MINISTRY OF EDUCATION OF THE REPUBLIC OF AZERBAIJAN
Order
No. F-463

Baku city, 28 July 2022

On the Approval of the Bachelor’s Degree Program in "Information Security" Specialization

In connection with the implementation of measures arising from the Decree No. 1315 of the President of the Republic of Azerbaijan dated 17 April 2021, titled "On certain measures to ensure the security of critical information infrastructure," and in order to improve personnel training in the field of cybersecurity in our country, it has become necessary to develop a competency-based and student-centered study program for the "Information Security" specialization that meets international and modern requirements, as well as the needs of the labor market.

Accordingly, by Order No. F-149 dated 30 March 2022 of the Ministry of Education of the Republic of Azerbaijan on the preparation of the study program for the "Information Security" specialization. this program was developed by local and international experts and representatives of the labor market.

Taking into account the above, as well as the development trends of information technologies in the 21st century, and based on Articles 8.10-1 and 13.5 of the Statute of the Ministry of Education of the Republic of Azerbaijan,

I hereby order:

1. To approve the Bachelor’s degree program in the "Information Security" specialization (attached).
2. To instruct the rectors of the relevant higher education institutions to ensure the preparation, approval, and implementation of curricula aligned with the approved program starting from the 2022/2023 academic year.
3. The Department of Science, Higher and Secondary Specialized Education (Yaqub Piriyev) shall address the matters arising from this order.
4. The Department of Information and Citizen Services (Rashad Khanlarov) shall ensure the distribution of this order in accordance with the delivery list.
5. The supervision of the execution of this order shall be entrusted to Deputy Minister Firudin Gurbanov.

Basis: Decree No. 1315 of the President of the Republic of Azerbaijan dated 17 April 2021 "On certain measures to ensure the security of critical information infrastructure"; Order No. F-149 of the Ministry of Education dated 30 March 2022, "On the preparation of the study program for the Information Security specialization".

MINISTRY OF EDUCATION OF THE REPUBLIC OF AZERBAIJAN

Bachelor’s Degree Program in the Specialty (Basic Higher Medical Education)

Code and Title of Specialty (Program): 050615 –“Information Security”

BAKU – 2022

BACHELOR’S DEGREE PROGRAM IN THE SPECIALTY

1. General Provisions

1.1. The Bachelor's Degree Program in the specialty "050615- Information Security " (hereinafter referred to as the Education Program in the specialty) has been developed in accordance with the Law of the Republic of Azerbaijan “On Education,” relevant decisions of the Cabinet of Ministers of the Republic of Azerbaijan, as well as the “Classification of specialties (programs) for the bachelor's level (basic higher medical education) of higher education.”

1.2. The objectives of the Education Program are as follows:

-To define the graduate's competencies in the specialty, the framework of the specialty, teaching and learning methods for courses, assessment methods, learning outcomes, and requirements for infrastructure and human resources for training personnel, as well as opportunities for students to undergo practical trainings, gain employment, and continue their education;

-To inform students and employers about the knowledge, skills, and learning outcomes acquired by graduates;

-To provide relevant information to experts involved in the evaluation of the compliance of staff training with this Education Program.

1.3. The Education Program is mandatory for all higher education institutions operating in the Republic of Azerbaijan, regardless of their subordination, form of ownership, or organizational-legal form, that offer bachelor's degree training in this specialty.

1.4. Under a five-day work week, the total weekly workload of a student, including classroom and extracurricular activities, is 45 hours (excluding special-purpose higher education institutions). The volume of classroom hours per week must not exceed 50% of the total weekly workload. Depending on the specifics of the specialty, the weekly workload may vary.

2. Graduate Competencies

2.1. Upon completion of the Education Program, the graduate must acquire the following general competencies:

-Oral and written communication skills in Azerbaijani within the field of specialization;

-Communication skills in at least one foreign language relevant to the specialty;

-Systematic and comprehensive knowledge of the historical, legal, political, cultural, and ideological foundations of Azerbaijani statehood, as well as its place and role in the modern world, and the ability to forecast the future development of the national state;

-Ability to identify threats and challenges facing the state;

- Cyber hygiene practices;

- Ability to approach problem-solving creatively and conduct independent research;

-Ability to identify and select additional information resources for problem-solving;

-Ability to analyze, synthesize, and apply relevant information for professional purposes;

- Ability to think critically and analytically, to learn independently, and to make decisions;
-Ability to work in a team and to reach collaborative solutions to problems;
-Ability to adapt to new circumstances, take initiative, and demonstrate a determination to succeed;
-Ability to plan and organize professional activities, enhance existing skills, manage time effectively, and complete tasks on schedule;
-Commitment to social and environmental responsibility, civic consciousness, ethical conduct, and quality-oriented work;
-Skills of self-assessment and self-criticism aimed at improving one’s knowledge and abilities.

2.2. By the end of the Education Program, the graduate must acquire the following professional competencies:

2.2.1. Competency Module A: Preventive Protection of Information Systems

Skills	Knowledge
Continuous Monitoring of Cyber Threats and Developments Related to Cybersecurity	Risk Catalogs Based on Information Sources Including Security Reports from Manufacturers, Forums, Technical Committees, and Others
Cyber Threat Analysis and Report Preparation	Strategic, Tactical, Operational, and Technical Concepts, Along with Cyber Threat Intelligence (CTI) Levels
Determination of requirements for assets regarded as objects of threats in information security- protection targets	Assets Recognized as Targets of Information Security Threats – Protection Subjects Information Security Requirements related to These Assets Information Security Metrics. The Concepts of Key Performance Indicators (KPIs) and Acceptable Limits

Detection of Security Weaknesses and Vulnerabilities	Auditing and Various Audit Types, Including Risk Assessment, Vulnerability Evaluation, Penetration Testing, and Compliance Audits;
	Penetration Testing Procedures and Tools for Identifying Security Weaknesses /Vulnerabilities and Ensuring Compliance;Indicators of Compromise (IOCs) and Indicators of Attack (IOAs);
	Proactive Threat Hunting;General Legal Provisions Regarding Cybercrime.

Elimination of Weaknesses and Vulnerabilities	Standards Based on Information Security Policy System-Specific Technical and Organizational Controls for Data Protection, Along with Security Solutions and Advanced Practices Methods and Tools for Strengthening System Protection (Penetration Testing, Information Security Audit) Methods and Tools for Conducting Security Testing of Software Terminals
Implementation of Tactical Methods	Tactical Methods and Devices for Combating Cyberattack and Cybercrime (such as Detection and Preventive Methods and Tools)
Assessment of Information Security	Information Security Measurement and Metrics; Assessment of Protection Efficiency
Providing Technical Consultations to Stakeholders	System-Oriented Consulting Principles. Communication Models and Standards
Providing Training Sessions to Stakeholders	Methodological and Didactic Principles. Planning and Implementation of Trainings

2.2.2. Competency Module B: Detection of Information Security Incidents

Skills	Knowledge
Systems Monitoring	Procedures and Tools for Monitoring Networks, Applications, Server Services, Storage Solutions, Devices, and Peripherals Technical Solutions and Devices for Attack Detection, Including Network Firewalls (Security Walls), Next-Generation Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Web Application Firewalls (WAFs);Security Information and Event Management (SIEM) Systems
Data Analysis and Interpretation	Analysis of Logs Using Various Methods Detection of False Positives Use of Scripting Languages (Bash, Python, Awk, Perl, etc.) for Data Analysis Data Analysis Methods Presentation Methods for Summarized Information

Security Incident Prioritization	Internal Policies and Processes Incident Classification and Prioritization Directing Incidents to Investigation
Security Incident Documentation	Task Tracking Systems for Managing Incidents Throughout Their Lifecycle Information Components Related to Incidents or Requests
Monitoring of Security Incident Management	Management of Incidents Based on Operational Level Agreements (OLA) and Service Level Agreements (SLA) Escalation Procedures Aligned with OLA and SLA Requirements

2.2.3. Competency Module C: Management of Information Security Incidents

Skills	Knowledge
Implementation of Immediate (Emergency) Actions	Incident Response Plan Requirements Emergency Technical Actions Including Isolation, Deactivation, or Termination of Systems or Services
The Identification, Collection, Documentation, Storage, Utilization, Protection, and Presentation of Evidence	Digital Forensics Policies and Principles Compliance with Legal Acts and Regulatory Documents Methods for Identification, Collection, Documentation, Preservation, Use, Protection, and Presentation of Evidence
Cause and Effect Analysis	Attack and Incident Investigation Static and Dynamic Analysis of Malware Forensic Examination of Systems, Networks, and Memory Methods and Techniques Used for Structured and Systematic Root Cause Analysis
Organization of Security Measures	Technical and Administrative Controls Effective Communication Skills and Methods with Stakeholders
Assistance in System Restoration	Business Continuity Management Emergency Recovery Measures

2.2.4. Competency Module D: Planning and Implementation of Information Security Solutions

Skills	Knowledge
Determination of System Boundaries and Requirement Identification	Modeling of Systems, Subsystems, and Their Boundaries

	Description of Interfaces; Definition of "S.MA.R.T." (Specific, Measurable, Achievable, Relevant, and Time-Bound) Objectives
Feasibility and Effectiveness Assessment	Feasibility Evaluation Methods (such as proof of concept, feasibility justification, modeling, and pilot projects)
Assessment of Workload and Expenses	Cost Evaluation Techniques Cost Planning and Calculation Ensuring Financial Oversight and Reporting
Implementation of Evaluations	Preparation of Evaluation and Assessment Criteria Requirements and Performance Indicator Characteristics Comparative Analysis of Solution Alternatives Facilitation of Effective Negotiations and Procurement Support
Implementation of Subprojects	Project and Subproject Planning Risk Management and Communication Quality Control Project Management and Reporting
Team Management	Specific Contextual and Situational Leadership Behavior Communication Models and Rules Team Building and Motivation Conflict Management within the Team

3. Structure of the Education Program

3.1. The Education Program consists of 240 ECTS credits (4 years).

Number of Courses	**Course Title**	**ECTS credits**
	General Courses	30
1	**History of Azerbaijan** This subject systematically studies the emergence, formation, and development of modern statehood traditions of Azerbaijan in a chronological sequence. It analyzes and examines the role of political, ideological, economic, and cultural factors in the formation of modern Azerbaijani statehood. The course also provides a	5

	systematic analysis of the position and role of the Republic of Azerbaijan in the modern world.	
2	**Business and Academic Communication in the Azerbaijani Language** Within the scope of this course, special attention is given to developing students' skills in delivering presentations, oratory, as well as academic and business writing in the Azerbaijani language.	4
3	**Business and Academic Communication in a Foreign Language** Within the scope of this course, special emphasis is placed on developing students’ skills in delivering presentations, oratory, academic and business writing, as well as oral and written communication in one of the foreign languages relevant to their field of study.	15
4	**Elective Courses** (Elective courses are determined by the higher education institution. Depending on the specialization of the program, additional elective courses may be included. The student must select two courses, each carrying 3 credits.)	6
4.1	Philosophy	3
	Sociology	
	Fundamentals of Law	
	Engineering Ethics	
	Critical Thinking	
4.2	Fundamentals of Entrepreneurship and Introduction to Business	
	Education and Career Planning	
	TOTAL	30
Specialized Courses		
5	**Fundamentals of Information Security** This course primarily introduces students to the field of information security. The course covers the subject, scope, fundamental principles, concepts, and objectives of information security. It teaches the knowledge and skills that an information security specialist must possess, as well as the connections with other subjects and specialties. The lectures aim to clearly describe the areas covered by information security for the students, while practical sessions demonstrate the application of the acquired knowledge in professional activities, thereby shaping the mindset specific to an information security specialist.	6
6	**Fundamentals of Programming**	6

	Within the scope of this course, students are taught to independently develop programs in any programming language, implement data structures and well-known algorithms associated with them, and analyze the algorithms' runtime and memory usage. Additionally, version control of code is taught. The course also covers the use of a modern programming environment (such as IntelliJ, Visual Studio, etc.), through which students develop skills to identify errors in programs and test the code. Writing appropriate test scenarios for program testing is also included among the course topics. Ultimately, students acquire practical knowledge such as conducting analyses on various structured data and automating specific tasks based on the acquired skills.	
7	**Mathematical Analysis** The Mathematical Analysis course is primarily based on differential and integral calculus of single-variable and multivariable functions, as well as the theory of series. While mastering this course, students must possess essential knowledge about numerical sequences, comprehend the concepts of limits, continuity, and uniform continuity of single-variable and multivariable functions, differential and integral calculus, numerical and functional series, and focus on learning their applications in applied mathematics, computer science, and cryptology.	6
8	**Fundamentals of Cybersecurity** Within the scope of this course, the conceptual model, role, and importance of cybersecurity are taught, along with its distinction from information security and their interrelations. Various cyberattack vectors and common vulnerabilities, threats, and risks in the field of cybersecurity, the characteristics of each stage of the cyberattack chain and the necessary measures to counteract them, the role and features of technical and organizational measures in ensuring cybersecurity are also studied.	6
9	**Fundamentals of Networks** In this course, students are taught the design and practical application of computer networks. The course provides information about advanced network equipment. Basic concepts of the OSI model and IP addressing, including IPv4 and IPv6, are covered. General information about different types of network models such	6

	as LAN, WLAN, MAN, and others is provided. Additionally, fundamental knowledge of wireless (radio wave-based) networks, including satellite-based networks, is included.	
10	**Linear Algebra** Within the scope of this course, matrices and the general theory of systems of linear algebraic equations, as well as linear transformations, quadratic forms, and other important topics are taught. Students study operations on matrices, calculation and properties of determinants, various solution methods for systems of algebraic equations, and the reduction of quadratic forms to their canonical form along with their applications. By mastering these topics and comprehending their applications, students are considered to have achieved the objectives of the course.	6
11	**Operating Systems** This course examines important issues related to the design and implementation of operating systems. During the course, a brief overview of the evolution of modern operating systems is provided, along with an explanation of the operating principles of their main components. The course reviews principles developed for the allocation of operating system resources (such as disk, network, and processors), as well as for providing and protecting common services required by programs. The course covers process and memory management, the working principles of file systems, and the functioning of distributed systems.	5
12	**Network Security** Within the scope of this course, in order to comprehend network security issues, students are taught in-depth knowledge of computer networks. They are expected to become familiar with concepts such as RADIUS, TACACS+, Kerberos, SSO, LDAP, and others, as well as gain knowledge about different types of network devices (e.g., IDS, IPS). The course includes topics such as network auditing and logging, sniffing mechanisms in networks, and necessary configurations to ensure network security. Students also comprehend and apply existing network security protocols. Furthermore, they are introduced to modern security technologies and frameworks such as SIEM, SOAR, and UEBA.	5
13	**Discrete Mathematics**	5

	The Discrete Mathematics course studies the elements of mathematical and predicate logic, graph theory, Boolean algebra, combinatorics, and the study of relationships between discrete structures. Students are expected to focus on comprehending precise logical concepts, applying various proof techniques, and using discrete mathematics methods for the development of optimal programs. Special attention must be given to the application of graph theory in fields such as cyber forensics and network security, which is also emphasized through practical exercises.	
14	**Web Security** Within the scope of this course, students learn the operating principles of web applications, the logic of their visualization by browser programs, and the principles of their interaction with servers.Subsequently, they acquire practical knowledge about how and where security vulnerabilities in web applications and web services originate, as well as how such vulnerabilities/weaknesses can be mitigated.In addition, the course covers advanced practices for ensuring security in web applications, common vulnerabilities and weaknesses, and the methods and tools used for exploiting these vulnerabilities.	5
15	**Probability Theory** The Probability Theory course studies the probability patterns of mass random events and develops methods for collecting and processing statistical data to obtain scientific and practical results. Students mustparticularly focus on the application of probability definitions, the calculation of numerical characteristics of random variables, and the application of various theorems to problem-solving.	5
16	**Legal Aspects Of İnformation Security And Cybersecurity** Within the scope of this course, the legal norms regulating public relations arising in the field of information security and cybersecurity are taught. During the course, special attention must be given to the fundamentals of information law, the normative-legal framework related to information security and cybersecurity, mechanisms for the protection of fundamental human rights and freedoms in the field of information, as well as the legal aspects of the protection of personal data, state secrets, and confidential	5

	information, the the legal mechanisms for combating cybercrime and the legal aspects of information warfare/cyber warfare.	
17	**Information Security Management Systems** Within the scope of this course, students will acquire the necessary knowledge for comprehending the relevance, fundamentals, planning, and organization of Information Security Management Systems (ISMS). They develop skills to integrate ISMS with other management systems within an organization. In addition, students will study the principles, role, and methods of implementing international standards related to ISMS—primarily ISO/IEC 27001, as well as other standards such as ITIL and COBIT—depending on the specific characteristics of the organization's field of activity.	5
18	**Database Security** Within the scope of this course, the foundational essential knowledge of database management systems (DBMS) is provided, followed by instruction on the basic principles of ensuring information security during the design, implementation, and operation of DB. The course also covers the identification and prevention of potential security vulnerabilities and weaknesses in DB, methods, and tools for counteracting relevant cyberattacks, as well as methods and tools for conducting security audits in DB. In addition, fundamental information and concepts related to cloud-based and NoSQL types of databases are taught.	5
19	**Cloud Security** This course covers the concept of cloud technologies, their benefits, and the differences from traditional services. Students acquire the necessary knowledge and skills to examine security models and risks associated with cloud services, methods for their prevention, and approaches to security from various perspectives, to develop effective security strategies for cloud environments.	5
20	**Fundamentals of Cryptography** Within the scope of this course, students study a brief history of the emergence and development of traditional cryptography, its relevance, application areas, and existing challenges, modern cryptosystems and encryption methods, along with how cryptography ensures the principles of information security.	5

	The course reviews block, stream, and public-key encryption algorithms, as well as advanced cryptographic algorithms, providing information related to their practical applications.	
21	**Fundamentals of Penetration Testing** This course teaches students the methods and tools of penetration testing, including its planning, preparation, and execution stages. Students learn to perform simulated cyberattacks in a laboratory environment to identify vulnerabilities and weaknesses in systems and to approach systems from different perspectives. The course covers techniques for active and/or passive information gathering from information systems. Additionally, students learn how to exploit discovered vulnerabilities to escalate privileges, assess the potential damage that can be caused to the facility, evaluate risk factors, and implement preventive measures. Additionally, students are trained to prepare detailed reports on the results of penetration testing.	8
22	**Fundamentals of Electronics and IoT Security** This course provides knowledge about electronics, microcontrollers, and devices created using them, with a special focus on various wired and wireless networks used by the Internet of Things (IoT) and related systems, as well as the security of these networks. It covers the physical protocols and communication methods used by IoT devices, along with communication protocols, explaining their strengths and weaknesses. Additionally, the course clarifies information security issues related to IoT devices, including potential cyberattacks targeting them and cyber defense methods.	5
23	**Secure Programming** This course explains security vulnerabilities that arise from software source code and their characteristics, providing the essential knowledge needed to eliminate these vulnerabilities. Within the course framework, students will be taught methods and tools for ensuring that code complies with security requirements throughout the entire software lifecycle, from development to operation. Students will also learn the fundamentals of setting up an appropriate laboratory environment and gain practical experience in performing static application security testing (SAST) and dynamic application security testing (DAST) within this environment.	5
24	**Fundamentals of Digital Forensics**	8

	Within the scope of this course, essential topics are taught related to the investigation of security incidents and the conduct of digital forensics, the identification, collection, documentation, preservation, use, protection, and presentation of digital evidence. Special emphasis must be placed on acquiring knowledge about the concept, types, and principles of forensic computer-technical examination/digital forensics, forensic diagnostics and investigation processes, digital forensic tools and techniques, necessary resources for obtaining and analyzing digital evidence, as well as common challenges in the field of digital forensics. In addition, students will gain practical experience with both open-source solutions and advanced tools developed by leading vendors.	
25	**Security of Industrial Control Systems** Within the scope of this course, students will study critical infrastructures and their significance, gaining insight into cybersecurity issues related to such infrastructures. They will learn about non-IT protocols (such as Modbus, DNP3, ICCP, etc.), technologies (including SCADA, PLC, DCS, etc.), and methods and tools used to ensure the security of Operational Technology (OT) environments, particularly in industrial control systems.	5
26	**Civil Defense** Within the scope of this course, students will gain information on the fundamentals of civil defense, its forces and means, the characteristics of emergencies, and the protection of the population in emergencies, public awareness on civil defense, methods for eliminating the consequences of emergencies, and the use of individual and collective protective equipment. The course also includes information on ensuring the resilience of industrial facilities during emergencies and the basic principles and assessment methods related to their operational continuity.	3
	TOTAL	120
	Courses Determined by the Higher Education Institution	60
Practical training		
Practical training		30
TOTAL		30
Total Number of Credits		240

Note: The sequence of specialization subjects is recommended in Appendix 1. Recommendations regarding elective courses to be determined by the higher education institution are reflected in Appendix 2.

4. Teaching and Learning

4.1. The teaching and learning environment must be organized in such a way that students can achieve the intended learning outcomes specified in the educational program.
4.2. Teaching and learning methods must be described in relevant documents (for example, in the instructor's syllabus, etc.) and made publicly accessible (for example, on the university's website, in the program brochures, etc.).
4.3. Teaching and learning methods must be continuously reviewed and improved by taking innovative educational practices into account. The regular enhancement of teaching and learning methods must be an integral part of the university's quality assurance system.
4.4. Different teaching methods must be used in the learning process. These methods must encourage a student-centered approach and promote active student participation in the learning process. Examples of possible teaching and learning methods include:
-lectures, seminars, practical assignments;
-presentations and discussions, debates;
-individual work/research (e.g., working with practical examples, direct engagement in practical projects);
-projects;
-problem-based learning;
-fieldwork;
-role-playing games;
-reports;
-group assessments;
-expert method;
-video and audio conferencing technologies;
-video and audio lectures;
-distance learning;
-simulations;
-etc.
Note: The listed methods may be selected and/or modified depending on the specifics of the specialization.
4.5. A balance between theoretical education and practical training must be maintained. The main focus must be on strengthening practical skills in accordance with the changing needs of the labor market.

4.6. The educational program must support students' independence and foster the concept of lifelong learning. By the end of the educational process, students must be able to work independently in any direction and have the ability to continue their education throughout their lives.

5. Assessment

5.1. Assessment must be organized so that the achievement of students' expected learning outcomes, skills can be effectively measured. This must enable monitoring of progress, evaluating the extent to which educational program outcomes are achieved, facilitate feedback exchange with students, and help form the initial conditions for improving educational programs.

5.2. Assessment methods must be described in relevant documents (e.g., course syllabus, program descriptions, etc.) and be accessible to everyone (e.g., on the university website, program brochures, etc.). The subject instructor is required to define the assessment methods for the course, utilizing the table provided in Appendix 3.

5.3. Assessment methods must be continuously reviewed and improved, taking into account innovative teaching practices. Regular updating of assessment methods must be part of the higher education institution's quality assurance system.

5.4. Different assessment methods must be used during the teaching process. These methods must promote a student-centered approach and encourage students' active role in the learning process. Examples of possible assessment methods include:

-written assignments;
- knowledge and skills tests, computer-based tests;
-oral presentations;
-surveys;
-open discussions;
-practical training reports, fieldwork reports;
-evaluation of skills based on practical and laboratory observations;
-project reports;
-portfolio assessment;
-frontal questioning;
-group and self-assessment;
-etc.

Note*:* The listed methods can be selected and/or modified depending on the specifics of the course.

5.5. Methods used for assessing learning achievements must be based on clearly defined criteria and allow for accurate and reliable determination of the student's knowledge, skills, and competency levels throughout the educational process. During assessment, instructors must adhere to the principles of transparency, impartiality, mutual respect, and humanism.

5.6. Students must be given the opportunity to discuss all aspects of their education, including the assessment process, with instructors and evaluators. The higher education institution must

establish assessment and appeal procedures related to grades in accordance with relevant regulations.
5.7. Academic ethics holds an important place in the educational process. Students are taught to observe academic honesty and to comprehend the issue of plagiarism. They must be informed about intellectual property rights concerning intellectual work.

6. Learning Outcomes of the Program and Each Course

6.1. The determination of the learning outcomes of the educational program, as well as the learning outcomes of each course and the preparation of each course syllabus, fall under the authority of the higher education institution/academic staff.
6.2**.** Learning outcomes are reflected in Appendix 4. The matrix of learning outcomes (Appendix 5) must reflect the relationship between courses and learning outcomes.
6.3. To ensure that the educational program provides theoretical and practical content that meets the changing needs of society and the labor market, current academic program and course syllabi must be regularly updated.

7. Infrastructure and Human Resources

7.1. The implementation of the teaching, learning, and assessment processes of the educational program requires that the higher education institution possess the following infrastructure:
-Classrooms, laboratories, and computer labs equipped with the appropriate software and internet access for conducting lectures, practical, and laboratory classes as stipulated in the curriculum;
-A modern material and technical base equipped with physical equipment and/or simulators for students and faculty to carry out relevant projects and scientific research work, including individual devices to enable independent research**.**
7.2. As a rule, the academic staff of higher education institutions hold academic degrees. Furthermore, specialists with appropriate experience from governmental, private institutions, and other organizations may be engaged in the teaching process.

8. Practical Training

8.1. Practical training is important for the practical application of a student’s theoretical knowledge as well as for strengthening professional skills.
8.2. The practical training can be organized in private companies, government institutions, research laboratories (as well as universities, the Azerbaijan National Academy of Sciences, local or international private organizations and companies, etc.).
8.3. Prior to the practical training, a contract must be signed between the higher education institution and the company/enterprise/laboratory where the practical training will take place. At the same time, based on the student’s individual request, permission may be granted for the student to undertake an practical training at another company, enterprise, or laboratory relevant to their

specialty, including abroad. The contract shall specify the terms, the rights and responsibilities of the students, and other necessary details.

8.4. The practical training is evaluated by the higher education institution based on the report prepared by the student at the organization where the practical training was completed.

9. Course Projects

9.1. Each year, students complete a course project for a subject determined by the higher education institution.

9.2. These course projects may be prepared individually or in groups.

9.3. Course projects must pertain to topics of practical significance in the field of Information Security.

10. Employment and Lifelong Learning

10.1. Graduates specializing in Information Security can work in various professions related to ensuring information security in both the public and private sectors. Some of these professions and roles are listed as examples (recommendations) in Appendix 6.

10.2. The higher education institution must conduct regular surveys regarding the employment of graduates of the Educational Program, publish information about vacant positions on its website, and organize job fairs.

10.3. To improve students' employment rates, the higher education institution may invite labor market representatives to conduct master classes and/or seminars.

10.4. Graduates of this Educational Program may continue their studies at the master's level in the following specialties:

-060509 - Computer Science
-060631 - Computer Engineering
-060632 - Information Technology and Systems Engineering
-and other relevant specialties

10.5. The knowledge, skills, and approaches acquired during the education period constitute the basic prerequisites for graduates to independently pursue lifelong learning.

Appendix 1

The teaching sequence of specialized courses

Course titles	Number of credits
1st academic year, 1st semester	
Mathematical Analysis	6
Fundamentals of Information Security	6
Fundamentals of Programming	6
1st academic year, 2nd semester	
Linear Algebra	6
Fundamentals of Networks	6
Fundamentals of Cybersecurity	6
2nd academic year, 1st semester	
Discrete Mathematics	5
Operating Systems	5
Network Security	5
2nd academic year, 2nd semester	
Web Security	5
Legal aspects of information security and cybersecurity	5
Probability Theory	5
3rd academic year, 1st semester	
Information Security Management Systems	5
Database Security	5
Cloud Security	5
Civil Defense	3
3rd academic year, 2nd semester	
Fundamentals of Cryptography	5
Fundamentals of Penetration Testing	8
Security of Electronics and IoT Devices	5
4th academic year, 1st semester	
Secure Programming	5
Fundamentals of Digital Forensics	8
Security of Industrial Control Systems	5

Appendix 2

Recommended Elective Courses

1. Security Equipment
2. Fundamentals of Data Center Operations
3. Security of Corporate Network (Information) Systems
4. Malware Analysis
5. Machine Learning
6. Fundamentals of Digital Image and Video Processing
7. Applied Statistics and Data Analytics
8. Parallel and Distributed Computing
9. Graph Theory
10. Security of Mobile and Wireless Devices
11. Security of VoIP Systems
12. Blockchain Technologies
13. Numerical Methods
14. Digital Transformation
15. Systems Programming
16. Data Mining
17. System Design
18. Software Project Management
19. Software Engineering
20. C Programming Language
21. Programming for Mobile Devices
22. Web Programming
23. Research on Mobile Devices
24. Design and Analysis of Algorithms
25. Cloud Technologies
26. Social Network Analysis
27. Social Engineering

Appendix 3

Teaching and learning methods and assessment methods used to achieve the course learning outcomes

Course Title	Learning Outcomes	Teaching and learning methods used for each learning outcome	Assessment methods used for each learning outcome

Appendix 4

Learning Outcomes for the Educational Program and Courses

The higher education institution must determine the expected learning outcomes for the Educational Program and for each course.

Program Learning Outcomes (PLO)
PLO 1. The graduate musthave knowledge of the emergence, formation, and development of modern Azerbaijani statehood traditions. He/She mustbe able to analyze and study the role of political, ideological, economic, technological, scientific, and cultural factors in the formation of modern Azerbaijani statehood. He/She mustbe able to systematically analyze the place and role of the Republic of Azerbaijan in the modern world. The graduate must be informed about the development history of cybernetics, applied mathematics, information and communication technologies in Azerbaijan, as well as the traditions and potential in science, education, and industry in these fields, and the professional activities of world-class Azerbaijani specialists. The graduate mustacquire skills in delivering presentations, public speaking, and academic and business writing in the Azerbaijani language. He/She mustalso possess skills in making presentations, public speaking, academic and business writing, and oral and written communication in at least one foreign language. The graduate mustcomprehend the goals and objectives of the Information Security specialization, its interrelation with other fields, the importance of meeting the demands in the public and private sectors, and its future prospects. He/She mustrecognize the importance of engineering ethics and the necessity of applying the knowledge acquired in this field strictly within the framework of legislation and ethical norms, in accordance with professional responsibilities.
PLO 2. The graduate musthave knowledge of numerical and recursive sequences, the limit and continuity of functions, derivatives of functions, extrema of single-variable functions, indefinite integrals, definite integrals, numerical and power series, limits of multivariable functions, partial derivatives, and differentials. The graduate mustcomprehend the concept of matrices, operations

on matrices, transposition of matrices, computation of determinants of order two and three, determinant of the product of two matrices, Tarsian matrix and its existence, n-dimensional vector space, linear dependence of vectors, matrix rank, systems of linear algebraic equations, polynomials and operations on them, roots of polynomials, Horner's scheme, and quadratic forms.The graduate must have knowledge of elementary functions of Boolean algebra, their properties, operations on them, binary functions, the duality principle, the concept of graphs, geometric representation of graphs, connected, sub-, complete, isomorphic and homomorphic graphs, directed, undirected, and mixed graphs, regular and uniform graphs, encoding, decoding, one-to-one decoding, alphabet and regular coding, code selection, error sources, and criteria for one-to-one decoding. The graduate mustbe familiar with the subject of probability theory, classical probability, elements of combinatorics, Kolmogorov axioms, properties of probability, geometric probability, entropy and amount of information, Bernoulli scheme, probability distributions, discrete distributions, numerical characteristics of random variables, mathematical expectation, variance, Markov and Chebyshev inequalities, coefficient of asymmetry, covariance and correlation coefficient, and the law of large numbers.
PLO 3. The graduate mustpossess the following knowledge and skills: ability to apply knowledge and competencies in the preventive protection of information systems, minimization of information security risks, detection of threats and vulnerabilities, and prevention of their potential consequences. Ability to define the scope of information security, keep inventory of information assets and functional assets used in information processes, and document their respective functionalities. Competence in developing and managing information security policies, risk and incident management frameworks, and sub-policies for managing ICT services and ICT projects. Ability to define information security requirements for protected assets, including those with protective tools, and to determine information security metrics and indicators. Ability to identify security incidents caused by threats and their potential impacts on business continuity, as well as to assess their severity levels. Proficiency in cyber intelligence, including the ability to identify threats, threat-related attempts and preparations, and to propose preventive countermeasures. Ability to provide recommendations regarding the provision of cryptographic services, to audit and evaluate the information security management system, and to develop local (corporate) normative legal acts, guidelines, and practical implementation playbooks in accordance with information security policies.
PLO 4. The graduate mustpossess the knowledge and skills necessary to organize and implement incident management processes, including continuous monitoring, regular audits, expert assessments, and other control mechanisms for detecting information security incidents.Ensure the execution of operational processes related to the Security Operations Centre (SOC) within the information security organizational unit; identify and assess information security events within protected assets, detect security incidents, and determine their severity levels, types of consequences, and their impact levels; apply methods for detecting, evaluating, and classifying information security incidents and their consequences for business continuity; demonstrate awareness of cyber-forensics and the collection of digital evidence, including comprehending and ensuring compliance with security and chain-of-custody requirements for preserving digital findings and evidence.
PLO 5. The graduate mustpossess the knowledge and skills to manage configurations and changes in protected assets to eliminate vulnerabilities as part of the response to information security incidents; select the appropriate response options for information security incidents, such as blocking, restoration, modification, updating, improvement, switching to backup

versions, and rollback to previous states; develop, implement, and apply relevant playbooks for incident response, and know the procedures for escalating to external support during crises; be knowledgeable in the administration of software and technical protection services (controls) that safeguard information.
PLO 6. The graduate mustacquire knowledge and skills to plan and implement information security solutions, including the design, development, preparation, and deployment of these solutions in accordance with predefined levels of excellence and trustworthiness of ICT tools; apply project management principles related to the design and deployment of information security solutions; determine and document the requirements (Request for Proposal, RFP) for protected ICT products within the scope of information security, including software tools, electronics, electrical engineering, telecommunications, and other technical support systems; conduct an analysis of the compliance of the ICT product with the technical requirements of its intended application domain, using appropriate standards and methods such as GAP analysis; be aware of various development approaches for ICT products, including the Waterfall (cascade) and Agile (iterative) methodologies, and possess the necessary knowledge to select the appropriate methodology (e.g., Scrum, Lean, Extreme Programming (XP); define and document the technical requirements (Statement of Requirements, SOR) and technical specifications (Terms of Reference, TOR) for ICT products; ensure and document the verification testing of ICT products, including mechanisms for validating the implementation of technical requirements and specifications.

Course Learning Outcomes – (CLOs)
Course Learning Outcomes for the subject “History of Azerbaijan” (CLOs)
CLO 1 Comprehends the emergence, formation, and development of modern Azerbaijani statehood traditions.
CLO 2 Demonstrates knowledge of Azerbaijani statehood during ancient and medieval periods, and in the 15th–18th centuries, including the establishment of a major Eastern empire by the Azerbaijani people.
CLO 3 Analyzes and researches the role of political, ideological, economic, and cultural factors in the formation of modern Azerbaijani statehood.
CLO 4 Acquires knowledge of the loss of Azerbaijani statehood in the early 19th century, its political, economic, and social consequences; the national struggle for statehood in Azerbaijan; the establishment of the Azerbaijan Democratic Republic (the First Republic); the Second Republic; Azerbaijani statehood during the Soviet Empire; the beginning of the independence movement in the late 1980s and the restoration of independent statehood.
CLO 5 Systematically analyzes the place and role of the Republic of Azerbaijan in the modern world.
CLO 6 Comprehends the creation of a secure international environment for the protection of modern statehood, the struggle for the restoration of territorial integrity, and Azerbaijan’s rise as a leading state in the Caucasus region.

Course Learning Outcomes for the subject “Business and Academic Communication in the Azerbaijani Language” (CLOs)
CLO 1 Has knowledge of the history of the Azerbaijani language, its development, and ways to enrich it.
CLO 2**:** Knows about the periods in history when the Azerbaijani language faced oppression and aggression from hostile forces, and how, thanks to the national unity and pride of the people, it was successfully preserved, including the contributions of prominent commanders and statesmen in this effort.
CLO 3**:** Analyzes scientific information related to their specialty in the Azerbaijani language and prepares oral and written presentations.
CLO 4: Demonstratse academic and professional public speaking skills in the Azerbaijani language.
CLO 5**:** Preserves the uniqueness of the Azerbaijani language, uses translation to become
CLO 6**:** Engages in the struggle to maintain the purity of the Azerbaijani language, protects it from foreign elements, and ensure its vitality.

Course Learning Outcomes for the subject “Psychology” (CLOs)
CLO 1 To acquire knowledge about the subject and methods of psychology, its place within the system of sciences, its main fields, and the primary directions of psychological thought development.
CLO 2 To comprehend the structure of the human psyche, the role of consciousness and unconsciousness in regulating behavior, and have an overview of motivation and psychological regulation of behavior and activity.
CLO 3 To possess knowledge of the fundamental categories and concepts of psychology, including cognitive, emotional-volitional, and motivational domains of the psyche; personality and the features of its development and formation; thinking, communication and activity; temperament, character, abilities; and issues related to education and self-development.
CLO 4 To be able to analyze professional and problematic educational situations, organize professional communication and interaction, individual and joint decision-making, and reflection.
CLO 5 To be capable of diagnosing individuals’ personal and psycho-psychological characteristics, as well as their cognitive and professional activity styles.
CLO 6 To apply acquired knowledge in solving various psychological practical problems and decision-making processes in education, pedagogy, industry and commerce, as well as in combating unlawful behavior and other relevant fields.

Course Learning Outcomes for the subject “Sociology” (CLOs)
CLO 1 To be able to use the fundamental principles and methods of social, humanitarian, and economic sciences in solving social and professional problems. To take into account global, national, and regional characteristics, as well as current conditions, in the development of the social sphere and governance.

CLO 2 To develop independent thinking and critical analysis skills in addressing social issues.
CLO 3 To acquire the competence to identify problems arising in any sphere of society and to seek more adequate solutions.
CLO 4 To gain proficiency in conducting sociological research and analyzing its results.
CLO 5 To have knowledge of the social life, well-being, and behavioral characteristics of various social groups. To be able to apply the specific features of the national-cultural context and the activities of different national, gender, age groups, and social institutions as subjects of social projects.
CLO 6 To creatively apply basic sociological knowledge in professional activities and in the analysis of various social phenomena.

Course Learning Outcomes for the subject “Fundamentals of Law” (CLOs)
CLO 1 To acquire general knowledge about the concept, essence, functions, features, and sources of law, as well as the constitutional foundations of the legal system.
CLO 2 To develop an comprehending of the fundamental regularities of law’s functioning, its interaction with the state and other social institutions, and the main development trends in the sovereign Republic of Azerbaijan.
CLO 3 To study the constitutional structure of the Republic of Azerbaijan, the constitutional legal status of individuals and citizens, their fundamental rights, freedoms, and duties.
CLO 4 To comprehend the social value of law as an effective legal regulator of social relations; develop a legal mindset oriented towards combating legal violations and protecting the rights and freedoms of citizens; and foster adherence to the rule of law as the foundation for professional duties.
CLO 5 To comprehend the concept and characteristics of legal norms and normative legal acts; learn the classification and types of legal norms using the legislation of the Republic of Azerbaijan as an example; and acquire knowledge about the system of normative legal acts according to the Constitution of the Republic of Azerbaijan.
CLO 6 To comprehend the concept and essential aspects of lawful behavior, legal violations, and legal responsibility; acquire necessary knowledge about the types of legal responsibility, the procedures for imposing legal responsibility, and the grounds for exemption from legal responsibility.

Course Learning Outcomes for the subject “Engineering Ethics” (CLOs)
CLO 1 Distinguishes between ethical and unethical situations and makes moral judgments in dilemma conditions.
CLO 2 Comprehends the importance of prioritizing public safety, health, and welfare above all else.
CLO 3 Recognizes the necessity of providing services only within one’s authorized scope of competence.
CLO 4 Comprehends the role of acting as a loyal representative of the employer or client.

CLO 5 Demonstrates behavior that enhances the honor, reputation, and usefulness of the profession by acting honorably, responsibly, ethically, and legally; and acknowledges the importance of using only legal and reliable sources during professional service.
CLO 6 Recognizes the importance of adhering to ethical and honor codes during social experiments and data collection.

Course Learning Outcomes for the subject “Critical Thinking” (CLOs)
CLO 1 Develops the ability to select the optimal choice among possible alternatives.
CLO 2 Learns to approach problem-solving in a systematic and continuous manner.
CLO 3 Cultivates tolerance for others’ opinions and enable others to express their views.
CLO 4 Acquires the habit of thoughtful, timely, and well-informed reasoning.
CLO 5 Builds trust in results based on fact-driven thinking and develops the ability to approach problems with the goal of forecasting outcomes.
CLO 6 Learns skills and methods for analyzing issues or problems and drawing logical conclusions.

Course Learning Outcomes for the subject “Fundamentals of Entrepreneurship and Introduction to Business” (CLOs)
CLO 1 To comprehend the main economic and legal institutions of entrepreneurship, the core aspects of business planning, the formulation of entrepreneurial intent, and the active application of socio-economic tools in entrepreneurial activity.
CLO 2 To be able to prepare a business plan, establish an enterprise, build business partnerships, and determine the optimal organizational structure and infrastructure in line with business characteristics. To know the key concepts and tools required for effective business management.
CLO 3 To demonstrate knowledge of the principles governing the main and auxiliary functions within an enterprise structure. To learn the types and methods of management and apply them effectively in organizational functions.
CLO 4 To comprehend the concept of production, production processes, production systems, and features of modern production management; to be able to plan necessary raw materials, materials, and semi-finished goods for the uninterrupted operation of business entities.
CLO 5 To identify the impact of environmental factors on enterprise performance and respond appropriately to those influences.
CLO 6 To analyze, evaluate, and manage business processes.

Course Learning Outcomes for the subject “Education and Career Planning” (CLOs)
CLO 1 Describes the career development process and helps students comprehend the stage they are currently in.
CLO 2 Explains the impact of demographic, economic, and organizational changes on the world of work and on individuals' career development decisions.

CLO 3 Uses various modern assessment tools and reflective activities to identify personal priorities, skills, interests, strengths, and values.
CLO 4 Gains information about organizations, professions, and industries.
CLO 5 Learns how to present oneself to the labor market in an honest and professional manner by developing skills in writing CVs, presentations, and cover letters.
CLO 6 Prepares effectively for interviews related to internships and prospective job opportunities.

Course Learning Outcomes for the subject “Fundamentals of Information Security” (CLOs)
CLO 1 To have knowledge of important concepts in information security, including terminology used in documents and business discussions. To comprehend the basic and specific requirements in information security and their formation characteristics.
CLO 2 To be familiar with the conceptual model of information security and have a basic comprehending for forming relevant requirements to ensure information security.
CLO 3 To have knowledge of the key legal regulations in the field of information security, their requirements, and application rules, as well as be able to monitor their development. To be aware of global, regional, and national standards, norms, and best practices in information security, track their evolution, and have opinions on their implementation..
CLO 4 To comprehend organizational forms and methods for ensuring information security. To know the main principles for providing information security and study the technical methods and tools used.
CLO 5 To possess general knowledge about risks in information security, their characteristics, and management. To comprehend the relevance, formation, and application of information security policies and know methods for their enforcement. To have general knowledge of the fundamentals, features, relevance, and procedural rules of information security auditing.
CLO 6 To have general knowledge of the legal, organizational, and technical foundations of information protection tools, their application areas, as well as the development and certification of such tools in accordance with regulations, the rules for recognizing foreign certificates issued for information protection tools.

Course Learning Outcomes for the subject “Fundamentals of Programming” (CLOs)
CLO 1 Is capable of freely writing programs in any programming language. Comprehends the concepts of conditionals, loops, functions, objects, and classes. Knows data types and how they are stored in memory. Comprehends the compilation process and the concepts of bytecode and machine code.
CLO 2 Is knowledgeable about data structures such as arrays, linked lists, stacks, queues, graphs, and trees, as well as classical algorithms operating on these data structures. Is able to implement these data structures and algorithms in any programming language.
CLO 3 Is able to analyze the runtime and memory usage of algorithms. Is capable of making correct decisions on algorithm selection considering system capabilities and limitations.

CLO 4 Is familiar with at least one professional development environment used for programming. Is able to compile programs, perform debugging, and manage code versions (e.g., using the Git version control system) within that environment.
CLO 5 Has knowledge of methods of testing software modules and can write test scenarios. Is aware of code readability and quality criteria.
CLO 6 Using the acquired knowledge, is able to develop programs for converting between different file formats, creating various parsers, analyzing logs, and extracting data through interfacing with different systems.

Course Learning Outcomes for the subject “Mathematical Analysis” (CLOs)
CLO 1 To comprehend the definition of the limit of a sequence, the concepts of convergent and divergent sequences, and the basic properties of limits.
CLO 2 To possess knowledge of the limit of a function, the definition of continuity at a point, key properties of continuous functions, and types of discontinuities.
CLO 3 To comprehend the definition of the derivative of a function, its fundamental properties, the definition of the differential at a point, and related theorems. To be familiar with the definitions of local maxima and minima, necessary conditions for extrema, and the first and second-order sufficient conditions.
CLO 4 To be able to define a partition of an interval and its properties; to comprehend the definition of the definite integral and the class of integrable functions.
CLO 5 To know the definition of a numerical series, necessary condition for convergence, and the properties of convergent series. To comprehend the radius and interval of convergence for power series, the Cauchy-Hadamard formula, and the concept of Taylor series.
CLO 6 To possess knowledge of partial derivatives and differentials of multivariable functions.

Course Learning Outcomes for the subject “Fundamentals of Cybersecurity” (CLOs)
CLO 1 To possess knowledge of the fundamental concepts and principles of cybersecurity.
CLO 2 To comprehend the importance of cybersecurity management. To be familiar with the organizational forms and methods for ensuring cybersecurity.
CLO 3 To be knowledgeable about the key principles, technical tools, and methods used to ensure cybersecurity. To comprehend vulnerabilities, threats, gaps, and risks, as well as their characteristics and basic risk management approaches.
CLO 4 To be familiar with the functions of essential tools used in both defensive and offensive cybersecurity.
CLO 5 To be able to implement security policies by applying security management tools (controls, methods, and techniques). To possess general knowledge about the relevance, development, and application of cybersecurity policies and the means of their implementation.
CLO 6 To comprehend global, regional, and national cybersecurity standards, regulations, and best practices, and be capable of monitoring their development.

Course Learning Outcomes for the subject “Fundamentals of Networks” (CLOs)
CLO 1 To possess basic knowledge of computer networks.
CLO 2 To comprehend network transmission devices, their characteristics and limitations, key network hardware components, and their functions.
CLO 3 To recognize different network topologies and comprehend network architectures, design principles, and communication protocols.
CLO 4 To identify the OSI layers, comprehend the principles of IP addressing, subnetting, IP address distribution, and address classes.
CLO 5 To be able to configure and set up routing in networks and install appropriate network devices corresponding to various OSI layers.
CLO 6 To comprehend the fundamental concepts related to ensuring network security and reliability.

Course Learning Outcomes for the subject “Linear Algebra” (CLOs)
CLO 1 To comprehend the general definition of a matrix, its various types, all operations on matrices and their key properties, as well as matrix transposition. To be proficient in computing determinants of second- and third-order matrices.
CLO 2 To possess knowledge of the concepts of minors and cofactors, the expansion of a determinant along a row or column, the inductive definition of higher-order determinants, and methods for calculating them. To be able to compute the determinant of a product of two matrices and the inverse of a square matrix. To be capable of performing operations on orthogonal and block matrices.
CLO 3 To comprehend the concept of *n*-dimensional vectors, the definition of linear dependence of vector systems, the necessary and sufficient condition for linear dependence, and methods for calculating the rank of a matrix. To possess knowledge of the definition, basis, and dimension of a vector space; linear transformations; matrices of linear transformations; and operations on them. To comprehend the concepts of eigenvalues and eigenvectors of a matrix, and be able to use algorithms to find them.
CLO 4 To have knowledge of systems of linear algebraic equations, including homogeneous and non-homogeneous linear systems, as well as consistent and inconsistent systems. To be able to solve systems of linear algebraic equations using the Cramer’s rule and the Gauss method, and solve homogeneous linear algebraic systems.
CLO 5 To have knowledge of polynomials, arithmetic operations on them, and the algorithm for polynomial division with remainder. Mustcomprehend Bézout’s theorem and the algorithm of Horner’s scheme. Mustknow Lagrange and Newton methods for finding bounds of real roots of polynomials.
CLO 6 To comprehend quadratic forms, their representation in matrix form, and canonical form of quadratic forms. Must be able to transform a quadratic form into its canonical form using Lagrange and Jacobi methods.

Course Learning Outcomes for the subject “Operating Systems” (CLOs)
CLO 1 Distinguishes between various operating systems, comprehends their differences, and identifies their areas of application.
CLO 2 Explains the core functions of operating systems, including process management and hardware interaction.
CLO 3 Comprehends inter-process communication mechanisms and the principles of parallel processing.
CLO 4 Describes how an operating system manages memory and utilizes relevant tools and methods for memory-based analysis.
CLO 5 Comprehends the architecture of file systems and input/output mechanisms in different operating systems and knows how to interact with them through programming interfaces.
CLO 6 Comprehends the main security mechanisms in operating systems and the principles of access control and privilege management.

Course Learning Outcomes for the subject “Network Security” (CLOs)
CLO 1 To be able to organize authentication, identification, and rule-based access control within a network.
CLO 2 To be able to conduct network auditing and logging activities.
CLO 3 To comprehend protocols and connection types related to network security, and be familiar with methods of connecting IoT devices to the Internet or other networks.
CLO 4 To be able to configure and manage DMZ (Demilitarized Zone) settings when integrating or connecting networks with other networks.
CLO 5 To possess essential knowledge of next-generation firewalls.
CLO 6 To be aware of known network attacks and comprehend the methods for preventing them or mitigating their effects in a short period of time.

Course Learning Outcomes for the subject “Discrete Mathematics” (CLOs)
CLO 1 To possess knowledge of elementary Boolean functions and their properties. To be able to express functions using formulas and work with structurally similar formulas. To comprehend tautologies, contradictions, and the equivalence of logical expressions.
CLO 2 To be familiar with binary functions and the principle of duality. To be able to expand Boolean algebra functions with respect to variables and construct their perfect disjunctive and conjunctive normal forms.
CLO 3 To know the basic applications of Boolean functions in modeling digital circuits and cryptographic primitives.
CLO 4 To comprehend the necessary elements of number theory used in public-key cryptography and their application in relevant cryptographic algorithms.
CLO 5 To possess knowledge of the fundamental elements of finite fields and be familiar with examples of their applications in cryptographic algorithms.

CLO 6 To be able to comprehend graph representation techniques and algorithms for finding shortest paths in weighted graphs and apply them to network modeling (e.g., OSPF).

Course Learning Outcomes for the subject “Web Security” (CLOs)
CLO 1 To comprehend how web browsers function, and possess knowledge of the design, development, and deployment principles of web applications.
CLO 2 To be able to create secure web pages using modern technologies. To have knowledge of HTML, CSS, and JavaScript.
CLO 3 To comprehend how the HTTP protocol works, how SSL certificates operate, and how they contribute to securing web pages.
CLO 4 To be aware of the nature of common attacks on websites.
CLO 5 To comprehend how modern web services such as REST and GraphQL work.
CLO 6 To be familiar with the OWASP Top 10 security vulnerabilities, be able to identify them, and apply mitigation techniques to prevent them.

Course Learning Outcomes for the subject “Probability Theory” (CLOs)
CLO 1 To comprehend the concepts of stochastic experiment and events. To be able to perform operations on events. To have knowledge of the classical definition of probability and basic combinatorics.
CLO 2 To comprehend the concepts of conditional probability and independence of events. To master the total probability and Bayes’ theorems. To comprehend the concepts of entropy and information quantity and be able to apply them to problems related to information encoding.
CLO 3 To know Bayes’ theorem, the concepts of random variables and distribution functions, and be familiar with some common discrete and continuous distributions. To comprehend Poisson random processes, Markov chains, and basic models of queuing systems.
CLO 4 To be familiar with major discrete distributions (Bernoulli, Binomial, Poisson, and Geometric distributions). To know the major continuous distributions (Uniform, Exponential, Normal, and Cauchy distributions).
CLO 5 To be able to determine the distribution of the sum of independent random variables and the distribution of functions of random variables. To know the expected value and other statistical characteristics of random variables.
CLO 6 To comprehend higher-order moments, covariance, and correlation coefficient concepts.

Course Learning Outcomes for the subject “Legal Aspects of İnformation Security And Cybersecurity” (CLOs)
CLO 1 To acquire knowledge of the fundamentals of information law, its sources, elements of legal relations, and subjects of legal norms, as well as the fundamental human rights and freedoms in the field of information.

CLO 2 To be familiar with the main directions of state policy in the information field in the Republic of Azerbaijan, relevant strategies and state programs, and to comprehend the national security interests and information security policy of the country.
CLO 3 To be acquainted with the main normative legal acts related to information security and cybersecurity, and to know their requirements.
CLO 4 To acquire general knowledge of the legal and organizational aspects of ensuring the security of critical information infrastructure, including the classification of infrastructure
CLO 5 To comprehend the legal requirements for the protection of personal data, as well as information considered state secrets and confidential information, including professional, commercial, investigative, and judicial secrets; and know the liability measures for violations of these legal requirements.
CLO 6 To acquire general knowledge of the concept and classification of cybercrimes, the legal basis for combating cybercrime, as well as the notions and characteristics of information warfare and cyber warfare, modern challenges, and the legal aspects of hybrid warfare.

Course Learning Outcomes for the subject “Information Security Management Systems” (CLOs)
CLO 1 Comprehends the concept, purpose, and fundamental principles of information security management.
CLO 2 Comprehends the necessity of organizing information security management and recognizes its benefits.
CLO 3 Is familiar with local and international standards related to information security management.
CLO 4 Comprehends the structure and scope of the ISO/IEC 27000 family of standards.
CLO 5 Acquires knowledge of the key concepts and principles of the ISO/IEC 27001:2013 standard, including the main terminology used in the standard.
CLO 6 Comprehends the requirements of the ISO/IEC 27001:2013 standard and the methods of their implementation.

Course Learning Outcomes for the subject “Fundamentals and Security of Database” (CLOs)
CLO 1 Comprehends the main functions of Database Management Systems (DBMS). Is capable of working with several modern DBMS platforms. Knows how relational DBMS system catalogs operate and what information they contain. Is able to perform database auditing and logging to ensure security and reliability.
CLO 2 Manages user profiles, password policies, permissions (rights), and roles in DBMS to implement fundamental security measures.
CLO 3 Identifies causes of database availability issues. Comprehends backup strategies, synchronization methods, and load balancing techniques.

CLO 4 Knows the methods for maintaining data integrity in databases. Is capable of applying various encryption techniques and solutions at different levels (file system, table, column, etc.) in databases.
CLO 5 Is aware of threats originating from application programs. Comprehends SQL injection attacks and related threats, and knows prevention techniques.
CLO 6 Comprehends NoSQL database types, their operating principles, practical significance, and their advantages and disadvantages compared to traditional DBMS.

Course Learning Outcomes for the subject “Cloud Security” (CLOs)
CLO 1. Presents the principles of cloud services, provides general information about the basic services offered, and comprehends the differences, advantages, and disadvantages compared to traditional services.
CLO 2 Is capable of designing simple solutions using cloud services and implementing appropriate security measures through both theoretical and practical approaches.
CLO 3 Explains serverless computing, its characteristics and distinctions, as well as the responsibilities related to security issues within these services.
CLO 4 Knows the framework, methods, and criteria for measuring risks and vulnerabilities in the cloud environment.
CLO 5 Is able to use network security tools in the cloud environment.
CLO 6 Recognizes symptoms of data breaches in the cloud, monitors them, identifies their causes, and possesses the ability to prevent them.

Course Learning Outcomes for the subject “Fundamentals of Cryptography” (CLOs)
CLO 1 To comprehend the differences between classical and modern cryptography, and is familiar with cryptanalysis methods of classical ciphers. To have knowledge of the distinctions between symmetric and asymmetric encryption systems.
CLO 2 To know how the principles of information security—confidentiality, integrity, authentication, and non-repudiation—are ensured using cryptographic methods.
CLO 3 To comprehend the differences between block ciphers and stream ciphers, be familiar with corresponding algorithms and their application areas.
CLO 4 To have knowledge of algorithms related to public-key cryptography and their applications. To be informed about the Public Key Infrastructure.
CLO 5 To comprehend the properties of hash functions, how integrity is ensured through their use, and their role in digital signatures.
CLO 6 To be knowledgeable about advanced cryptographic protocols and their applications.

Course Learning Outcomes for the subject “Fundamentals of Penetration Testing” (CLOs)
CLO 1 You will become familiar with the principles and techniques of penetration testing.
CLO 2 You will learn the stages of the penetration testing process.
CLO 3 You will be introduced to active and passive information gathering methods.

CLO 4 You will learn how to identify, exploit, and assess the risk of security vulnerabilities for a given target, as well as propose mitigation strategies.
CLO 5 You will become familiar with the tools used during penetration testing.
CLO 6 You will acquire knowledge on preparing professional reports based on the results of penetration tests.

Course Learning Outcomes for the subject “Security of Electronics and IoT Devices” (CLOs)
CLO 1 Recognizes OSAS electronic components such as logic circuits, converters, resistors, capacitors, transistors, inductive coils, and diodes; is capable of assembling circuits using these components.
CLO 2 Is able to use simulation software to observe and test electronic circuits.
CLO 3 You can use measuring instruments to measure the main parameters of electrical circuits.
CLO 4 Is familiar with various protocols for data exchange between devices.
CLO 5 Is knowledgeable about different technologies for wireless communication between devices.
CLO 6 Is able to study information security issues related to IoT devices, comprehends possible cyber-attacks against them, and has knowledge of methods of protection from such attacks.

Course Learning Outcomes for the subject “Secure Programming” (CLOs)
CLO 1 Comprehends what software security is and the reasons why vulnerabilities occur.
CLO 2 Comprehends the structure of computer memory, memory overflow issues, and how related exploits work.
CLO 3 Has knowledge the importance of considering security aspects during software architecture design and the principles of vulnerability prevention.
CLO 4 Is capable of using tools for software code audit, including automated dynamic and static code testing.
CLO 5 Comprehends the importance of security throughout the entire software development lifecycle and the principles of monitoring it.
CLO 6 Is able to perform secure code audits and is knowledgeable about the most common software security vulnerabilities worldwide.

Course Learning Outcomes for the subject “Fundamentals of Digital Forensics” (CLOs)
CLO 1 To comprehend the role and importance of digital forensics in forensic computer-technical expertise; to be familiar with its types, research methods, and be able to apply them.
CLO 2 To be able to distinguish digital evidence of probative value, to comprehend their types and significance.
CLO 3 To study the procedural principles of identification, collection, documentation, storage, use, protection, and presentation of digital evidence.
CLO 4 To acquire knowledge and skills to use necessary resources and equipment for the identification, collection, documentation, storage, use, protection, and presentation of digital evidence, as well as be able to apply open-source and advanced solutions.

CLO 5 To conduct forensic diagnostics of digital evidence, evaluate obtained results, and be able to formulate conclusions.
CLO 6 To have knowledge of the necessary legal procedures and requirements to ensure the admissibility of evidence.

Course Learning Outcomes for the subject “Security of Industrial Control Systems” (CLOs)
CLO 1 To comprehend the differences between IT and OT environments, as well as the protocols and operation of OT systems.
CLO 2 To be able to identify vulnerabilities and weaknesses in systems within critical infrastructures and to acquire methods to mitigate them.
CLO 3 To be familiar with systems such as PLC, DCS, RTU, HMI, and AVR used in critical infrastructures.
CLO 4 To be able to identify potential cyber threats in critical infrastructures and to perform risk analysis.
CLO 5 To know how to apply appropriate cybersecurity measures from the IT environment to the OT environment.
CLO 6 To be capable of analyzing incidents related to critical infrastructures and to comprehend the necessary steps to identify root causes.

Course Learning Outcomes for the subject “Civil Defense” (CLOs)
CLO 1 To know the fundamentals, forces, and means of civil defense.
CLO 2 To comprehend emergencies and their characteristics.
CLO 3 To acquire knowledge on the protection of the population during emergencies and public awareness related to civil defense.
CLO 4 To be capable of using personal and collective protective equipment.
CLO 5 To have knowledge of the fundamentals of ensuring and assessing the operational stability of industrial facilities during emergencies.
CLO 6 To possess knowledge on organizing and implementing measures to eliminate the consequences of emergencies.

Appendix 5

Matrix of Courses and Educational Program Learning Outcomes

Higher education institutions must determine how courses support the achievement of the learning outcomes of the Educational Program for the respective specialty, using the table below

		Program Learning Outcomes					
Block Title	**Course Titles**	**PLO 1**	**PLO 2**	**PLO 3**	**PLO 4**	**PLO 5**	**PLO 6**
General Courses	History of Azerbaijan	X					
	Business and Academic Communication in the Azerbaijani Language	X					
	Azerbaijani Statehood and Ideology	X					
	Business and Academic Communication in a Foreign Language	X					
	Fundamentals of Information Security	X		X			X
	Fundamentals of Programming		X		X		
	Mathematical Analysis		X		X		
	Fundamentals of Cybersecurity	X		X			X
	Fundamentals of Networks			X	X		
	Linear Algebra		X				
	Operating Systems					X	
	Network Security					X	
	Discrete Mathematics		X	X			
	Web Security			X			
	Probability Theory and Mathematical Statistics		X		X		
	Legal Aspects Of İnformation Security And Cybersecurity		X	X			
	Information Security Management Systems			X	X	X	X
	Database Security			X		X	
	Cloud Security			X		X	
	Fundamentals of Cryptography				X		
	Fundamentals of Penetration Testing			X			
	Fundamentals of Electronics and IoT Security					X	
	Secure Programming			X			X

		Program Learning Outcomes					
Block Title	**Course Titles**	**PLO 1**	**PLO 2**	**PLO 3**	**PLO 4**	**PLO 5**	**PLO 6**
	Fundamentals of Digital Forensics				X		
	Security of Industrial Control Systems	X					X