methodical Council of KPI named after Igor Sikorskyi (protocol No. 1 dated 09/02/2022) at*

the request of the Academic Council of the Faculty of Informatics and Computing (protocol No. 11 dated 07/11/2022). Updated. https://comsys.kpi.ua/metodichni-vkazannya-po-disciplinam

3. Dem'yanenko, V. A. Security of programs and data [Electronic resource]: ed . help _ to labs _ practicum / V. A. Demyanenko, Yu. A. Kuznetsova. - Kharkiv: National. aerospace _ University named after M. E. Zhukovsky "Kharkiv. aircraft _ Institute of Technology", 2021. - 95 p. http://dspace.library.khai.edu/xmlui/handle/123456789/798

4. Security of programs and data [Text] : Study guide / Seniv M.M., Yakovyna V.S. Lviv Polytechnic, 2018 - 256 p.

Additional literature

5. Verbitsky O.V. Introduction to cryptology . - Lviv, NTL, 1998. - 248 p.

6. National standard of TZI of Ukraine ND TZI 2.5-004-99 Criteria for evaluating the security of information in computer systems against unauthorized access. Valid since July 1, 1999.

7. The national standard of TZI of Ukraine ND TZI 2.5-005-99 Classification of automated systems and standard functional profiles of protection of processing information from unauthorized access. Valid since July 1, 1999.

8. DSTU ISO/IEC 27001:2015 Information technologies. Protection methods. Information security management systems. Requirements;

9. DSTU ISO/IEC TS 27008:2019 Information technologies. Protection methods. Guidelines for assessing information security protection;

10. DSTU ISO/IEC 27018:2019 Information technologies. Protection methods. Code of Best Practices for Protecting Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors.

11. Weissman C. Security Controls in the ADEPT-50 Time Sharing System. // Proceedings AFIPS, FJCC. - 2010. - v. 35. – pp. 119-133.

12. Hartson R., Hsiao D. Full protection specification in the semantic model for database protection languages. // Proceedings Annual Conference ACM. - Houston, New York. - 2014. - pp. 90-95.

13. Harrison MA. Russo WL Protection in Operating Systems. // Communications of the ACM. - 2014. - v. 19, No. 8. - pp. 461-471.

14. Spier MJ A Model Implementation for protective domains. // International Journal on Computer Information Science. – 2021. – v. 2, No. 3. - pp. 201-229.

15. Bell DE, LaPadula LJ Secure computer systems: mathematical foundations and models. // M74-244, The MITER Corp., Bedford, Mass. - May 1999.

16. Bell DE Secure computer systems: a refinement of the mathematical model. // Springfield, The MITER Corp. – 2018. – Report No. 2574, pp. 75

17. Graham RM, Denning PJ Protection - Principles and Practice. // Proceedings AFIPS. – 2018. – v.40, pp. 417-429.

18. Denning DE A Lattice Model of Secure Information Flow. // Communications of the ACM. -2011. – v. 19, No. 5. - pp. 236-243

19. *Landwehr C., Heitmeyer C., McLean J. A security model for military message systems. // ACM Trans. on Computer Systems. – 2017. – V. 2, No. 3. – pp. 198-222.*

Educational content

5. Methodology

Lecture classes

No	*The name of the topic of the lecture and a list of main questions (list of didactic tools, links to information sources)*
1	***Chapter 1. Introduction.*** ***Lecture 1. Problems of information protection in computer systems and networks (CSM).*** *Main issues: Concept of unauthorized access (USA), vulnerability of KSM, threat of intrusion, channel of information leakage. The main directions of threats to the NSD and the channels of information leakage from the KSM. Targets, subjects and schemes of active and passive*

	invasions. *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
2	***Chapter 2. A comprehensive approach to the creation of information protection systems in computer systems.*** ***Lecture 2. Regulatory and legal basis of information protection.*** *Main questions: The concept of information with limited access and protection systems. The main directions and means of information protection in KSM. Models of provably sufficient information protection systems. Adept conceptual model . Concept of object and category. Denning's model . Concept of security domain. Landwehr model . The concept of the perimeter of responsibility.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
3	***Lecture 3. The matrix model of the Bell and La Padula protection system .*** *Main issues: Concept of subject, vector of rights and access manager. Extension of access rights. Model of the KSM safety monitoring system. Concept of threat factor and statistical anomaly. Anomaly indication vector.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
4	***Section 3. Identification of subjects and access control based on the password system.*** ***Lecture 4. User identification based on the password system.*** *Key questions: Requirements for passwords. Password storage scheme in Unix OS. Analysis of the characteristics of the system of simple passwords. Anderson's formula. Examples.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
5	***Lecture 5. Modifications of the password system.*** *Main issues: Confirmation of access rights based on the unilateral and bilateral "handshake" procedure . Logs: registration and operational. Logging-based security monitoring on Unix and Windows.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
6	***Chapter 4. Discrete delimitation of subjects' access to information in the limited matrix model of the protection system.*** ***Lecture 6. Access lists and formation of user categories.*** *Main issues: Inheritance of rights. Locks, keys and access conditions in the OS. Mandate lists and implementation of the "minimum privileges" principle. Mandatory access in the Unix OS .* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
7	***Chapter 5. Computer approaches to cryptographic protection of information with limited access.*** ***Lecture 7. Encryption based on one and many alphabetic substitutions.*** *Main questions: Concept of cipher and secret key. Caesar's Cipher. Permutation-based encryption. Cipher "wandered" . Problems of decryption and cryptanalysis .* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
8	***Lecture 8. Bigram ciphers.*** *Key questions: Viginer cipher and Wheatstone squares . Encryption machines. Stream ciphers with unlimited key length. Encryption by "throwing".* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
9	***Chapter 6. Symmetric encryption in communication systems with open communications.*** ***Lecture 9. Organization of data transfers in secret systems according to Shannon .*** *Main questions: Entropy maximization means. Encryption based on alternating permutations*

	and substitutions. Lucifer system . *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
10	***Lecture 10. Federal DataEncryption Standard encryption standard. (DES).*** *Main questions: General scheme and masking function with keywords. Key control unit in DES. 3-DES algorithm and four modes of implementation of DES-based cryptographic protection.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
11	***Chapter 7. Asymmetric encryption systems based on public and secret keys.*** ***Lecture 11. New direction in cryptography according to Diffie and Hellman .*** *Main questions: Irreversible functions in encryption. Three schemes and tasks of cryptoprotection . RSA system. Modular arithmetic. Algorithm of fast discrete potentiation . The processor is an RSA accelerator.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
12	***Lecture 12. The problem of generating large prime numbers.*** *Key questions: Rabin's test and Fermat's little theorem. Simplicity checks. Examples.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
13	***Lecture 13. Key calculation schemes and algorithms for the RSA system.*** *Main questions: Classical and advanced algorithms of Euclid. Examples.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
14	***Chapter 8. Increasing cryptoresistance in asymmetric encryption systems.*** ***Lecture 14. Estimates of the cryptoresistance of the RSA algorithm.*** *Main issues: Comparison with DES and 3-DES schemes. Examples.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
15	***Lecture 15. El-Gamal encryption system .*** *Main questions: Schemes and algorithms of key calculations for the El-Gamal system . Examples of encryption and decryption.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
16	***Chapter 9. Authentication of subjects and establishment of "trust" relationship in distributed systems and networks.*** ***Lecture 16. Establishing "trust" of subjects based on symmetric encryption systems.*** *Basic questions: Concepts of master key and variable key. Communication establishment protocols. Establishing "trust" of subjects based on asymmetric encryption systems. The concept of a public key certificate. Communication establishment protocols.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
17	***Lecture 17. Establishing message integrity based on symmetric and asymmetric encryption systems.*** *Main issues: Concept of message signature and digital signature. Organization of "trust" communication in the protocols of "open orders". The concept of electronic checks and receipts.* *Video recording of the lecture: https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*
18	***Chapter 10. Electronic payment systems. Means of increasing "trust" of virtual relations.*** ***Lecture 18. Electronic trade.*** *Main issues: Security protocols. Hierarchy of signatures in trust relations.* *Video recording of the lecture:* HYPERLINK "https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr"*https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code : 12096*

Control works

The purpose of the tests is to consolidate and verify theoretical knowledge from the educational component, students' acquisition of practical skills in independent problem solving and the compilation and compilation of programs.

Control work KR1 is performed after studying sections 1 - 5.

Control work KR2 is performed after studying chapters 6 - 10.

Laboratory work

The purpose of conducting a cycle of laboratory work is for students to acquire the necessary practical skills for developing and researching mock-up samples of information protection subsystems, which are the embodiment of effective approaches and algorithms for creating a comprehensive system of information protection against unauthorized access, researching the characteristics of the necessary data structures, developing and debugging individual components of the console interface security administrator.

Laboratory work includes:

- *formulation of the input problem,*
- *theoretical information on methods and means of problem solving,*
- *analysis of mathematical and algorithmic support,*
- *justification of the choice of research software,*
- *development of a structural diagram of interaction of protection subsystems,*
- *results of step-by-step algorithm verification,*
- *results of model experiments,*
- *interpretation of modeling results and conclusions,*
- *program listing.*

No	*List of laboratory works.*
1	***Laboratory work 1.*** *Development and research of a software subsystem for discrete control of access to a separate information carrier with a complex directory structure.*
2	***Laboratory work 2.1.*** *Programming and research of a user identification subsystem based on simple passwords with requirements control and log support.* ***Laboratory work 2.2.*** *Programming and research of user authentication subsystem during operation using "question-answer" and secret functions.*
3	***Laboratory work 3.1.*** *Programming and researching the monitoring subsystem to detect anomalies and dangerous events regarding the information being protected.* ***Laboratory work 3.2.*** *Development of a software layout for research and step-by-step verification of the algorithm of fast discrete potentiation and other operations with arbitrary length of operands.*
4	***Laboratory work 4.*** *Development of a software layout for the study and step-by-step verification of algorithms for generating large prime numbers with the formation of an HPV database.*
5	***Laboratory work 5.*** *Development of a software layout for research and step-by-step verification of RSA - key management subsystem, encryption and decryption of messages.*
6	***Laboratory work 6.*** *Development of a software layout for research and step-by-step verification of DES - a subsystem of signature formation, encryption and decryption of messages.*
7	***Calculation and graphic work (Laboratory work 7).*** *Development of a software layout according to an individual task. The use of artificial intelligence tools for the task of security monitoring, improvement of software components from ЛР1-6. Carrying out experimental research, design in accordance with the simplified structure of scientific works.*

Self-study work

No. z/p	*Type of self-study work*	*Number of hours*
1	*Preparation and performance of laboratory work*	*40*
2	*Preparation for MKR. Development of lecture material and additional sources.*	*6*
3	*Implementation of RGR*	*20*
	Total hours of SRS	*66*

Policy and control

6. Policy of academic discipline (educational component)

The following factors are taken into account when enrolling and evaluating laboratory works:

- *Complete completion of the task for laboratory work according to the individual option;*
- *Timeliness of laboratory work according to the schedule;*
- *Independent performance of laboratory work and absence of signs of plagiarism;*
- *Answers to questions about the content of laboratory work during its defense.*

When evaluating control works, the following are taken into account:

- *Correctness and completeness of tasks;*
- *The number of completed tasks under limited time conditions;*
- *Independent performance of tasks and absence of signs of plagiarism;*
- *The number of control attempts.*

To prepare for the tests, students receive a list of theoretical questions and the content of typical problems that will be in the tests.

During the first and second attestation (calendar control), the number of laboratory works and control works enrolled at the time of the attestation is taken into account.

Policy on academic integrity: The Code of Honor of the National Technical University of Ukraine "Kyiv Polytechnic Institute" https://kpi.ua/files/honorcode.pdf establishes general moral principles, rules of ethical behavior of individuals and provides a policy of academic integrity.

7. Types of control and rating system for evaluating learning outcomes (RSO)

Current control: *exercises in lectures, testing, performance of RGR, MKR, performance and defense of laboratory work.*

Calendar control: *is carried out twice a semester as a monitoring of the current state of meeting the syllabus requirements .*

Semester control: *exam.*

Conditions for admission to semester control: *completed and protected laboratory work, MKR (or courses on the distance platform of Courser , etc.)*

Table of correspondence of rating points to grades on the university scale:

Table of correspondence of rating points to grades on the university scale :

Scores	***Rating***
100-95	Excellent
94-85	Very good
84-75	Good
74-65	Satisfactory
64-60	Sufficient
Less than 60	Fail
Admission conditions not met	Not allowed

The overall rating of the student after the end of the semester consists of points obtained for:

- performance and protection of laboratory work (LR1-LR6);

- performance of calculation and graphic work (LR7);

- execution of modular control work (MCW);

Laboratory work

Weight score. *Laboratory works LR1-6 have a weighting point of 10.*

It is planned to independently perform six laboratory works and computational and graphic work (by choice). The topics of the laboratory works are coordinated with the participation and content of the lecture topics. The full implementation of the laboratory works allows you to acquire practical skills of programming security systems. The teacher assigns individual practical tasks to each LR, which are performed personally by each student. Also, to get additional points, the student can complete an extended additional task.

Evaluation criteria: *The basic option is 6 points, with the protection of an additional practical task up to 10 points.*

Calculation and graphic work

Weight score. *Calculation and graphic work (LR 7) has a weighted score of 20.*

Independent performance of calculation and graphic work is planned. Completion of LR7 involves a creative interpretation of the previous works of LR1-6, and improvement of one of the software components used in LR1-6 (at the student's choice). The report from LR7 includes reports from LR1-6, a description of modifications, comparative experiments, and a list literature with a link to its own git repository .

Evaluation criteria: *The basic option is 12 points, with the defense of an additional practical task up to 20 points.*

Modular control works

Weight score. *Two control papers have a weighted score of 10 each.*

It is planned to perform two modular control tasks (KR1, KR2) during the calendar control (tasks are issued a week before the start of the calendar control). Upon agreement with the students, the deadlines for KR1 and KR2 can be extended. It is also possible to combine KR1 and KR2 into one extended MKR work.

Evaluation criteria: *In the tasks for KR1 and KR2, points are assigned for the corresponding questions. The student chooses the questions to be answered independently.*

Additional (bonus) points

Additional points are provided for activity in lectures (1 point), for completing extended additional tasks for LR1-7 (2 points), participation in hackathons , solving Olympiad problems in programming and other activities (points are agreed with students individually). The maximum bonus point is 10. Upon agreement with the student council , it is possible to draw "prize points" on the day of the faculty using pseudo-random number generators.

Penalty points

Penalty points are not provided. If the student does not perform additional tasks for LR1-7, then the minimum score for the corresponding LR will be credited (Table 1).

Calendar control

Calendar control is based on the current rating. A condition for a positive certification is the value of the student's current rating of at least 30% of the maximum possible at the time of the certification. The score required for obtaining a positive calendar control is brought to the attention of the students by the teacher no later than 2 weeks before the start of the calendar control.

Semester control form. Exam.

The student's semester rating consists of the points he receives for the types of work, respectively.

Evaluation of individual types of student's educational work (units)

Type of educational work	*Total jobs*
Performance and protection of laboratory works LR1-6	*36..60*
Implementation and protection of RGR (LR7)	*12..20*
Implementation of CR1	*6..10*
Implementation of CR2	*6..10*
Rating for the semester	*60-100*

A necessary condition for a student's admission to the automatic exam is his individual semester rating, not less than 60 points, and completed LR1-6. If the mentioned requirements are not met, the student will not be admitted to the exam. To increase the grade, it is allowed to rewrite KR1, KR2 and retake LR1-6, LR7.

8. Additional information on the discipline (educational component)

As part of the study of the discipline "Software Security", it is allowed to credit the points obtained as a result of distance courses on the "Coursera" platform , provided that the program of this course has been approved in advance with the teacher and provided that an official certificate is obtained (if possible, free of charge). Points for courses in which there are only test tasks are counted in the number of hours at least 60, and with a score of 55 (instead of ЛР1-ЛР7). Thus, the maximum score is limited to 75 (taking into account test papers). If the courses have a practical part, then the reports from the practical parts can be counted as laboratory work, in which case the maximum score is limited to 100.

The working program of the academic discipline (syllabus):

Designed by associate professor of the department of Computer Engineering, Ph.D., Artem Mykolayovych Volokita

Adopted by the Department of Computer Engineering (Protocol No. 10 dated 05/25/2022).

Approved by the Methodical Commission of the faculty (protocol No. 10 dated 06.9.2022).